UNIVERSIDAD DE CHILE
FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS
DEPARTAMENTO DE INGENIERÍA ELÉCTRICA

DISEÑO E IMPLEMENTACIÓN DE EXPERIENCIAS DOCENTES PARA UN SITIO PROVEEDOR DE SERVICIOS INTERNET

RODRIGO ANDRÉS PAREDES MORALEDA

2000

UNIVERSIDAD DE CHILE
FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS
DEPARTAMENTO DE INGENIERÍA ELÉCTRICA

DISEÑO E IMPLEMENTACIÓN DE EXPERIENCIAS DOCENTES PARA UN SITIO PROVEEDOR DE SERVICIOS INTERNET

RODRIGO ANDRÉS PAREDES MORALEDA

COMISIÓN EXAMINADORA		NOTA (nº)	CALIFICACIONES (Letras)	FIRMA
PROFESOR GUÍA SR. ALFONSO EHIJO	:	……	……	……
PROFESOR CO-GUÍA SR. ALAIN COPPENS	:	……	……	……
PROFESOR INTEGRANTE SR. CLAUDIO HELD	:	……	……	……
NOTA FINAL EXAMEN DE TÍTULO	:	……	……	……

MEMORIA PARA OPTAR AL TÍTULO DE
INGENIERO CIVIL ELECTRICISTA

SANTIAGO DE CHILE
AGOSTO 2000

RESUMEN DE LA MEMORIA
PARA OPTAR AL TÍTULO DE
INGENIERO CIVIL ELECTRICISTA
POR : RODRIGO PAREDES MORALEDA
FECHA : AGOSTO DE 2000
PROF. GUÍA : SR. ALFONSO EHIJO

DISEÑO E IMPLEMENTACIÓN DE EXPERIENCIAS DOCENTES PARA UN SITIO PROVEEDOR DE SERVICIOS INTERNET

En la actualidad el análisis y diseño de las redes de computadores considera con mayor frecuencia los servicios ofrecidos por la *"red"*, por ejemplo: web, correo electrónico, etc. De este modo, cobra relevancia el conocimiento y comprensión de los servicios y sus mecanismos de implementación.

Esta memoria aborda el tema de los servicios Internet a través de un laboratorio docente, donde propone un plan sistemático con el cual se consigue la puesta en marcha de un Proveedor de Servicios Internet (ISP) a pequeña escala y de baja inversión, en adelante ISP mínimo. En las primeras tres experiencias se familiariza al alumno con los tópicos básicos asociados a un ISP, y en las tres siguientes se muestra como implementar el ISP en cuestión.

La metodología empleada comienza con un estudio de la arquitectura de hardware necesaria y del sistema operativo Linux. Luego se determinan los servicios básicos que presta un ISP. Con esta base se planifica la segmentación del proceso de implementación del ISP mínimo. La segmentación se materializa en la confección de las guías de laboratorio, donde se muestran las acciones a seguir para poner en marcha los servicios contemplados. Por último se realiza la validación técnica de las guías experimentales.

Para la confección de las guías de laboratorio se incluye un método que ya ha sido probado en otras memorias. El cuerpo de las guías consiste en una colección de pasos necesarios para la implementación de las actividades. Los pasos se separan en grupos temáticos o secciones. Se incluyen puntos de control intermedios y un cuestionario final, de modo que el alumno pueda controlar el grado de entendimiento de las actividades realizadas. Adicionalmente se acompaña material de apoyo para las guías de laboratorio.

Para la realización del laboratorio docente se utilizó la menor infraestructura de hardware posible, de modo de poder implementarlo en las instalaciones del laboratorio de Internetworking que actualmente dispone el Departamento de Ingeniería Eléctrica de la Universidad de Chile.

Como resultado de esta memoria se diseñaron seis guías experimentales que tratan los siguientes temas: Introducción a los ISP; Instalación de Linux y verificación inicial del sistema operativo; Administración básica de Linux; Habilitación de los servicios DNS, HTTP, TELNET y FTP; Habilitación de los servicios de conectividad y Habilitación de mecanismos de seguridad, servicios de correo electrónico y PROXY.

Con los mecanismos propuestos en las guías de laboratorio se logra poner en correcta operación los servicios del ISP mínimo, lo que prueba la validez técnica de las experiencias.

Para realizar la implementación de un ISP de mayor envergadura, se indican algunas consideraciones en el capítulo cinco de Discusión.

En lo inmediato, las guías propuestas en esta memoria sirven de apoyo a los cursos EL64E: "Redes de Computadores" y EL54B: "Sistemas de Procesamiento de la Información" y son complementarias para el curso EL717: "Seminario de Sistemas Digitales", impartidos en el Departamento de Ingeniería Eléctrica, Universidad de Chile.

Como una continuación del trabajo se puede considerar la implementación de laboratorios docentes orientados a tópicos tales como servicios de alta disponibilidad, planificación de redes, servidores de acceso, seguridad en redes, sistemas de administración y calidad de servicio. Con estos laboratorios se potenciará la cobertura en la docencia de postítulo impartida en el Departamento de Ingeniería Eléctrica.

a mis padres, César y Isa,
a Waldo, César y Paz
y a mis queridos sobrinos,
Cesitar y Valentina

XXIII

–¡Buenos días! –dijo el principito.

–¡Buenos días! –respondió el comerciante.

Era un comerciante de píldoras perfeccionadas que quitan la sed. Se toma una por semana y ya no se siente ganas de beber.

–¿Por qué vendes eso? –preguntó el principito.

–Porque con esto se economiza mucho tiempo. Según el cálculo hecho por los expertos, se ahorran cincuenta y tres minutos cada semana.

–¿Y qué se hace con esos cincuenta y tres minutos?

–Lo que cada uno quiere...

–Si yo dispusiera de cincuenta y tres minutos –pensó el principito– me iría a la fuente con toda tranquilidad...

Tomado de “El Principito”, de Antoine de Saint Exupéry

AGRADECIMIENTOS

Tengo que agradecerle a muchas personas que estuvieron conmigo durante mi larga estadía por la Escuela, en estos años he aprendido mucho de ellos y quisiera darles un reconocimiento por todo su apoyo.

En primer lugar le doy las gracias a la mujer más valiente que he conocido, mi querida y amada madre, Isa, no sé si hubiese llegado tan lejos sin tu incondicional apoyo. También agradezco a mi padre, César, que aunque muchas veces no supe entender tus consejos, siempre estuviste ahí cuidándome, haciendo tu mejor esfuerzo.

A mis dos hermanos Waldo y César por todo su apoyo también les debo mucho, y a ti Paz por ayudarme a aprender a querer a los demás y darnos tus bellísimos hijos, Cesitar y Valentina.

A mis amigos Jorge León y Juan Manuel Vargas y sus familias por la infinidad de momentos que tuvimos desde que nos conocimos en el Instituto Nacional.

A todas las personas que forman parte del preuniversitario José Carrasco Tapia, en especial a Carlos Lillo, Ana Cáceres, Luis Carrasco, Paola Torres y María Teresa Villarroel por todas las cosas que hicimos juntos y las que vendrán.

A mis compañeros de escuela Juan Pérez, Eduardo Morales y Fernando Flattow, a los que les deseo mucho éxito en sus vidas.

A mis amigas Paula Miño y Estrella Callejas, que me dieron esa clase de apoyo que sólo ellas saben dar.

A mis profesoras Carmen Ortiz y Nancy Lacourly, por sus trucos y consejos.

A Alfonso, mi profesor guía, por su irrefrenable apoyo y estímulo.

A FirstCom Chile, y mis colegas de Ingeniería y Desarrollo por toda la ayuda que me dieron, que no fue poca.

A todos Ustedes, muchas gracias.

Índice

Índice de Ecuaciones

Índice de Figuras

Índice de Tablas

Capítulo 1: Introducción

1.1 Marco General

Actualmente, el proceso de convergencia entre los "Sistemas de Comunicaciones Tradicionales" tales como la red telefónica publica conmutada (PSTN) y las "Redes de Computadores" es un hecho. Se materializa con la Internet global y sus servicios desde los más fundamentales (E-mail, WWW, FTP) hasta algunos más sofisticados tales como voz sobre IP (VoIP), mensajería multimedial unificada y otros.

Esta convergencia del las comunicaciones y la computación ha originado nuevos desafíos tecnológicos y nuevas oportunidades de negocios. Dentro de estas oportunidades figura el surgimiento de empresas orientadas a dar conectividad a otras compañías a la Internet y a proveer los servicios Internet. Este concepto se materializa en los Proveedores de Servicio Internet.

El tema principal de esta memoria consiste en desarrollar los tópicos asociados a un ISP de pequeña escala y de baja inversión, desde la perspectiva de experiencias docentes de laboratorio. Se construyen seis guías experimentales, las que pretenden apoyar el entendimiento de los aspectos a considerar en un ISP, dirigidas tanto a los alumnos del Departamento de Ingeniería Eléctrica (DIE), como a otros profesionales interesados en el área.

1.1.1 Presentación del Tema

En el contexto del trabajo desarrollado, las "Experiencias Docentes" son experimentos orientados a un laboratorio tanto de pregrado como de postítulo, destinados a llevar a la práctica los conocimientos adquiridos en los cursos abocados al tema "Redes de Computadores" que se dictan en el DIE, vale decir los cursos "Redes de Computadores" y "Redes de Alta Velocidad" y el programa de postítulo en Internetworking dictado en el departamento. Se realizará especial hincapié en los servicios Internet.

Los contenidos cubiertos en estos cursos son: protocolos de enrutamiento, modelos de referencia de arquitecturas de redes (OSI, TCP/IP y ATM), el stack de protocolos TCP/IP, seguridad en redes, servicios Internet, etc. En el laboratorio se pretende cohesionar estos temas y de este modo comprender el funcionamiento de un ISP.

Esta memoria se concentrará en los tópicos asociados a la puesta en marcha de un ISP, principalmente desde el punto de vista de los servicios Internet.

1.1.2 Objetivos Generales

Los objetivos principales de este trabajo son los siguientes:

- Establecer un esquema sistemático para el proceso de puesta en marcha de un ISP de pequeña escala y de baja inversión.
- Diseño, Implementación y validación de experiencias para un laboratorio tanto de pregrado como de postgrado orientado al tema de los ISP.

Esto se traduce en desarrollar un conjunto de seis "Guías Paso a Paso", que permitan a los alumnos poner en práctica los conocimientos adquiridos en los cursos de redes de computadores e Internetworking.

1.1.3 Objetivos Específicos

Para conseguir que los alumnos entiendan el funcionamiento y puesta en marcha de un ISP mínimo, se consideran los siguientes objetivos específicos:

- Plantear una segmentación del proceso de implementación de un ISP. Esta segmentación se concretará en el diseño de guías de laboratorio, en donde se especifiquen los pasos a seguir para conseguir cada etapa del proceso de implementación de un ISP. De entre las actividades a realizar se destaca:
  - Implementación de Métodos de Acceso (dedicado y conmutado).
  - Introducción a la Seguridad en Redes.
  - Habilitación de Servicios Internet (DNS, WWW, FTP, E-mail).
- Utilizar una metodología para la implementación de las experiencias de laboratorio, de manera de generar las "Guías Paso a Paso" para cada sesión de laboratorio.
- Validar las experiencias de laboratorio, de manera de poder evaluar la calidad de las guías desarrolladas, desde el punto de vista práctico, y así garantizar el éxito de las experiencias propuestas.

1.2 Motivación

Las motivaciones del presente estudio incluyen razones comerciales, tecnológicas y docentes.

Desde el punto de vista comercial y tecnológico, Internet es un excelente negocio pleno en desafíos tecnológicos. Inicialmente el foco de los ISP comerciales apuntaba al ofrecer conectividad a sus clientes. Actualmente, la explosión de popularidad que ha conseguido Internet, ha impulsado a los ISP comerciales a proveer servicios tales como E-mail, FTP, web hosting, servicios de contenido, E-commerce y otros. De este modo, el mercado de los ISP está ávido de profesionales capacitados en el tema.

Desde el punto de vista docente, actualmente en el DIE se imparten cursos teóricos enfocados al tema Internetworking, y se está comenzando a ofrecer cursos con orientación práctica. Por lo cual este trabajo se presenta como un apoyo para mejorar la docencia en el departamento, en especial se suma a los incipientes esfuerzos por mejorar la componente experimental en la docencia en redes de computadores, apelando a la estrategia de aprendizaje "Aprender Haciendo", que resulta idónea para este tipo de estudio.

Para plantear un esquema sistemático en la implementación de un ISP, se muestra un plan de sesiones experimentales, de modo que el alumno desarrolle las actividades y consiga poner en marcha el ISP mínimo al menor costo posible.

Dentro de los alcances del trabajo figura que los alumnos que desarrollen las experiencias debieran ser capaces de poner en marcha ISP pequeños (por ejemplo, un ISP que satisfaga los requerimientos de una empresa pequeña o mediana). Este ISP pequeño, o ISP cliente, presta la mayor cantidad posible de servicios a su entorno local, y a través de un enlace de comunicaciones, se conecta a la Internet a través de un ISP mayor o ISP proveedor, de donde puede obtener los otros servicios que se ofrecen en la red. Esta situación se muestra en la Figura 1.

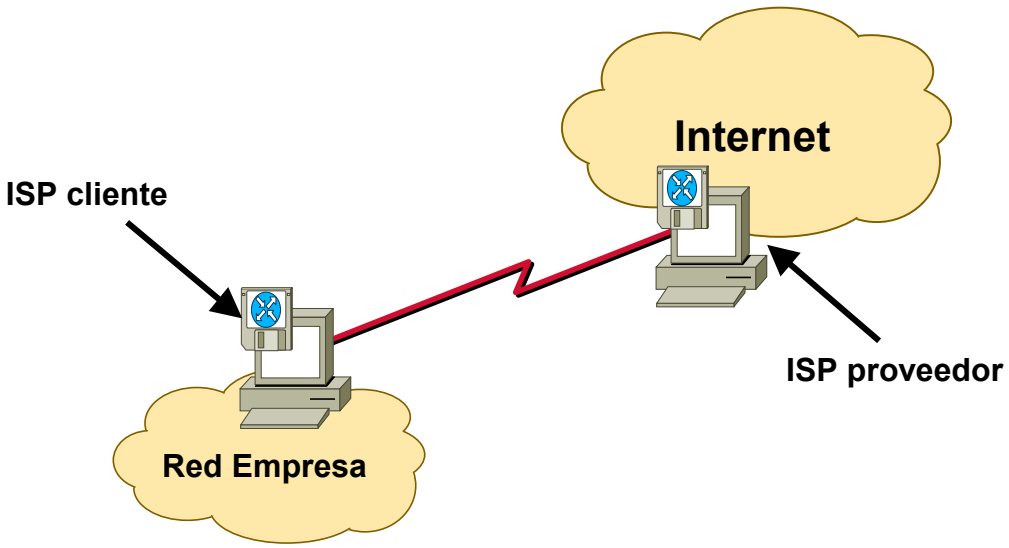


Figura 1. Conexión de un ISP cliente a su proveedor

1.3 Reseña Histórica

A mediados de la década de 1970, la Agencia de Proyectos de Investigación Avanzada de Defensa de Estados Unidos (DARPA) se interesó en establecer una red de conmutación de paquetes para proveer comunicaciones robustas entre instituciones de investigación civiles y militares. DARPA y otras organizaciones gubernamentales entendieron el potencial de la tecnología de conmutación de paquetes y estaban comenzando a enfrentar el problema de la comunicación transparente entre sistemas de computación disímiles.

Con el objetivo de la conectividad heterogénea en mente, DARPA, consolidando las investigaciones de la Universidad de Stanford y Bolt, Beranek and Newman (BBN), desarrolló una serie de protocolos de comunicación. El resultado de este esfuerzo, completado a fines de 1970, fue la familia de protocolos Internet, de los cuales el Protocolo de Control de Transmisión (TCP) y el Protocolo Internet (IP) son los dos más conocidos.

Durante los años 1980, las tecnologías Internet y las redes fueron adoptadas por otras agencias gubernamentales y otros países, de modo de potenciar el sector de negocios privados y las organizaciones gubernamentales, educacionales, etc. Hoy, las tecnologías de Internet e Internet han encontrado aceptación masiva y son usadas por cientos de miles de organizaciones alrededor del mundo. La organización internacional global para la coordinación de Internet es la Sociedad Internet (ISOC) [ISOC].

Internet en Chile comienza como una iniciativa académica, con el surgimiento de dos redes universitarias (REUNA y RDC), que se conectaban a la red global a través de enlaces satelitales, pero sin conexión entre ellas. A medida que se popularizó el servicio, nacieron sitios ISP asociados a empresas del área de las telecomunicaciones (ENTEL, Terra, VTR, FirstCom) que ofrecen Internet a particulares y a empresas en general, con velocidades de acceso desde 64 Kb a 10 Mb o superiores.

Los primeros ISP inicialmente no estaban conectados entre sí debido a que el mayor requerimiento de tráfico fue hacia el extranjero; esto implicaba que a menudo las conexiones nacionales eran mucho más lentas que las internacionales. Con el pasar del tiempo, el crecimiento del contenido y los servicios de información nacionales motivaron a que los ISP interconectaron sus redes, lo que disminuyó ostensiblemente los tiempos de retardo y espera de las comunicaciones. Luego empresas de otros rubros distintos al de las telecomunicaciones (por ejemplo empresas comerciales o empresas de servicios

informáticos), habilitaron pequeños ISP en sus oficinas, que fueron conectados a los ISP principales, de modo que sus empleados pudieran aprovechar las oportunidades que abre Internet, conectándose con mayores velocidades, y aumentando la gama de servicios ofrecidos y utilizados. Así las empresas nacionales (tanto medianas y como grandes empresas) pudieron acceder a servicios tales como E-MAIL, WWW, FTP, noticias USENET, telnet, etc., administrando su información en forma local, lo que disminuye la dependencia de estas empresas a sus proveedores Internet.

1.4 Hipótesis de Trabajo y Metodología

Una de las restricciones que se imponen al trabajo es el de minimizar en lo posible los costos, debido a esto se trabajará sobre la base de computadores económicos que operen con el sistema operativo LINUX, que es de distribución gratuita.

La metodología propuesta para llevar a cabo el trabajo es la siguiente:

1. Estudio de la arquitectura de hardware necesaria para el sitio.
2. Estudio de las características de LINUX.
3. Determinación de los servicios básicos que presta un ISP.
4. Plantear la segmentación de las etapas de la implementación.
5. Generación de las guías de laboratorio para cada segmento de la implementación.
6. Validación técnica de las guías.

1.5 Descripción de Contenidos

En el capítulo uno Introducción, se muestra el marco general del trabajo, sus objetivos, la motivación y las hipótesis de trabajo.

En el capítulo dos Antecedentes, se muestran los conceptos básicos de Internetworking, la arquitectura de Internet, una breve descripción del sistema operativo Linux y la descripción básica de un ISP.

En el capítulo tres Metodología, se detallan las hipótesis de trabajo, la estructura de las guías de laboratorio, la metodología de construcción del ISP mínimo y la planificación de las experiencias.

En el capítulo cuatro Resultados, se muestran los resúmenes de las guías del laboratorio docente de ISP.

En el capítulo cinco Discusión, se realiza una revisión de los resultados, de modo de analizar la aplicabilidad de la metodología propuesta. También se hacen comparaciones con ISP comerciales de mayor tamaño.

En el capítulo seis Conclusiones, se presentan las principales conclusiones obtenidas en el trabajo y posibles innovaciones futuras.

En el capítulo siete Referencias y Acrónimos, se detallan todas las fuentes de información, sean estas en medios impresos o digitales. Para el caso de los digitales se indica la fecha de la obtención de la información. También se presenta una lista de acrónimos utilizados en la memoria, ordenados alfabéticamente.

En los Anexos se incluyen todas las guías de laboratorio desarrolladas, e información de apoyo tanto para la memoria y como para las experiencias.

Capítulo 2: Antecedentes

En este capítulo se mostrará una visión panorámica de una serie de conceptos fundamentales para el entendimiento del resto del documento. Parte de la información contenida en esta sección se complementa con los anexos.

2.1 Estructuras de Redes

Hasta ahora no existe alguna taxonomía que permita clasificar todas las redes que se conocen actualmente, pero una buena manera para resolver esta situación es analizar las siguientes características: la tecnología de transmisión y la escala geográfica de la red [Tanenbaum 1997] y [Neira 1998].

Dentro de las tecnologías de transmisión destacan dos tipos: las redes de difusión y las redes punto a punto.

Respecto a la escala geográfica se distinguen las redes de área local (LAN), las redes de área metropolitana (MAN) y las redes de área amplia (WAN). Para entender las diferencias entre las LAN, MAN y WAN hay que analizar tres características: tamaño, tecnología de transmisión y topología.

En las redes de difusión todas las máquinas comparten un único canal (o medio) de comunicación. Luego, los mensajes de datos (o paquetes) enviados por una máquina cualquiera son recibidos por todas las demás. Dentro del paquete existe información relativa a la dirección de destino, de modo que si una máquina recibe un paquete verifica el campo de direccionamiento, y si es la que le corresponde toma el mensaje y lo procesa, si no, lo ignora. Este tipo de red permite definir con relativa facilidad dominios de difusión colectiva o selectiva, es decir, una máquina envía información hacia todas las otras (difusión colectiva) o a una colección determinada de computadoras (difusión selectiva), lo que se conoce en la jerga como dominios de broadcasting y multicasting, respectivamente. Este esquema de conexión es usado preferentemente en las LAN y MAN, debido a la simpleza de su implementación.

Las redes punto a punto se caracterizan por tener una gran cantidad de conexiones entre pares individuales de máquinas. Con esta configuración, para que un paquete viaje de una máquina a otra, eventualmente deberá visitar otras máquinas intermedias.

Dependiendo de la topología de la red, el camino que seguirá el mensaje será único, o existirán varias opciones, por lo que los algoritmos de enrutamiento cobran gran importancia en el desempeño de una red punto a punto. Debido a la forma de las redes punto a punto, el transporte de los paquetes sigue una estrategia conocida como almacenamiento y reenvío (store and forward). Las redes WAN utilizan este esquema de red, puesto que permite una mayor flexibilidad al realizar la implementación física de la red.

2.1.1 Redes de Área Local (LAN)

A menudo las LAN se instalan dentro de localidades de pequeña extensión geográfica, tales como edificios o campus de pocos kilómetros de extensión. Esto permite que una institución sea dueña de toda la red, incluyendo los equipos y las líneas de transmisión, y más importante aún, sea capaz de administrar localmente sus instalaciones. Este tipo de red es usado frecuentemente para compartir recursos informáticos (espacio en disco, sistemas de impresión, etc.) e intercambiar información.

A menudo, la tecnología de transmisión empleada por las LAN corresponde a un cable sencillo al cual se conectan todas las computadoras, es decir son redes de difusión. Las velocidades usuales de estas redes son de 10 a 100 Mbps, tienen retardo de décimas de microsegundo, y experimentan pocos errores. Nuevas LAN pueden operar a velocidad aún mayores, de varios cientos o miles de Mbps.

En general, en una LAN se utilizan las topologías de bus o de anillo, las que se muestran en la Figura 2, aunque también se pueden emplear otras topologías más complejas.

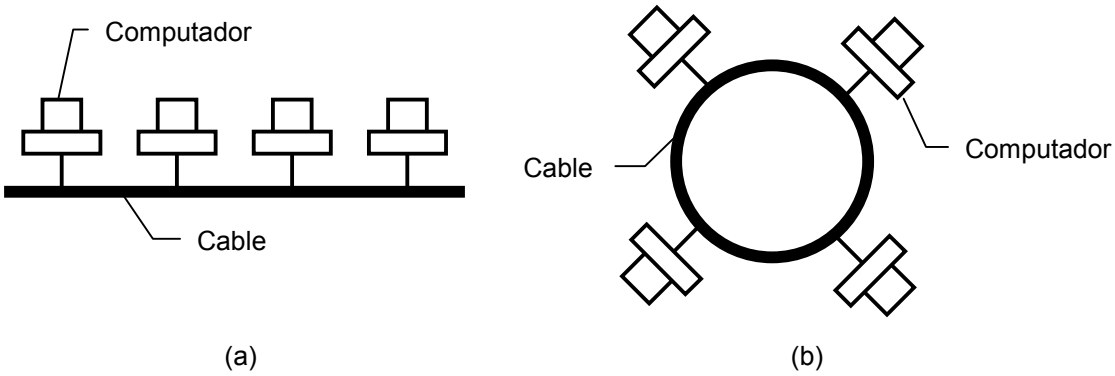


Figura 2. Topologías de redes LAN. (a) Bus. (b) Anillo

En el bus, cuando el canal está libre, es decir ninguna máquina transmite a través de él, cualquier máquina puede asumir la función de maestra transmitiendo información y las otras quedan imposibilitadas de transmitir hasta que la maestra termine su paquete. Cuando se da el caso de que dos o más máquinas intenten transmitir a la vez, se necesitan mecanismos de arbitraje para discernir cual máquina lo hará primero.

Un ejemplo de red tipo bus es la IEEE 802.3, muy similar a Ethernet. Los mecanismos de arbitraje también se denominan métodos de acceso al medio físico, para Ethernet se emplea conjuntamente el método de Muestreo y el de Contención. Cuando se intenta transmitir un mensaje, la máquina muestrea el canal para verificar que nadie lo esté utilizando, y si ocurre alguna colisión, mediante contención, se fuerza a que todas las máquinas dejen de enviar paquetes a la red. Esto se conoce en la jerga como CSMA/CD.

En un anillo, cada bit de un paquete se propaga por sí mismo, recorriéndolo completamente en el tiempo que toma transmitir pocos bits, en general, antes de que el paquete completo sea transmitido. Al igual que en las redes de bus, se necesitan mecanismos de arbitraje para resolver conflictos de acceso simultáneo al anillo.

Un ejemplo de red tipo anillo es la IEEE 802.5, conocida como token ring. El método de acceso al medio físico de token ring es Paso de Testigo. Paso de Testigo es un esquema de control de turnos, que permite que una máquina pueda transmitir sin realizar colisiones con las otras máquinas de la red. El testigo es un paquete especial, que constantemente circula por la red. Si la máquina recibe el testigo significa que puede transmitir. Si tiene información para enviar, conserva el testigo, envía su información, y vuelve a transmitir el testigo; si no tiene información que enviar a la red, la máquina le cede el testigo a la siguiente en el anillo.

Las redes de difusión se pueden dividir en estáticas y dinámicas, dependiendo de cómo se asigna el canal. Una asignación estática típica divide el tiempo en intervalos discretos, y mediante un algoritmo de asignación cíclico, se permite a cada máquina transmitir únicamente cuando llega su turno. Este método desperdicia la capacidad del canal, puesto que cuando una máquina no tiene nada que decir durante su segmento, ninguna otra lo puede utilizar, debido a esto muchos sistemas intentan asignar el canal por demanda o dinámicamente.

Los métodos de asignación dinámica para un canal compartido pueden ser centralizados o distribuidos. Cuando es centralizado, una de las máquinas asume la labor de arbitrar cuál es la siguiente que puede “hablar”. La unidad arbitradora escoge quien transmite a través de recepción de solicitudes, procesamiento de prioridades u otro algoritmo. En el caso de la asignación dinámica distribuida, no se tiene la entidad central de arbitraje, por lo que cada máquina en forma autónoma debe decidir si transmite o no.

2.1.2 Redes de Area Metropolitana (MAN)

Una MAN es básicamente una versión más grande de una LAN y normalmente se basa en una tecnología similar. La extensión geográfica es hasta unas decenas de kilómetros, y puede ser privada o pública. Una MAN puede manejar datos y voz, e incluso estar vinculada con una red de televisión por cable local. En general, una MAN administra un solo medio de transmisión compuesto por uno o dos enlaces (con dos enlaces se pueden implementar medidas de respaldo de la conexión) y contiene pocos elementos de conmutación, lo que simplifica bastante su diseño.

Ejemplos de MAN son las redes IEEE 802.6, o Bus Dual de Cola Distribuida (DQDB), y la red Interfaz de Datos Distribuidos por Fibra (FDDI). Mayor referencia de estas tecnologías en [Tanenbaum 1997].

Un aspecto clave de las MAN es que hay un medio de difusión único al cual se conectan todas las computadoras, lo cual simplifica mucho el diseño de la red. Se pueden emplear MAN para interconectar LAN distribuidas en una ciudad.

2.1.3 Redes de Área Amplia (WAN)

Una red WAN se extiende sobre un área geográfica extensa, un país, un continente, o todo el mundo. Contiene una colección de máquinas dedicadas a ejecutar programas de aplicación para los usuarios, llamados hosts, las que están conectadas entre sí por una subred de comunicaciones, o simplemente subred. Esta separación de tareas, hosts por un lado y subred por el otro, se hace para simplificar el análisis y diseño total de la red.

En general, para la subred de una WAN se pueden diferenciar dos elementos: las líneas de transmisión, y los elementos de conmutación. Las líneas de transmisión se encargan de mover bits desde una máquina a otra. Los elementos de conmutación o conmutadores son computadoras que se encargan de conectar dos o más líneas. Cuando el conmutador recibe información por una línea de entrada, debe escoger una línea de salida para reenviarlos. En general la subred constituye una red punto a punto, salvo en el caso de que se trate de una subred satelital, donde es más propio hablar de red de difusión.

En una WAN los hosts pertenecen a redes locales que cuentan con uno o más conmutadores, también se tiene el caso de hosts directamente conectados al conmutador. El conjunto de conmutadores y líneas de comunicación forma la subred de comunicación. Note que la subred es capaz de conectar distintos tipos de LAN, tal como se aprecia en la Figura 3.

Como ya se mencionó, en una WAN es característica la existencia de líneas de comunicación entre pares de nodos de conmutación, pero para establecer una comunicación entre conmutadores que no comparten una línea de transmisión debe hacerse indirectamente, a través de los otros conmutadores de la subred. En esta estrategia de comunicación intervienen nodos de conmutación intermedios, los que reciben el paquete completo antes de reenviarlo por la línea correspondiente (y sólo cuando la línea esté libre de transmisiones), por lo cual estas subredes se clasifican como de almacenamiento y reenvío. Una excepción a esta regla son las subredes satelitales, donde se usa la metodología de difusión para el transporte de los paquetes de información.

Para el diseño de la subred punto a punto de una WAN, se tienen varias topologías. Para WAN de envergadura pequeña se puede emplear una topología densa en conexiones, tal como es la malla completa, pero a medida que aumentan los nodos de conmutación de la subred, la cantidad de enlaces necesarios para la malla completa crece considerablemente, puesto que al agregar el n-ésimo nodo, se deben agregar n - 1 nuevos enlaces. Siguiendo este razonamiento, para calcular el número de enlaces necesarios se debe resolver la sumatoria mostrada en la Ecuación 1, y como se observa, el resultado es de $O(n^2)$, con n la cantidad de nodos de la subred.

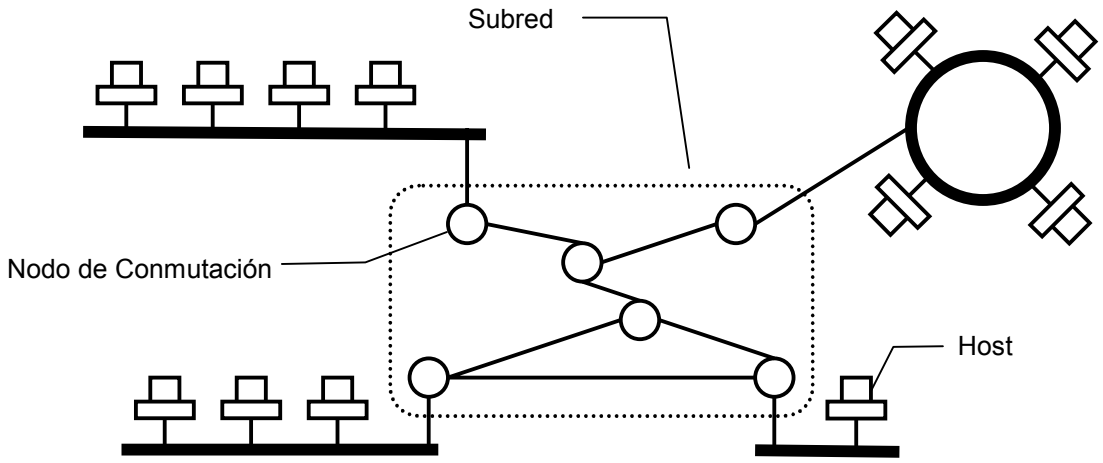


Figura 3. Relación entre hosts y la subred

$$\sum_{0}^{n-1} i = \frac{(n-1)n}{2}$$

Ecuación 1. Número de enlaces en una topología de malla completa

Este resultado hace inviable la implementación de la topología malla completa para la subred de una WAN con 5 o más conmutadores. Afortunadamente existen otras topologías para la construcción de la subred, las que se muestran en la Figura 4.

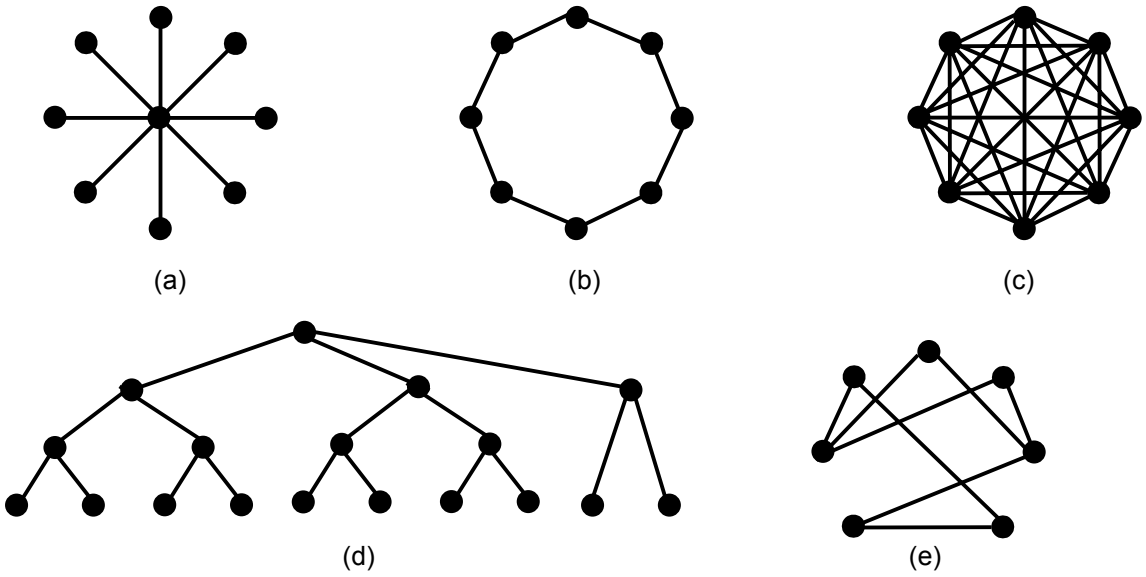


Figura 4. Topologías frecuentemente usadas para subredes punto a punto. (a) Estrella. (b) Anillo. (c) Malla completa. (d) Árbol. (e) Irregular

El lector podrá apreciar que en general las alternativas de conexión corresponden a topologías con muy baja densidad de enlaces, del orden *O(n)*, con *n* la cantidad de nodos, lo que podría comprometer la disponibilidad de los servicios a nivel global en la WAN, por esto, una vez que se escoge la alternativa de conexión, es importante establecer las políticas de respaldo de conectividad. Es importante destacar que a medida que aumenta la complejidad de la red, ésta comienza a perder su simetría con lo que se convierte en una red punto a punto irregular.

La alternativa de subred satelital, consiste en que los conmutadores poseen una antena por medio de la cual pueden enviar / recibir octetos (la palabra española para referirse a los bytes) hacia / desde el satélite. Es usual que estos conmutadores estén conectados a una subred punto a punto terrestre, con lo que se consigue una subred de comunicaciones híbrida de gran cobertura.

2.2 Arquitecturas de Redes

Para enfrentar el diseño e implementación de una red, conviene emplear un modelo de capas, de manera de poder dividir funcionalmente el problema. Gracias a este tipo de modelos, se puede transformar un problema de gran tamaño en varios problemas pequeños y manejables. Este tipo de metodología obedece a una de las reglas con mayor frecuencia usadas en ingeniería: "dividir para conquistar".

Cada capa se construye sobre la inferior. El número de capas, su nombre, contenido y función difieren de red en red, sin embargo, en todos los modelos jerárquicos de capas, el propósito de una capa es ofrecer servicios a la superior de manera transparente, es decir, sin que ella tenga conocimiento sobre cómo se realizan dichos servicios.

La Figura 5 muestra una red cuatro capas. La capa n del Host 1 conversa con la capa n del Host 2, basado en un protocolo de comunicación de capa n, que corresponde a un conjunto de reglas y convenciones que norman la transferencia de la información. Las entidades de las capas correspondientes en máquinas diferentes se denominan pares. Si bien es cierto que la abstracción que ofrece este modelo es que una entidad puede comunicarse con su par, esto en realidad no ocurre. La comunicación real consiste en que cada capa pasa datos e información de control a su capa inmediatamente inferior hasta llegar a la capa 1. Bajo la capa 1 se tiene el medio físico a través del cual se transfiere la información hacia la otra máquina. Una vez que la información llega al medio físico bajo la capa 1 del otro Host, “suben” los datos y la información de control en la máquina destino realizando el camino inverso. En la Figura 5 se muestran líneas continuas para las comunicaciones reales, y punteadas para las comunicaciones virtuales.

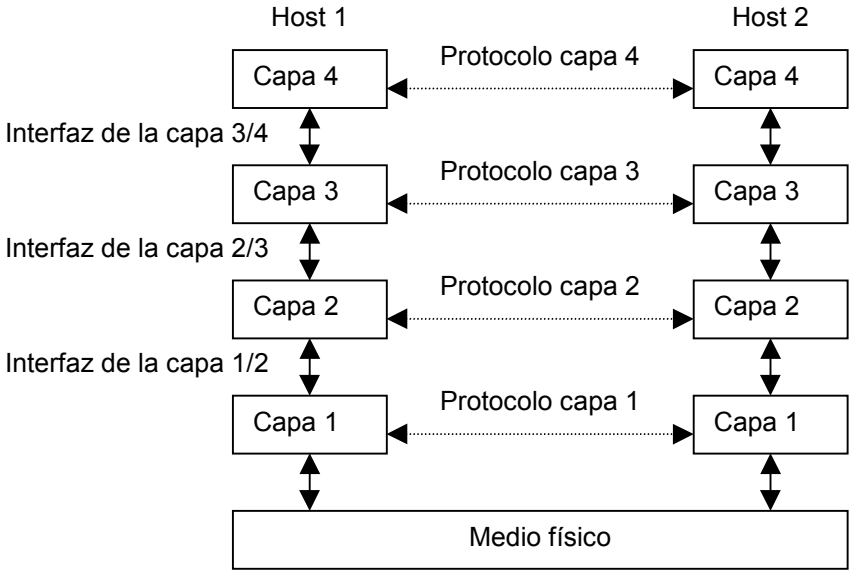


Figura 5. Capas, protocolos e interfaces en una red

Entre cada par de capas se tiene una interfaz. La interfaz define qué operaciones y primitivas de servicio ofrece la capa inferior a la superior. Las primitivas de servicio son los mecanismos con que una capa ofrece sus funcionalidades a la capa superior. La correcta definición de una interfaz es clave en la construcción de redes, pues permite por un lado minimizar la información transferida de capa en capa y

por otro reemplazar la implementación de la capa por otra totalmente distinta sin que la capa superior o inferior se entere de este detalle.

El conjunto de capas y protocolos recibe el nombre de Arquitectura de Red, cuya especificación debe tener la información suficiente como para que un implementador sea capaz de escribir un software o construir hardware para una capa dada, y que éste opere de acuerdo a los protocolos establecidos.

2.3 Modelos de Referencia

A continuación se mostrarán breves descripciones de dos ejemplos de modelos jerárquicos de capas, estos son el modelo de referencia OSI de la Organización Internacional de Estándares (ISO), y el modelo de referencia TCP/IP. El modelo OSI es ampliamente usado para formalizar los conceptos en redes debido a su fuerte componente docente y didáctica, lamentablemente no se tiene ninguna implementación comercial exitosa de este modelo. El modelo TCP/IP es el estándar de facto de Internet.

2.3.1 Modelo de Referencia OSI

El modelo OSI se muestra en la Figura 6 y como se observa, tiene siete capas. Se basa en una propuesta de la Organización Internacional de Normas, como un primer paso para la estandarización internacional de los protocolos empleados en diversas redes. El principal propósito del modelo de referencia OSI es entregar recomendaciones que permitan una integración global de las distintas tecnologías de comunicaciones de redes públicas.

Los principios que se emplearon al diseñar las capas de modelo OSI son:

- Se debe crear una capa siempre que se necesite un nivel diferente de abstracción.
- Cada capa debe realizar una función bien definida.
- La función de cada capa se debe definir en función de protocolos estandarizados internacionalmente.
- Los límites de las capas deben elegirse a modo de minimizar el flujo de información a través de las interfaces.
- La cantidad de capas debe ser suficiente para no tener que agrupar funciones distintas en la misma capa y lo bastante pequeña para que la arquitectura no se vuelva inmanejable.

No es tema de esta memoria profundizar en el modelo OSI. A continuación se mostrará una breve descripción de lo que hace cada capa.

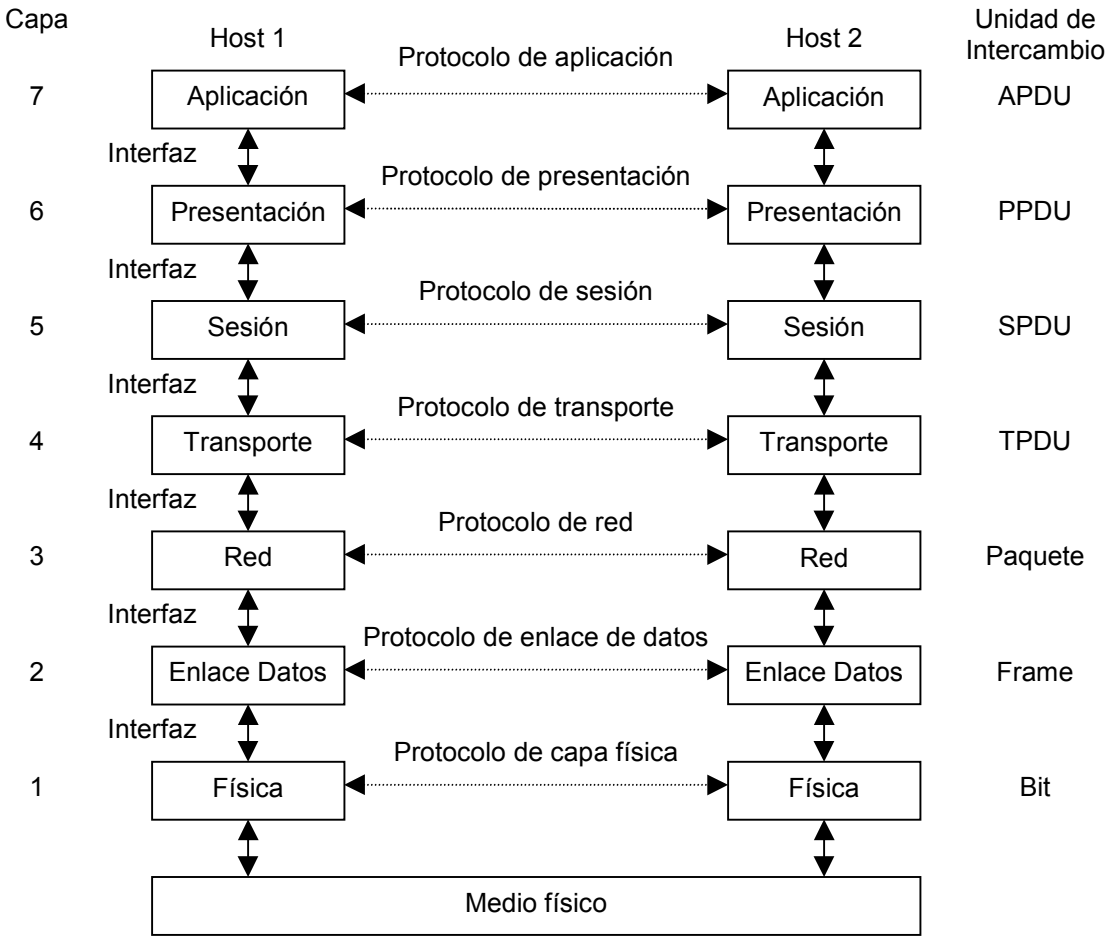


Figura 6. El modelo de referencia OSI

2.3.1.1 La capa física

La capa física tiene que controlar la transmisión de bits por un canal de comunicación. Esto significa que debe verificar que cuando emisor envíe un bit 1, el receptor lo reciba como bit 1, no como bit 0. Las preguntas que se plantean a este nivel son: ¿Qué nivel de voltaje corresponde al 0 lógico, y cuál al 1?, ¿Cuántos microsegundos se necesitan para transmitir un bit?, ¿La transmisión será en una dirección (comunicación simplex), en ambas direcciones pero no simultánea (comunicación halfduplex) o en ambas direcciones y simultánea (comunicación duplex)?, ¿Cómo se establece la conexión inicial, y cómo se interrumpe cuando ambos extremos solicitan la desconexión?. Junto con esto, a este nivel se definen el tipo de conector a emplear, las especificaciones mecánicas, eléctricas, térmicas, etc. de las interfaces físicas que se utilizaran. También se preocupa de la interacción con el medio físico que está bajo la capa física.

2.3.1.2 La capa de enlace de datos

La principal tarea de esta capa es tomar un medio de transmisión en bruto y transformarlo en una línea que parezca libre de errores de transmisión y ofrecer este canal confiable a la capa de red. Para hacer esto, toma la información de la capa de red, y la divide en porciones de decenas, cientos o miles de bytes llamadas frames, los transmite en orden secuencial, procesa los “acuse de recibo” (ACK) que devuelve el receptor y toma acciones cuando hay errores en la transmisión. Dado que la capa física sólo se preocupa de transmitir los bits sin importarle su contenido o significado, es la capa de enlace de datos la que se

preocupa de definir y detectar los límites de cada frame, lo que se puede hacer a través de símbolos especiales (por ejemplo cadenas de bits que violen los patrones válidos) y así poder reconstruir la información para entregarla a la capa de red.

Esta capa debe preocuparse de la recuperación de errores, lo que se puede resolver mediante la retransmisión de frames en caso de errores en la transmisión. También debe preocuparse de manejar las transmisiones duplicadas de frames, o de acuses de recibo.

En esta capa se tiene que resolver el problema de compatibilizar las velocidades de transmisión y recepción de máquinas distintas, de modo que una máquina rápida no sature a una lenta. La función de compatibilizar la velocidad se coparte con otras capas del modelo OSI, en particular con la capa de transporte.

2.3.1.3 La capa de red

Esta capa se ocupa de controlar el funcionamiento de la subred de comunicaciones. Una consideración clave de diseño es determinar como se encaminan los paquetes desde la fuente a su destino. Las rutas se pueden basar en tablas estáticas que se "alambran" en la red y rara vez cambian, también se pueden determinar al inicio de cada conexión, o pueden ser altamente dinámicas, determinándose con cada paquete de acuerdo a la carga actual de la red.

Es aquí donde se realiza control de congestión de la red, que trata de evitar que se formen cuellos de botella por exceso de paquetes circulando en la subred, lo que disminuye el nivel de las prestaciones.

En esta capa se realizan funciones de contabilidad. Se pueden contar los paquetes, bytes o bits que un cliente (un usuario de la red) transfiere por la red. El proceso de la contabilidad y tarificación de la red se puede complicar cuando el tráfico de una subred tenga como destino otra subred con otro sistema de contabilidad y tarificación.

Al transferir paquetes a través de la subred es probable que en algún momento alguno de los enlaces falle, y es la capa de red la que se preocupa de recuperar este tipo de errores. Por otro parte, para prevenir la congestión en la subred, la capa de red se puede preocupar de balancear la carga por los enlaces de la subred de modo de mantener un nivel razonable de tráfico circulando en las líneas.

Como se puede apreciar, la capa de red tiene gran importancia en las redes de punto a punto, en cambio, como en las redes de difusión el medio por el cual se transmiten los paquetes es único, esta capa tiene muy pocas funciones o en algunas ocasiones no está presente.

A este nivel ya se pueden considerar conexiones end to end (de un extremo al otro), es decir la capa de red de una máquina “ve” a su capa par de la otra, con la salvedad de que la comunicación se produce a través de saltos entre los nodos de la subred de comunicaciones.

2.3.1.4 La capa de transporte

La función básica de la capa de transporte es aceptar los datos de la capa de sesión, dividirlos en unidades más pequeñas si es necesario, pasarlos a la capa de red y asegurar que todos los trozos lleguen correctamente al otro extremo. Además todo esto se debe hacer de manera eficiente y en forma que aísle a las capas superiores de los cambios inevitables en la tecnología del hardware.

La capa de transporte ofrece a las capas superiores una canal libre de errores desde un extremo al otro de la comunicación. Nótese que esta funcionalidad la comparte con la capa de enlace de datos, con la diferencia que el control de errores en la capa de datos tiene sentido local (de un nodo a otro) y en la capa de transporte tiene sentido global (de un extremo al otro). Por otra parte, en la capa de red los paquetes pueden ser transmitidos por rutas distintas para llegar a su destino, y es en la capa de transporte en donde deben ser ordenados, si es que es necesario. Con esto se consigue que un programa en la máquina fuente sostiene una conversación con un programa similar en la máquina de

destino, haciendo uso de los encabezados de mensajes y de los mensajes de control. En las capas bajas (capa 1 y 2), los protocolos operan entre cada máquina y sus vecinas inmediatas, en la capa 3 la comunicación es de extremo a extremo a través de saltos en la subred, en cambio desde la capa de transporte hacia arriba (capa 4 a 7) los protocolos operan entre origen y destino (como si fuese una conexión directa) los que pueden estar separados por muchos conmutadores intermedios.

2.3.1.5 La capa de sesión

La capa de sesión permite a los usuarios de máquinas diferentes establecer sesiones entre ellos. Una sesión permite el transporte ordinario de datos, como lo hace la capa de transporte, pero también proporciona servicios mejorados que son útiles en algunas aplicaciones.

Uno de los servicios de la capa de sesión es manejar el control del diálogo. Las sesiones pueden permitir que el tráfico vaya en ambas direcciones simultáneamente, o sólo en una dirección a la vez. Si el tráfico puede viajar sólo en un sentido a la vez, la capa de sesión puede ayudar a llevar el control de los turnos.

2.3.1.6 La capa de presentación

Esta capa realiza ciertas funciones que se piden con suficiente frecuencia para justificar la búsqueda de una solución general, en lugar de dejar que cada usuario resuelva los problemas. Un ejemplo de esta situación es el manejo y adaptación de formatos de números enteros (complemento a uno, o complemento a dos), o la representación de caracteres (ASCII o Unicode). La capa de presentación se preocupa de realizar automáticamente los cambios, con lo que se libera al usuario de esta tarea.

2.3.1.7 La capa de aplicación

La capa de aplicación es la capa OSI más cercana al usuario, y no presta servicios a ninguna otra capa del modelo, en cambio, si presta servicios a las aplicaciones que están fuera del ámbito del modelo OSI. Estas aplicaciones pueden ser planillas de cálculo, procesadores de texto, terminales virtuales, etc.

2.3.1.8 Transmisión de datos en el modelo OSI

En la Figura 7 se muestra un ejemplo de cómo se pueden transmitir datos empleando el modelo OSI, utilizando el mecanismo de encapsulamiento. El proceso emisor tiene algunos datos para enviar al proceso receptor, por lo que entrega los datos a la capa de aplicación, la cual añade al principio del paquete un encabezado de aplicación AH (que puede ser nulo) y entrega el elemento resultante, la APDU, a la capa de presentación.

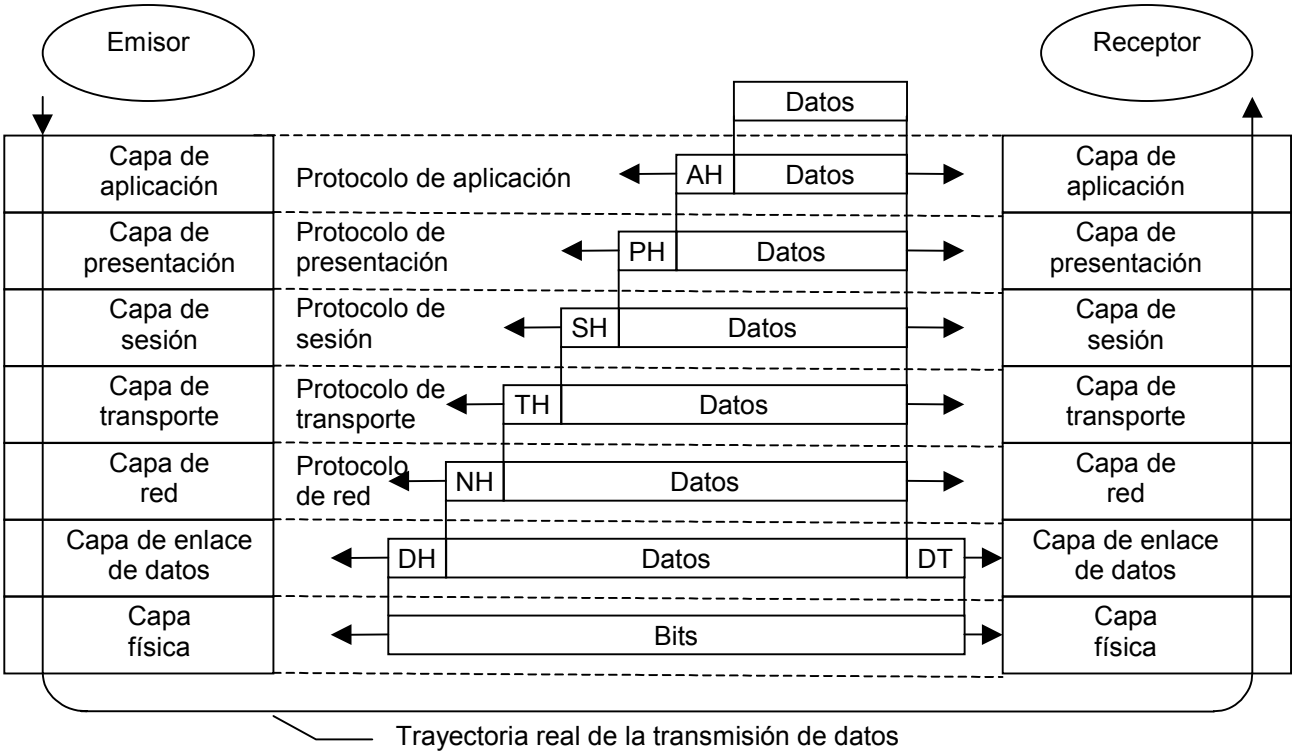


Figura 7. Ejemplo de uso del modelo OSI. Algunos encabezados pueden ser nulos

La capa de presentación puede transformar el paquete añadiéndole un encabezado PH, y entregando su resultado a la capa de sesión. La capa de presentación no sabe qué porción del paquete recibido son los datos del usuario, y cuál es el AH (si existe). Lo mismo sucede en la capa de sesión, y por último llega a la capa física, donde son transmitidos a la máquina receptora. En esa máquina, se retiran los encabezados a medida que el paquete sube desde la capa física hasta la de aplicación y luego los datos son tomados por el proceso receptor.

Es importante destacar que aunque la transmisión real de los datos es vertical (los datos deben “bajar” hasta el medio físico para ser transmitidos al siguiente nodo), cada capa se construye como si fuera horizontal. Esto significa que cuando la capa n recibe datos de la capa n + 1 (su capa superior), le añade un encabezado y lo transmite a la capa n de la máquina receptora. Desde su punto de vista, el hecho de que el mensaje está dirigido a la capa n – 1 (su capa inferior) de su propia máquina es un detalle de implementación que no tiene importancia.

2.3.2 El Modelo de Referencia TCP/IP

El modelo de referencia TCP/IP fue el que se usó en la antigua ARPANET, y actualmente se usa en la Internet mundial. Para entender las características del modelo TCP/IP es útil recordar cuáles eran los requerimientos que se le imponían. La ARPANET fue una red de investigación patrocinada por el DoD (Departamento de Defensa de los Estados Unidos). Luego de un tiempo, conectó a cientos de universidades e instalaciones de gobierno a través de líneas telefónicas. Cuando llegó el momento de añadir redes satelitales y de radio, los protocolos existentes fueron sobrepasados, de modo que se necesitó de una nueva arquitectura para la red. Se necesitaba conectar diversas redes de manera transparente.

Dentro de las preocupaciones del DoD estaba que alguno de los nodos de comunicaciones de la subred fueran víctimas de ataques en cualquier momento, afectando tanto el hardware como el software, y se deseaba que las conexiones permanecieran activas mientras las máquinas de origen y destino estuviesen operando, incluso si alguno de los nodos o líneas de transmisión en el trayecto dejaran de funcionar de manera repentina. También se pedía cierta flexibilidad en la arquitectura, pues se tenía la visión de aplicaciones con requerimientos divergentes, abarcando desde la transferencia de archivos hasta la transmisión de voz y video en tiempo real.

2.3.2.1 La capa internet

Todos estos requerimientos motivaron la elección de una red de conmutación de paquetes basada en una capa internet (o capa interred) carente de conexiones (lo que también se conoce como no orientado a la conexión). La capa internet, es el eje que mantiene toda la arquitectura. Su misión es permitir que los nodos inyecten paquetes en cualquier red y los hagan viajar independiente de su recorrido hacia su destino (el que podría estar en la misma red, o en otra distinta). Debido a que los paquetes viajan de manera autónoma, se puede dar la situación de que los paquetes lleguen en un orden diferente al que fueron enviados, en cuyo caso es labor de las capas superiores reacomodarlos, cuando se desee que la entrega sea ordenada.

Una analogía para entender el funcionamiento de la capa internet es el sistema de correos. Una persona puede depositar una serie de cartas internacionales en un buzón de su país, y confía en que la empresa de correos realizará su mejor esfuerzo para que las cartas lleguen al país de destino. Es probable que las cartas viajen a través de uno o más sitios intermedios (aeropuertos, oficinas postales, etc.) pero esto es transparente para los usuarios. Más aún, los usuarios no necesitan saber que cada país (esto es, cada red), tiene sus propias estampillas, tipos definidos de sobres y reglas de entrega.

La capa internet define un formato de paquete de datos y un protocolo oficial llamado IP, también se definen otros protocolos de capa internet. El trabajo de la capa consiste en entregar paquetes IP a donde se supone deben ir. A este nivel, la consideración más importante es el ruteo de los paquetes (qué camino seguirán los paquetes), y evitar la congestión en la red. Por esto se puede establecer una asociación entre las funcionalidades de la capa internet TCP/IP y la capa de red OSI. En la Figura 8 se muestra el modelo de referencia TCP/IP, y su correspondencia con el modelo de referencia OSI.

En adelante “Internet” se referirá a la red global, e “internet” a la capa internet del modelo TCP/IP.

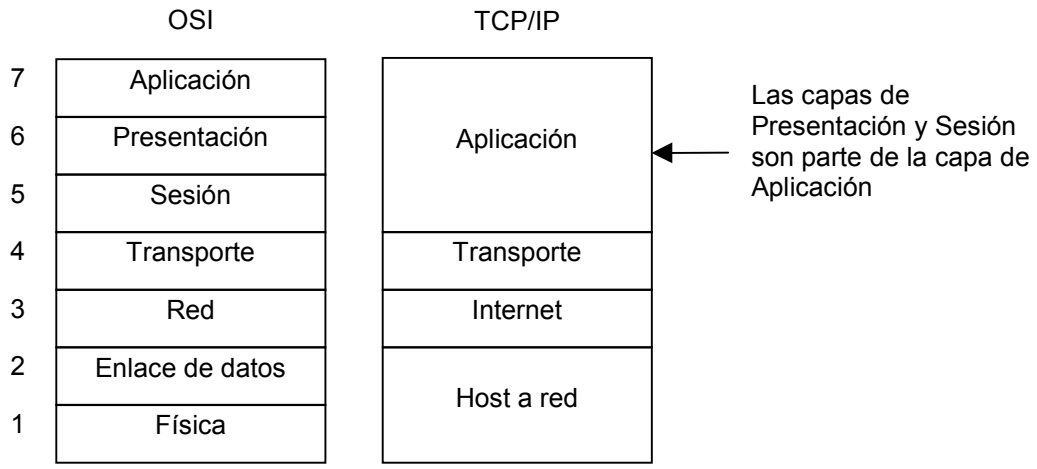


Figura 8. Las capas del modelo de referencia TCP/IP, comparadas con el modelo de referencia OSI

2.3.2.2 La capa de transporte

Esta capa, que está sobre la capa internet en el modelo TCP/IP, fue diseñada para permitir la comunicación entre las entidades origen y destino, equivalente a la capa de transporte en el modelo OSI. Se definieron dos protocolos de extremo a extremo: TCP y UDP.

TCP es un protocolo confiable orientado a la conexión. Un protocolo orientado a la conexión ofrece la abstracción de un túnel definido y fijo durante la transmisión, un ejemplo de protocolo orientado a la conexión es una llamada telefónica, donde una vez que se establece el circuito se conserva mientras dure la llamada. Un protocolo confiable garantiza que un flujo de bytes originado en una máquina se entregue sin errores en cualquier otra máquina de la red.

TCP particiona el flujo entrante de bytes, en mensajes de tamaño discreto y pasa cada porción a la capa internet. En el destino, el proceso TCP receptor reensambla los mensajes recibidos para formar el flujo de salida. TCP también se encarga de hacer control de flujo, de manera de que un emisor rápido no sature a un receptor lento con un exceso de mensajes.

UDP es un protocolo no orientado a la conexión y no confiable. Un protocolo no orientado a la conexión calcula la ruta que seguirá un paquete independientemente a los otros, un ejemplo de protocolo no orientado a la conexión es el sistema de correos, donde una carta no tiene por que seguir la misma ruta que otra para llegar a su destino. Un protocolo no confiable no garantiza la entrega del paquete a su destino, en la jerga también conoce como protocolo de mejor esfuerzo.

UDP se utiliza en aplicaciones que no necesitan la asignación de secuencia ni el control de flujo de TCP, o que deseen utilizar estrategias propias de control. También se usa para consultas de petición y respuesta de una sola ocasión, del tipo cliente-servidor, y en aplicaciones en que se privilegie la entrega pronta frente a la entrega precisa, como es el caso de voz o video en tiempo real.

2.3.2.3 La capa de aplicación

El modelo TCP/IP no tiene explícitamente consideradas las capas de sesión o presentación. La experiencia acumulada en OSI, donde fueron muy poco utilizadas dichas capas, mostró que fue acertado no considerarlas en TCP/IP.

Sobre la capa de transporte esta la capa de aplicación, la que contiene todos los protocolos de alto nivel. Entre los más antiguos están los de terminal virtual (TELNET), el de transferencia de archivos (FTP), el de correo electrónico (SMTP) y el de resolución de nombres (DNS). En la actualidad existen mucho más, y aparecen nuevos protocolos para responder a las necesidades de los usuarios [Spohn 1997], por ejemplo se tienen: el protocolo de transferencia de hiper textos (HTTP), el protocolo de llamada remota de procedimientos (RPC), el protocolo de transporte de noticias en la red (NNTP), y el sistema de archivos de redes (NFS), entre otros.

En la Tabla 1 se muestran algunos de los protocolos típicos de Internet y sus funcionalidades, y en la Figura 9 se muestran algunos protocolos de Internet agrupados según su capa de pertenencia.

Tabla 1. Protocolos típicos de Internet y su función

Protocolo	Función
TELNET	Permite que un usuario en una máquina ingrese a otra distante y pueda trabajar en forma remota y de modo transparente.
FTP	Ofrece un mecanismo por el cual se pueden transportar archivos de una máquina a otra de manera eficiente.
SMTP	Permite el transporte de los correos de una máquina a otra.
DNS	Permite relacionar o traducir los nombres de los nodos con sus direcciones de la red.
HTTP	Se emplea para la publicación de hiper páginas a través de servidores web y la recuperación en el computador del usuario.
RPC	Permite que un programa pueda usar los servicios de otro en forma remota. Este esquema se basa en el modelo cliente/servidor.
NNTP	Se utiliza para el transporte de artículos y noticias a través de la red.
NFS	Se utiliza para la administración de los sistemas de archivos a través de la red, se preocupa de controlar los permisos de los archivos, montar las unidades de manera transparente para el usuario, etc.

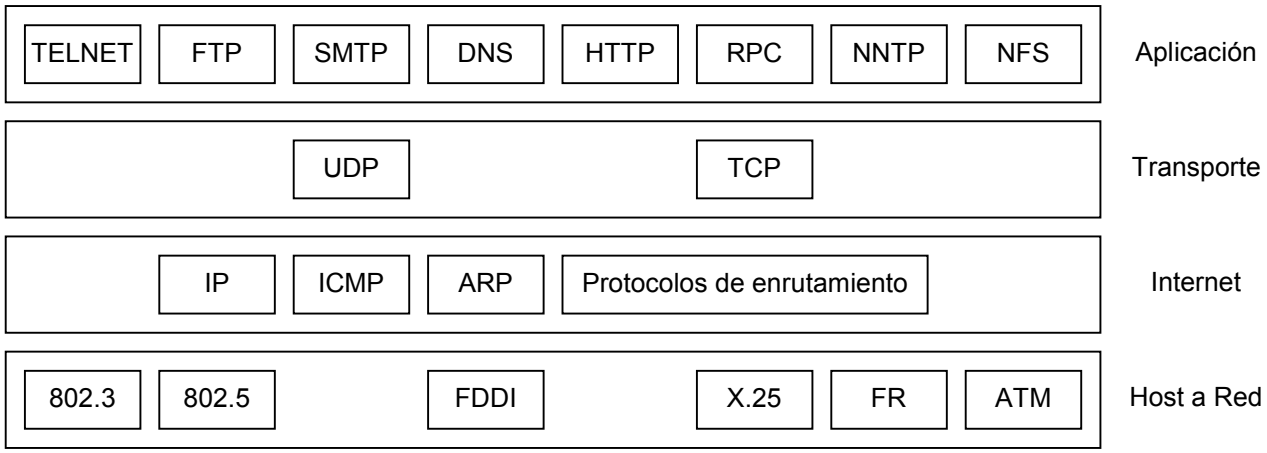


Figura 9. Protocolos y redes en el modelo de referencia TCP/IP

2.3.2.4 La capa del host a la red

En el modelo TCP/IP no especifica mayormente esta capa, por lo que muchos autores sentencian que "bajo la capa internet existe un gran vacío". Lo único que se indica es que el nodo se ha de conectar a la red mediante algún protocolo que permita enviar paquetes IP. Visto desde el punto de vista OSI, se debe escoger una implementación de la capa de enlace de datos y de la capa física que sea capaz de soportar el transporte de paquetes IP. Debido a esta indefinición de esta capa se origina la famosa frase "IP sobre todas las cosas".

2.4 Elementos de una Red

2.4.1 Dispositivos de Redes

Para diseñar una red de computadores, se dispone de los siguientes dispositivos básicos [Cisco IDB]: hubs, repetidores, bridges, switches y routers.

- Hubs: Los hubs o concentradores, son usados para conectar múltiples usuarios a un dispositivo físico, el cual es conectado a la red. Los hubs o concentradores realizan la misma labor de los repetidores regenerando las señales que pasan a través de ellos, y operan en la capa física del modelo OSI (OSI capa 1). A diferencia de un repetidor que tiene pocas puertas (2 en general), un hub repite las señales por varias puertas (de 5 a 24 puertas). Debido a que operan en la capa física, donde en general no se considera direccionamiento, no poseen facultades para establecer dominios.
- Bridges: El bridge es empleado para separar lógicamente segmentos dentro de la misma red, y operan en la capa de datos del modelo OSI (OSI capa 2). Una de las principales funciones de un bridge es poder realizar la traducción de paquetes de tecnologías de capa 2 (por ejemplo: en una puerta ethernet y en la otra token ring).
- Switches: El switch es similar al bridge, pero usualmente tiene más puertas. El switch provee un único segmento de red por cada puerta (esto se conoce como microsegmentación) siendo capaz de separar dominios de colisión. De este modo los errores producidos por colisiones de paquetes en un segmento no son transmitidos a los otros. Hoy en día los diseñadores de redes están reemplazando los hubs por switches de manera de incrementar las prestaciones y ancho de banda de una red, conservando las instalaciones de alambrado existentes. Al igual que los bridges, los switches operan en la capa de datos del modelo OSI (OSI capa 2).
- Routers: Los routers son equipos diseñados para interconectar redes en el ámbito de la capa de red del modelo OSI (OSI capa 3). Dentro de sus capacidades está la de separar dominios de broadcast,

lo que permite realizar un mejor empleo del ancho de banda en una red de gran extensión, de modo que los mensajes de difusión colectiva en una red sólo afectan a la red que los origina, sin utilizar los recursos de las redes vecinas. Los routers encaminan el tráfico de acuerdo al contenido del campo de direccionamiento de los paquetes de capa 3. Los routers son dependientes del protocolo.

Las técnicas de diseño e implementación de las redes actuales utilizan routers y switches para la gestión del tráfico, puesto que además de presentar un mejor desempeño, ofrecen mecanismos de crecimiento más flexible y escalable. Las redes previas se construían utilizando bridges y hubs.

2.4.2 Enlaces de Comunicaciones

La conexión de los distintos dispositivos de una red se realiza mediante enlaces de comunicación. Para ello se dispone de tecnologías de conectividad tales como enlaces seriales punto a punto (SLIP, CSLIP y PPP), Ethernet / IEEE 802.3, Token Ring / IEEE 802.5, X.25, FR, FDDI y ATM entre otros.

Estas tecnologías permiten encapsular la información del usuario de modo de poder transportarla desde un punto a otro en la red. No es tema de esta memoria ahondar en estas tecnologías, para mayor referencia consulte [Tanenbaum 1997].

2.5 Arquitectura de Internet

Como se indicó anteriormente, el modelo de referencia TCP/IP se constituye en la arquitectura de facto de Internet. Esta familia de protocolos permite la intercomunicación de una gran cantidad y variedad de computadores, de distinta capacidad y distinto sistema operativo, y fue comentada en la sección 2.3.2. “El Modelo de Referencia TCP/IP”. En esta sección se abordarán otros aspectos importantes en Internet: el mecanismo de direccionamiento de los nodos, la capacidad de encaminar los paquetes a través de la red y se mostrarán algunos de los servicios típicos que se ofrecen en Internet. Para mayor información refiérase a [Piquer 1997] y a [Kirch 1999].

2.5.1 Direccionamiento

Cada host o enrutador que esté conectado a la Internet tiene una dirección IP única, que se codifica en un espacio de direcciones de 32 bits. Las máquinas que estén conectadas a varias redes tienen direcciones IP diferentes en cada red.

Para simplificar los mecanismos de enrutamiento, la dirección IP se divide en dos porciones. La primera parte designa la dirección de red (bits superiores), y la segunda (bits inferiores) para designar la dirección de host. La porción de host, usualmente se divide en dos subporciones, la primera (si está presente) designa la dirección de subred (bits superiores) y la segunda a la dirección de host (bits inferiores). Las direcciones de subred son determinadas por el administrador si así lo decide, de modo de facilitar la administración en la red. El largo de los campos de red, subred y host son variables.

La notación actual de las direcciones IP consiste en cuatro números decimales separados por un punto (cada decimal codifica un byte sin signo: 0 a 255). Por ejemplo: 146.83.4.11.

Para indicar qué porción de una dirección IP corresponde a la red se emplea lo que se llama máscara de red. En la Tabla 2 se muestra el esquema de designación de máscaras de red empleado actualmente en Internet. En este esquema se definen clases y máscaras específicas para cada clase.

Tabla 2. Máscaras de red para direcciones IP

Clase	Máscara de red (binaria)	Máscara de red (decimal)
A	11111111.00000000.00000000.00000000	255.0.0.0
B	11111111.11111111.00000000.00000000	255.255.0.0
C	11111111.11111111.11111111.00000000	255.255.255.0

Dentro de las direcciones IP de una red dada, se tienen dos que están reservadas. Cuando todos los bits de la porción de host están en 0, se refiere a la red, y cuando todos los bits están en 1, se refiere a la dirección de broadcast.

Para especificar subredes, se modifica la máscara agregando bits en uno. Por ejemplo, la red de la Escuela de Ingeniería de la Universidad de Chile es 146.83.X.X, que corresponde a una clase B, con máscara 255.255.0.0. Las subredes de la Escuela son de 126 host, de modo que a la máscara de red se le agregan 9 bits en 1, con lo que se obtiene la siguiente máscara de red: 255.255.255.128.

Actualmente, las direcciones IP se escriben de modo de condensar la información de direccionamiento y máscara de red. Para esto a la dirección IP se le agrega el carácter '/' y a continuación el número de bits que corresponden a la máscara red y subred. Para el caso de una dirección de la escuela con subredes de 126 hosts, se tiene: 146.83.4.11/25. Note que el /25 indica que la máscara de red contiene 25 bits en 1, y quedan 7 bits para indicar el host.

Inicialmente, las direcciones se agruparon en clases según sus bits iniciales, y para cada clase se designaron cierta cantidad de bits para la red, y el resto para el host (y subred cuando corresponda). Actualmente se han designado ciertas direcciones IP que son utilizadas en las redes privadas, es decir redes definidas de acuerdo a los protocolos Internet, pero que no son de acceso público, sólo de acceso para la institución que administra la red [RFC 1918]. En el rfc citado se indica que estas direcciones IP son inválidas (puesto que son empleadas para direcciones privadas), de modo que si se van a usar, hay que tener cuidado de no anunciar estas direcciones a la Internet pública. Los formatos empleados para el direccionamiento se muestran en la Tabla 3. La X indica que el bit puede tomar el valor 0 ó 1.

Tabla 3. Formatos de dirección IP

Clase	Configuración de bits del byte superior	Bits red	Bits host	Número de redes	Host por red	Rango de direcciones posibles	Rango de direcciones IP inválidas
A	0XXX XXXX	8	24	126	16.777.214	1.0.0.0 a 127.255.255.255	10.0.0.0 a 10.255.255.255 (10.0.0.0/8)
B	10XX XXXX	16	16	16.382	65.534	128.0.0.0 a 191.255.255.255	172.16.0.0 a 172.31.255.255 (172.16.0.0/12)
C	110X XXXX	24	8	2.097.150	254	192.0.0.0 a 223.255.255.255	192.168.0.0 a 192.168.255.255 (192.168.0.0/16)
D	1110 XXXX	Dirección de difusión selectiva [RFC 1112]				224.0.0.0 a 239.255.255.255	
E	1111 0XXX	Reservadas para un uso futuro				240.0.0.0 a 247.255.255.255	

2.5.2 Enrutamiento

El enrutamiento es un mecanismo que se encarga de transportar la información desde un nodo inicial hasta uno final. Para ir de un nodo a otro de la red se puede enfrentar dos situaciones distintas:

- Los nodos están directamente conectados: Caso trivial, puesto que basta con escoger la ruta directa para la establecer la conexión.
- Los nodos no están directamente conectados: Se debe seleccionar una sucesión de pasos para llegar al destino.

El enrutamiento difiere del bridging, puesto que el primero se realiza con direcciones de la capa de red (OSI capa 3) por lo que tiene sentido global, en cambio el segundo se realiza con las direcciones de la capa de enlace (OSI capa 2) y sólo tiene sentido local.

El dispositivo de red que se encarga del enrutamiento se conoce como router, y puede estar conectado a dos o más redes. Otra denominación para los routers es gateways (pasarelas), que es un término empleado en muchas otras áreas de la industria, y con distintas funcionalidades. Por esta razón y a menos que se diga lo contrario, se considerará el término gateway como sinónimo de router.

Para enrutar los paquetes por la red se pueden utilizar técnicas de ruteo estático o dinámico. Las primeras son rutas que se configuran manualmente en las tablas de los routers, en cambio las segundas son establecidas a través de protocolos de enrutamiento que una vez configurados y puestos en marcha comienzan a aprender la topología de la red, actualizando automáticamente las tablas a medida que pasa el tiempo. Este proceso se conoce como convergencia de rutas.

En redes pequeñas se justifica el uso de rutas estáticas, pero a medida que la red crece, y aumenta el esfuerzo para actualizar manualmente las tablas de los routers comienza a tener sentido el empleo de protocolos de ruteo dinámico.

Los algoritmos de ruteo están basados en el análisis de tablas de rutas, las que son mantenidas en los routers y actualizadas ya sea manualmente, o a través de protocolos dinámicos de enrutamiento. En cada entrada de la tabla de enrutamiento se indica la red de destino, y el router que se debe emplear para llegar a ella, esto se conoce como el siguiente salto o next hop. El router que realiza la conexión se representa por una dirección IP de la red en la que se encuentra el router actual. También en esta tabla se indican las redes a las que está actualmente conectado el router local.

En la Tabla 4 se muestra la tabla de rutas del router A de la Figura 10, note que para las redes directamente conectadas, emplea la dirección de red de su propia interfaz (tipo directo), y sólo para las redes que no tiene directamente conectadas, utiliza las interfaces de otros routers de la red (tipo gateway), lo mismo sucede para el router B, tal como se ve en la Tabla 5.

Tabla 4. Tabla de enrutamiento IP del router A

Red	Next hop	Tipo
10.1.1.0/24	10.1.1.1	Dir
10.1.2.0/24	10.1.2.1	Dir
10.1.3.0/24	10.1.1.2	Gw
10.1.4.0/24	10.1.1.3	Gw

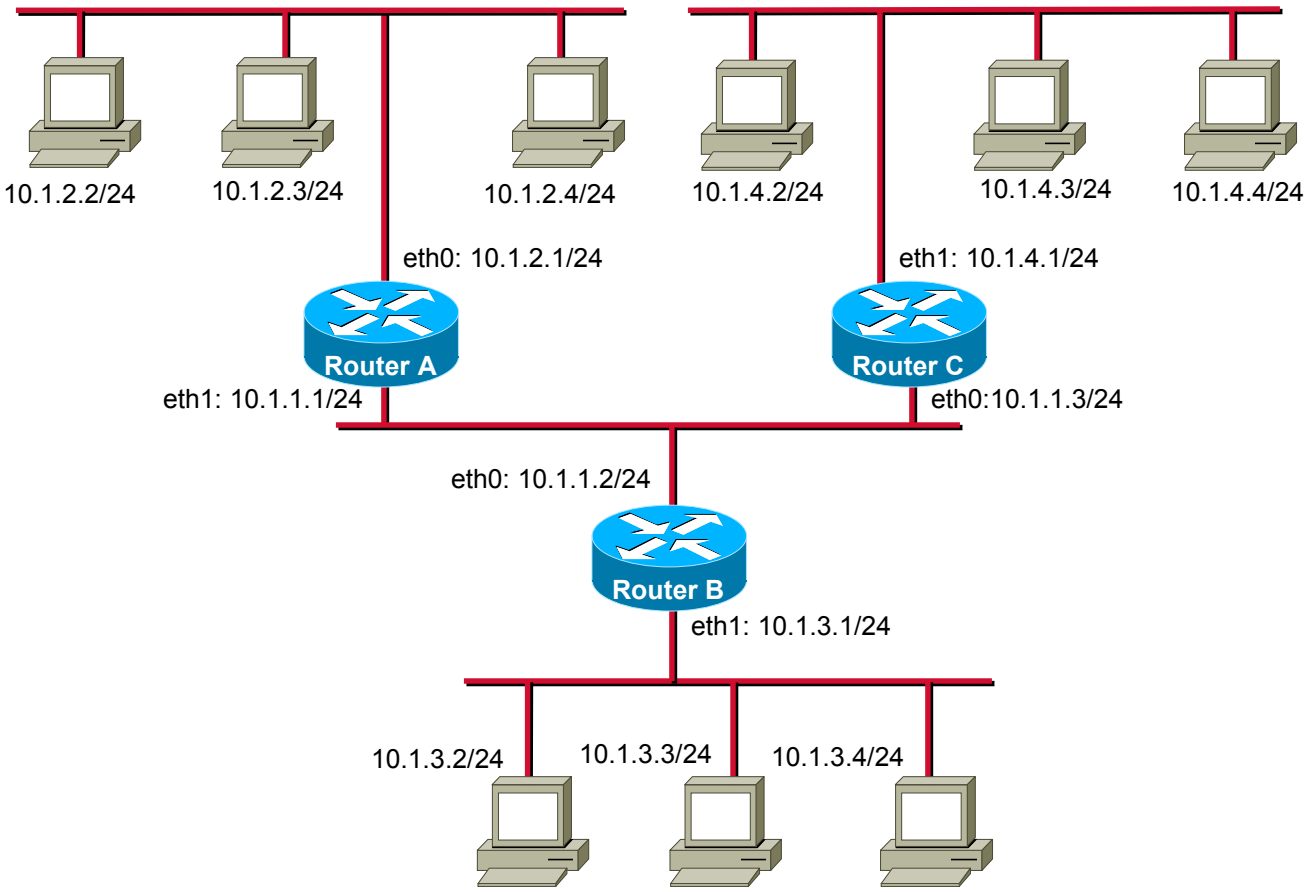


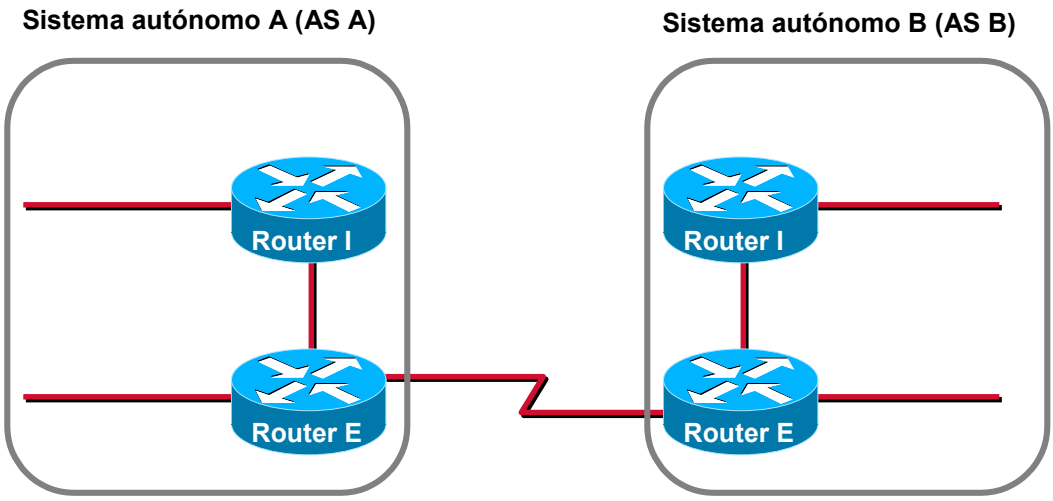
Figura 10. Enrutamiento IP

Tabla 5. Tabla de enrutamiento IP del router B

Red	Next hop	Tipo
10.1.1.0/24	10.1.1.2	Dir
10.1.2.0/24	10.1.1.1	Gw
10.1.3.0/24	10.1.3.1	Dir
10.1.4.0/24	10.1.1.3	Gw

Los enrutadores utilizados para intercambio de información dentro de un sistema autónomo (AS) son llamados enrutadores interiores, y ellos usan una variedad de protocolos de gateway interior (IGP) para cumplir esta labor. Los enrutadores destinados al intercambio de información entre sistemas autónomos, son llamados routers exteriores (o routers de borde), y utilizan protocolos de gateway exterior (EGP). En la Figura 11 se muestran dos sistemas autónomos (AS A y AS B), y el modo de conexión de los routers internos y externos. Internet está compuesto de miles de AS ordenados jerárquicamente.

El enrutamiento IP especifica que los datagramas (paquetes) IP viajan a través de la Internet de a un salto a la vez. La ruta completa no es conocida al principio del trayecto, sino que en cada parada, el próximo destino es calculado utilizando la información contenida en la tabla de rutas del nodo. La participación de cada nodo en el proceso de enrutamiento consiste sólo en el reenvío de paquetes basado en información interna, independiente de que los paquetes llegan a su destino final.



Router I: Router interior
Router E: Router exterior

Figura 11. Routers interiores y exteriores.

2.5.2.1 Protocolos de enrutamiento

Los protocolos de enrutamiento IP son dinámicos, esto significa que las rutas son calculadas a intervalos regulares de tiempo por un software especializado en los dispositivos de enrutamiento.

Dentro de los protocolos de ruteo interno se tiene:

- RIP: Protocolo de domino público, basado en el análisis de un vector de distancias, la última versión del protocolo se conoce como RIP-2 [RFC 2453].
- OSPF: Protocolo de dominio público, basado en el análisis de estados de los enlaces, la última versión del protocolo se conoce como OSPF versión 2 [RFC 2328].
- IGRP: Protocolo propietario de CISCO Systems Inc. [Cisco IGRP].
- EIGRP: Protocolo propietario de CISCO Systems Inc. [Cisco EIGRP].

Dentro de los protocolos de ruteo externo se tiene:

- BGP-4: Protocolo de dominio público, basado en el análisis de caminos, un derivado de vectores de distancias [RFC 1771].

2.5.2.2 Enrutamiento libre de clases

El enrutamiento libre de clases (CIDR) [RFC 1519] es una manera de prevenir la explosión en el crecimiento de las tablas de enrutamiento en Internet. El concepto básico de CIDR es la capacidad de resumir las entradas en la tabla de enrutamiento, de modo que una entrada represente a varias redes. Esto se consigue mediante la asignación de direcciones IP consecutivas.

Previo al desarrollo de CIDR se tenía que dada una red clase A, B o C, la máscara de red estaba implícita a la clase. En CIDR, todas las redes se manejan con una máscara explícita para poder dividirlas en red/host y de este modo olvidar el concepto de clase. De este modo se puede agrupar varias redes clase C contiguas, con una máscara común, extendiendo los bits de host hacia los de red, implementando lo que se conoce como superred. Por ejemplo las clases C 200.0.0.0, 200.0.1.0, 200.0.2.0 y 200.0.3.0 pueden agruparse en una superred 200.0.0.0 con máscara 255.255.252.0. Esto se puede denotar como 200.0.0.0/22.

Los requerimientos para resumir las redes son:

- Las múltiples direcciones IP a ser resumidas para el enrutamiento deben ser contiguas y compartir los mismos bits más significativos.
- Las tablas de enrutamiento y algoritmos deben ser extendidos para basar sus decisiones de enrutamiento en direcciones IP de 32 bits, y máscaras de red de 32 bits.
- Los protocolos de enrutamiento usados deben ser extendidos para llevar la máscara de 32 bits, además de la dirección de 32 bits. OSPF, RIP-2 y BGP-4 soportan CIDR.

2.5.3 Servicios Internet

La Internet ofrece una gran variedad de servicios para sus usuarios. Dentro de los servicios de mayor importancia se encuentran:

- Servicio de resolución de nombres.
- Servicio de correo electrónico.
- Servicio de noticias USENET.
- Servicio WWW.
- Servicio FTP.
- Servicio PROXY-CACHE.
- Servicio de IRC.
- Servicio de juegos.

2.5.3.1 Servicio de resolución de nombres

En general, las aplicaciones orientadas a los servicios de las redes no hacen referencia a las direcciones binarias (o decimales) de las máquinas que componen la red. En lugar de esto, los programas utilizan cadenas de caracteres ASCII (o nombres) tales como raparede@dcc.uchile.cl. Sin embargo, la red sólo maneja direcciones binarias, por lo que se necesita algún mecanismo que convierta los nombres en direcciones de red.

Inicialmente, en cada máquina de la red se escribía un archivo `hosts` en donde se listaban todos los hosts con sus direcciones IP. Pero a medida que la red aumentaba su tamaño, esta solución se hacía inviable. Para resolver este problema se diseñó el servicio de resolución de nombres (DNS) [RFC 1034] y [RFC 1035].

El DNS está constituido por una base de datos jerárquica y distribuida que es usada por las aplicaciones TCP/IP para establecer la asociación entre los nombres de hosts y sus direcciones IP. Se dice que es distribuida, puesto que no existen nodos que posean la información de nombres de toda la red, sino que existe un sistema cooperativo entre los servidores. El protocolo DNS permite a los clientes y servidores comunicarse entre ellos y de este modo compartir la información.

Para utilizar el DNS la aplicación invoca a un resolutor de direcciones y le entrega como parámetro el nombre del host. El resolutor a su vez envía la consulta al DNS local, el cual le retorna la dirección IP del host. Por último el resolutor retorna la dirección IP solicitada a la aplicación llamadora. El proceso para obtener un nombre dado una dirección IP es análogo. Note que el resolutor es parte de la aplicación, no del protocolo TCP/IP, y en varios lenguajes se tienen funciones de biblioteca que se encargan de esta labor (por ejemplo `gethostbyname` y `gethostbyaddr`).

El DNS organiza los nombres de los nodos en una jerarquía de dominios. Un dominio es una colección de nodos relacionados de alguna manera, como estar en la misma red o pertenecer a una misma organización o país.

El dominio raíz de la jerarquía se indica con un punto y agrupa al resto de los dominios. Para indicar que un nodo se expresa en notación de nombre de dominio completamente calificado (FQND), es decir, que incluye al dominio raíz, se debe terminar el nombre en un punto.

Dependiendo de su localización en la jerarquía, un dominio puede ser de primer, segundo o tercer nivel. Pueden existir otros niveles pero no son frecuentes. Los dominios de primer nivel están divididos en tres áreas:

- Arpa es un dominio especial usado para asociar direcciones IP a nombres, con esto se consigue realizar la resolución de nombres reversa (dado un número IP, a qué nombre de host corresponde).
- Los dominios genéricos. Estos dominios se muestran en la Tabla 6.
- Los dominios geográficos o de país. Esto son todos los dominios de dos caracteres que están basados en los códigos de países definidos por ISO 3166.

Tabla 6. Dominios genéricos

Dominio	Descripción
edu	Aquí se incluyen casi todas las universidades o centros de investigación norteamericanos.
com	Compañías u organizaciones con fines comerciales.
org	Organizaciones no comerciales. Las redes UUCP privadas se encuentran aquí.
net	Administrativos de red.
mil	Uso militar EEUU.
gov	Nodos del gobierno norteamericano.
int	Organizaciones internacionales.
uucp	Oficialmente, todos los nombres de nodos UUCP sin dominio han sido movidos a este nuevo dominio.

En las primeras redes se utilizó un programa llamado UUCP que permitía conducir tráfico de un nodo Unix a otro, de hay el nombre Unix to Unix Copy.

2.5.3.2 Servicio de correo electrónico

El correo electrónico es una de las aplicaciones de mayor uso. Permite enviar mensajes de un usuario a otro en la red, con la posibilidad de adjuntar archivos, lo que transforma el servicio en “encomiendas electrónicas”, aumentando enormemente sus potencialidades.

El mecanismo de envío de mensajes se ve en la Figura 12. El objetivo del Protocolo de Oficina Postal (POP3) y del Protocolo Simple de Transferencia de Correo (SMTP) es transferir los correos de modo confiable y eficiente. SMTP y POP3 son independientes del subsistema de transmisión en particular y requieren sólo de un flujo de datos ordenado y confiable (TCP).

El intercambio de correo entre distintos sitios es realizado por los Agentes de Transferencia de Mensajes (MTA) mediante SMTP. La aplicación agente de usuario establece una sesión SMTP/TCP con la MTA local para enviar los mensajes. Si la MTA no está disponible, los mensajes salientes son almacenados en la cola de correo saliente, para enviarlos posteriormente. Cuando la MTA recibe un correo para un usuario local, lo almacena en la casilla de mensajes entrantes para su posterior despacho. Por último el agente de usuario establece una sesión POP3/TCP con la MTA local para extraer los mensajes recibidos, dirigidos al usuario que fue autentificado en la sesión POP3.

En [RFC 822] se especifica el formato del correo electrónico, en [RFC 821] se especifica SMTP, y en [RFC 1725] se especifica POP3.

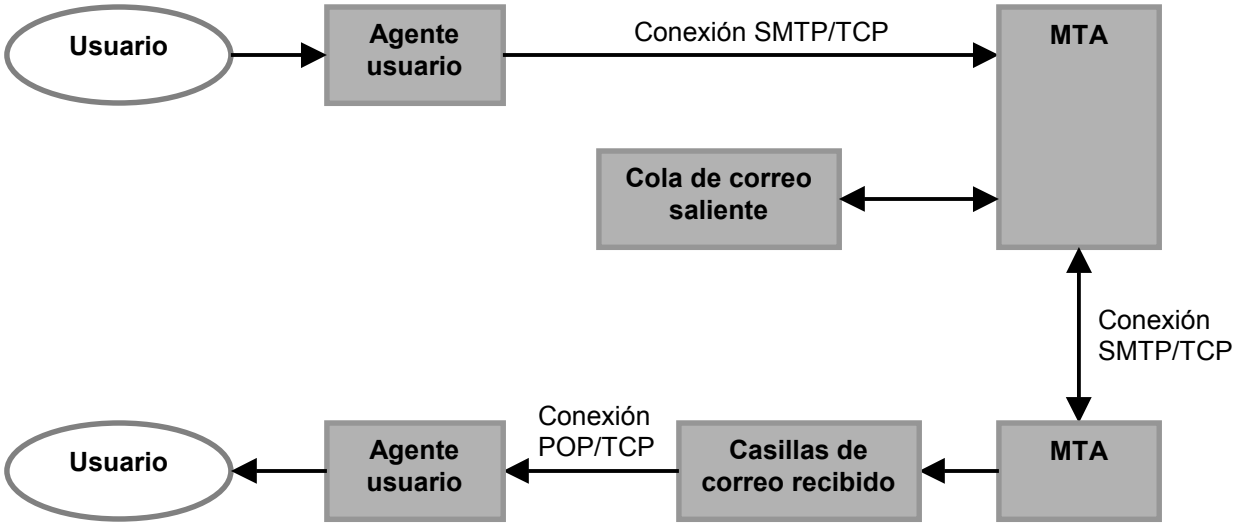


Figura 12. Esquema del correo electrónico Internet

2.5.3.3 Servicio de noticias USENET

USENET es un medio para que los usuarios de Internet se comuniquen informalmente acerca de un enorme rango de temas.

USENET es un sistema de discusión distribuido mundial. Se puede ver como una colección de noticias sobre varios temas que son publicados en servidores a lo ancho de la red bajo un esquema jerárquico. Los artículos son agrupados en lo que se conoce como newsgroup (grupo de noticias). Existen miles de grupos de noticias y es posible para los usuarios crear grupos nuevos. La mayor parte de los grupos de noticias están residentes en servidores conectados a Internet, pero hay algunos que residen en servidores que no son parte de la Internet. El protocolo original de USENET fue UUCP, actualmente se utiliza el protocolo NNTP [RFC 977].

Browsers como Netscape Navegator o Internet Explorer proveen soporte para USENET y pueden acceder a cualquier grupo de noticias que se escoja.

2.5.3.4 Servicio WWW

World Wide Web (WWW) comenzó en 1989 en el Centro Europeo de Investigación Nuclear (CERN). Su intención original era poder difundir de una manera uniforme y simple contenidos a través de la red, de modo que los científicos pudieran compartir su información. Para esto se creo un mecanismo de Localización Uniforme de Recursos (URL). Al cabo de cinco años, se transformó en la aplicación más popular de red.

Para acceder a los servicios web es necesario disponer de un browser, que es una aplicación que permite visualizar documentos escritos según el formato HTML, que es un “lenguaje de programación” ideado para la publicación de páginas web. Para obtener los archivos se emplea el protocolo HTTP.

Los documentos HTML pueden contener información en múltiples medios. En efecto, soporta la transmisión de texto plano, imágenes, sonidos, animaciones, etc. También permite dejar enlaces (links) a otros archivos HTML o de otro tipo soportado de modo transparente para el usuario. Esto flexibiliza y expande enormemente las capacidades del servicio.

Los browsers también pueden acceder a información mediante otros protocolos, por ejemplo: recuperar archivos con FTP, noticias con NNTP, etc.

2.5.3.5 Servicio FTP

FTP es un protocolo estándar de Internet. FTP es un mecanismo simple para intercambiar archivos entre computadores dentro de la red. Dentro de los usos del FTP está el transporte de páginas HTML desde el computador de desarrollo, hacia el servidor web. También es comúnmente usado para descargar programas desde los servidores FTP en Internet.

Como usuario, se pueden utilizar clientes FTP desde la línea de comando o con interfaces gráficas. El servicio permite agregar, sacar, borrar, renombrar, mover y copiar archivos en el servidor. Para ingresar al sitio, el servidor a menudo solicita la autentificación del usuario, a menos que se ingrese a sitios públicos como un usuario anónimo.

En [RFC 0959] se define el servicio.

2.5.3.6 Servicio PROXY-CACHE

El servicio PROXY-CACHE es un servicio de gateway de aplicación que utilizan algunos browsers para acceder indirectamente a otros servidores web o FTP. Cuando un cliente PROXY solicita una página web o archivo vía FTP, el servidor PROXY actúa de intermediario y solicita la página o archivo al destino final, y se la reenvía al cliente.

El servidor mantiene una copia local (y temporal) en su memoria principal y/o secundaria de todas las páginas y archivos que han solicitado. Luego frente a solicitudes repetidas de páginas o archivos, el servidor PROXY envía la que tiene en memoria principal o secundaria. De este modo se puede mejorar los tiempos de respuesta en situaciones donde existe un enlace lento para acceder a los destinos fuera de la red, frente a enlaces locales rápidos.

2.5.3.7 Servicio de IRC

Internet Relay Chat (IRC) es un sistema de conversación en línea (en tiempo real) que involucra por un lado una serie de reglas y convenciones y por otro software cliente/servidor. En Internet existe una gran variedad de aplicaciones clientes (mIRC para Windows, IRCle para Mac OS e irc2 para sistemas UNIX, irc2 fue el primer cliente diseñado para IRC) y sitios servidores de IRC (IRCnet en Europa, EFnet en norteamérica).

Para iniciar una conversación en IRC se necesita conectarse al servidor IRC, y luego el usuario se debe integrar a alguno de los canales disponibles.

Para transportar los datos IRC utiliza TCP. En general el puerto utilizado para el servidor es el 6667. Se puede utilizar IRC a través de un cliente Telnet.

2.5.3.8 Servicio de juegos

Con las mejoras en las capacidades de los computadores, y el aumento de la velocidad de las conexiones conmutadas, se han hecho populares servidores de juegos en Internet.

Este servicio permite realizar juegos competitivos, cooperativos, etc., entre jugadores de la red. En algún nodo (el servidor) se recibe y procesa la información que envía cada cliente (jugador), y luego de procesar la información, el servidor responde a los clientes sobre el nuevo estado del jugador.

Dentro de los tipos de juegos que se han hecho populares en Internet se tienen los juegos de estrategia, los juegos basados en entornos tridimensionales, u otros. Dentro de los juegos típicos están Quake, en alguno de sus sabores, servidores de juegos de Blizard, etc.

2.6 Sistema Operativo Linux

Unix, en cualquiera de sus sabores, es uno de los sistemas operativos de mayor popularidad, en segundo lugar después de los sistemas operativos de Microsoft (Windows 98/NT u otros), debido a su masiva distribución y amplio soporte básico. Fue originalmente desarrollado como un sistema multitareas para computadores de mediana y gran capacidad a mediados de los años 70.

Linux es un clon de dominio público del sistema operativo Unix, diseñado inicialmente para computadores personales. Entre las características de Linux se tiene soporte para multitareas, el sistema X Windows (un entorno de trabajo gráfico), soporte para redes TCP/IP entre otras [Welsh et al 1999].

En términos técnicos, Linux sólo es el kernel (núcleo) del sistema operativo, ofreciendo los servicios básicos de administración de procesos, memoria virtual, administración de archivos y dispositivos de entrada/salida. En otras palabras, Linux es el nivel más bajo del sistema operativo, es decir, el nivel que interactúa con el hardware de la máquina.

Sin embargo, el término “Linux” se utiliza para referirse al sistema completo, es decir, el kernel junto a las aplicaciones que corren sobre él: ambientes de trabajo y desarrollo, editores, interfaces gráficas, procesadores de textos, juegos, etc.

Linus Torvalds creo el kernel original de linux [Welsh et al 1999], inspirado en el sistema operativo Minix (creado por Andrew S. Tanenbaum para fines académicos). Posteriormente su trabajo fue complementado por un sinnúmero de voluntarios, principalmente usuarios de Internet, quienes intercambiaron código, reportaron errores y corrigieron problemas en un ambiente abierto.

2.6.1 Características del Sistema

El soporte de redes es una de las mayores fortalezas de Linux en términos de funcionalidad y desempeño. Linux soporta una gran variedad de aplicaciones de red, tales como NFS o NIS. Además soporta el paquete de aplicaciones Samba (www.samba.org), que permite que una máquina Linux actúe como servidor de archivos e impresión para Windows. Linux provee una completa implementación de TCP/IP, incluyendo drivers (administradores) para una gran cantidad de las tarjetas Ethernet, y soporte para los protocolos PPP, SLIP, PLIP. Ofrece un completo rango de servicios e implementaciones de servidores y clientes TCP/IP: FTP, Telnet, NNTP y SMTP. Por otro lado, Linux implementa un firewall, lo que permite configurar la máquina como firewall de una red, y también permite realizar enrutamiento estático y dinámico de paquetes.

Desde el punto de vista de tecnologías multimediales, Linux ofrece compatibilidad con una gran variedad de hardware, incluyendo tarjetas de audio y video actuales. Se han portado una gran variedad de ambientes de programación, incluyendo las herramientas MESA 3D, la implementación gratuita de OpenGL, un estándar de gráficas por computadoras propuesto por Silicon Graphics (www.opengl.org).

Linux ofrece soporte para multitareas, multiusuarios y multiprocesadores. Con la capacidad de soportar hasta 16 procesadores permite un alto nivel de desempeño para aplicaciones tipo servidor y científicas.

Linux puede coexistir en un computador que posea otros sistemas operativos instalados, tales como Windows 95/98/NT, OS/2, u otras versiones de Unix. El cargador del sistema operativo de Linux, LILO, permite al usuario seleccionar con que sistema operativo iniciar la máquina al momento de arrancar el computador, y es compatible con otros cargadores de sistemas operativos (por ejemplo el de Windows NT).

Linux puede correr en un amplio rango de arquitecturas de procesadores, incluyendo Intel x86, AMD Kx, SPARC, Alpha, PowerPC, MIPS y m68k. Se está trabajando para otras arquitecturas, por ejemplo la próxima generación de procesadores Intel “Merced”, y para sistemas con procesadores embebidos tales como las Palm.

Para el almacenamiento de datos, también posee una gran cantidad de sistemas de archivos. El sistema de archivos ext2fs fue diseñado específicamente para Linux. También se soporta Minix-1 y Xenix. Los sistemas de archivos de MS-DOS y Windows 95/98 (FAT16 y FAT32) también fueron implementados con compatibilidad completa, de modo que permite el acceso a unidades de disco duro y portátil de los sistemas operativos MS-DOS y Windows tanto para lectura como para escritura. También tiene soporte para los sistemas de archivos de OS/2, Apple, Amiga, y Windows NT (aunque en algunos casos sólo para lectura). Además soporta el estándar de CD-ROM ISO 9660 [Welsh et al 1999].

El núcleo de Linux es conocido como kernel monolítico, es decir que todos los administradores de dispositivos son parte del núcleo propiamente tal. Algunos sistemas operativos emplean microkernels, en donde los drivers de los dispositivos no son parte del núcleo (tales como el sistema de archivos, etc.) sino que son tratados como una aplicación cualquiera, por ejemplo Microsoft MSDOS. Linux también soporta la carga de módulos administradores en demanda. Hay ventajas y desventajas en ambos diseños: la arquitectura monolítica es común en muchas implementaciones de Unix y es la técnica aplicada en la mayoría de los diseños de kernel clásicos, y permite la habilitación en tiempo de arranque de los dispositivos del sistema. Por su parte, la técnica modular permite la habilitación de dispositivos en demanda sin tener que recompilar el núcleo nuevamente.

Un recurso escaso en los sistemas computacionales es la memoria principal del sistema. Con el objetivo de aumentar la memoria disponible del sistema, Linux implementa paginamiento de memoria, es decir, una cierta cantidad de espacio de disco habilitada como espacio de intercambio de memoria principal. Cuando el sistema requiere más memoria física, se activa el intercambio de memoria en disco, permitiendo correr grandes aplicaciones y soportando varios usuarios a la vez.

Sin embargo el espacio de disco no sustituye la memoria RAM física, puesto que el tiempo de acceso a disco es mucho mayor que el acceso a la memoria. El tiempo necesario para acceder al disco es del orden de 5 ms, en cambio el tiempo de acceso a la memoria es del orden de 10 ns (quinientas mil veces más rápido!!).

Los programas ejecutables enlazan dinámicamente las librerías de funciones, por otro lado estas librerías son compartidas por una gran variedad de aplicaciones. Esto por un lado permite que en la memoria principal se mantenga sólo una copia de la librería, y por otro que los archivos ejecutables ocupen mucho menos espacio en disco. También se permite el uso de ejecutables con enlace estático de las librerías de modo que el ejecutable posee todo el código de la aplicación en una única pieza de código.

Con respecto al tema de automatización de tareas, los sistemas Unix y Linux en particular, proveen una gran cantidad de utilitarios, incluyendo herramientas para programar tareas a ciertas horas (`crontab`), interpretes de comandos o shells y lenguajes de programación orientados a la administración que permiten una fuerte interacción con el sistema. Actualmente una de las herramientas más poderosas es el lenguaje Perl, que permite implementar una gran variedad de pequeñas herramientas que combinadas proveen grandes facilidades al administrador. Para mayor información sobre Perl se recomienda [Schwartz 1997].

2.7 Descripción de un ISP

2.7.1 Generalidades

Un Proveedor de Servicios Internet es una compañía que permite el acceso de otras compañías o individuos a la Internet, ofreciendo servicios Internet y conectividad. Dentro de los servicios que entrega figuran el correo electrónico (e-mail), construcción de sitios Web y su mantención (Web Hosting), servicios de resolución de nombres (DNS), servicios de noticias USENET, servicios de transferencia de archivos (FTP) entre otros.

Un ISP tiene el equipamiento y las líneas de acceso de telecomunicaciones necesarias para constituir un punto de presencia en Internet y así poder prestar servicios en un área geográfica dada. Los grandes ISP poseen enlaces de comunicaciones propios lo que los hacen menos dependientes de otros proveedores de telecomunicaciones, permitiéndoles de esta manera brindar mejores servicios a sus clientes.

Una clase especial de ISP son los proveedores de servicios Internet virtuales (VISP). Un VISP sólo provee los servicios Internet (web, e-mail, etc.) y no provee servicios de conectividad, puesto que los servidores de acceso para los clientes y la conexión a Internet son arrendados a otros ISP. Los servicios se implementan en la granja de servidores del sitio. La granja de servidores es el conjunto de máquinas que implementan los servicios.

Siguiendo el esquema inicial de los ISP, se pueden considerar las siguientes visiones:

2.7.2 Visión del Cliente

Para los clientes, un ISP tiene básicamente dos funcionalidades:

- Ofrece conectividad a la Internet: El ISP les abre la puerta a la nube Internet, de manera de poder utilizar todos los servicios que ofrece la red.
- Servicios de Internet: Una vez que la conexión se ha establecido, el ISP debe garantizar al cliente la disponibilidad de sus servicios. Se hace un especial hincapié a dos servicios que son masivamente empleados por los usuarios, estos son correo electrónico y WWW. Un tercer servicio de uso masivo es el de transferencia de archivos.

Esto se puede apreciar en la Figura 13.

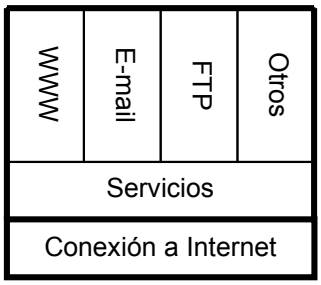


Figura 13. Visión del Cliente de un ISP

Los clientes de un ISP se pueden conectar desde su hogar, oficina, o lugares de acceso público. Para esto deben de disponer del software necesario. Windows 98/NT, Mac OS y Linux, entre otros, incluyen un conjunto de aplicaciones necesarias para establecer la conexión. Esto incluye el stack de protocolos TCP/IP. También se dispone de sitios web de donde pueden bajar aplicaciones libres de pago.

Los softwares de conexión, en combinación con los navegadores web Microsoft Internet Explorer o Netscape Communicator permiten a los usuarios el acceso a Internet, y a sus servicios. Ambos navegadores implementan HTML (web), NNTP (noticias), FTP (transferencia de archivos) y SMTP/POP3 (correo). Con esto, los usuarios están conectados a Internet, y pueden obtener otras aplicaciones o utilitarios desde la red.

Para facilitar el proceso de la primera conexión, algunos ISPs distribuyen un CD-ROM con software de licencia pública. Estos discos pueden ser usados como una excelente herramienta de marketing, entregando las aplicaciones preconfiguradas según los intereses del ISP.

2.7.3 Visión del Proveedor

La visión del proveedor es mucho más compleja, pues es él quien se encarga de entregar la conectividad a sus clientes. Obviamente, un ISP pequeño puede ser cliente de otro ISP mayor, delegando parte del problema de la conexión a Internet en el ISP mayor.

En términos conceptuales, no existe una gran disparidad entre un ISP y cualquier computador que esté en Internet. La única funcionalidad que marca la diferencia, es que el ISP es capaz de permitir la conexión de otros computadores a través de él, misión que podría asumir cualquier ordenador que posea conexión a Internet. Esta “capacidad especial” se debe a que el “computador ISP”, posee los permisos necesarios para interactuar con otros elementos de la red, tales como modems, routers o switches, que son los dispositivos que permiten el acceso a los clientes.

Por otro lado, el ISP ofrece servicios Internet, que son implementados en la granja de servidores, los que forman la red interna del ISP.

Para facilitar el análisis, el problema se subdivide en varios aspectos:

- Diseño de la red interna del ISP.
- Canal de conexión hacia la Internet.
- Canales de acceso hacia sus clientes.
- Planificación de los servicios prestados.
- Mecanismos de seguridad.

En lo medular todo ISP debe velar por dos objetivos, estos son:

1º Debe conservar alta disponibilidad de conectividad con la Internet y sus clientes.
2º Debe mantener alta disponibilidad en la prestación de los servicios básicos de un ISP.

Todas las otras prestaciones que el cliente desee pueden obtenerse una vez dentro de Internet utilizando los recursos que ya existen, por ejemplo para correo Hot Mail, para buscadores en Altavista, sitios de Web Hosting gratuitos, etc.

Siguiendo este desarrollo un ISP básico sólo necesita contar con tres elementos:

- Canal de acceso Cliente – ISP.
- Canal de acceso ISP – Internet.
- Servicios básicos (resolución de nombres).

En este caso, se tiene un ISP que sólo sirve de intermediario entre el cliente y la Internet.

Adicionalmente es sumamente importante implementar mecanismos de seguridad en el sitio, de modo de protegerlo frente a la gran variedad de ataques que disponen los hackers.

Para el caso en que se quieran mayores prestaciones o entregar una mejor calidad de servicio, entra en juego el diseño de la red interna del ISP y la planificación de los servicios que se ofrecerán a los usuarios. Para un análisis riguroso de esta situación, se deben considerar parámetros tales como:

- Cuál es el número de clientes conmutados y dedicados.
- Cuál es el ancho de banda asignado a los clientes.
- Cuáles servicios se prestarán en forma local desde la red interna, y cuáles desde Internet.
- Cuál es la estimación absoluta y porcentual de tráfico local y externo.
- Qué nivel de tolerancia a fallas se desea para el Sitio.
- Qué tiempo promedio, y mínimo entre fallos se espera.
- Qué especificación se quiere para el tiempo de recuperación de fallos.
- Qué alternativas de redundancia se utilizarán, etc.

Otro aspecto importante de considerar es qué parte del tráfico que sale de un ISP va dirigido a otros ISP locales, en caso chileno, otros ISP nacionales, con lo que divide el tráfico en nacional e internacional. De este modo se podría disminuir notablemente el tráfico hacia la Internet global (que corresponde al tráfico internacional), si existen conexiones interiores con los otros ISP de la región. En efecto, el tiempo de ida y vuelta a un sitio nacional es de aproximadamente de 115 ms, en cambio el tiempo de ida y vuelta a un sitio en Estados Unidos es de 1400 ms.

Para el diseño de la red interna del ISP conviene utilizar un modelo jerárquico de capas, de manera de poder dividir funcionalmente el problema. Este modelo consigue definir claramente la misión de los elementos de la red, con lo que se consigue administrar la red como una colección de unidades operativas independientes, replicables, y escalables. Por otra parte, un modelo jerárquico permite al administrador detectar, aislar y corregir las fallas con mayor facilidad.

Para la planificación de servicios se debe considerar desde la población objetivo, es decir, los requerimientos planteados por los clientes, hasta el nivel de servicios que ofrece la competencia. Es importante destacar que en el corazón de los servicios se encuentra el de resolución de nombres (DNS), pues permite la traducción de nombres a direcciones IP y la traducción reversa, funcionalidad vital en el ambiente Internet y es un servicio que no puede faltar en un ISP.

Una descripción más completa sobre los ISPs se encuentra en el Anexo I. “¿Qué es un ISP?”.

Capítulo 3: Metodología

En este capítulo se mostrarán los aspectos metodológicos considerados en la realización del trabajo:

- Hipótesis de trabajo: Define el estado inicial y el alcance del trabajo realizado en la memoria desde el punto de vista docente.
- Diseño de las guías del laboratorio: Muestra la estructura empleada en la confección de las guías del laboratorio.
- Metodología de construcción del ISP mínimo: Define el modelo considerado para la implementación del ISP de pruebas y la secuencia de tareas necesarias para poner en marcha el ISP mínimo.
- Planificación de las experiencias: Una vez determinado el mecanismo de construcción del ISP mínimo, se divide el trabajo en porciones de acuerdo a lo especificado en la Tabla 7 (página 40), las que serán cubiertas por cada una de las experiencias del laboratorio.

3.1 Hipótesis de Trabajo

A continuación se mostrarán los requisitos mínimos que necesitan satisfacer los alumnos que realizarán las experiencias del laboratorio de ISP. Además se mostrará cual es la infraestructura necesaria para la realización de los experimentos tanto en lo que se refiere al software como al hardware.

3.1.1 Perfil de los Alumnos

El laboratorio de ISP está ideado para alumnos de Ingeniería orientados al área de redes de computadores o para profesionales con una mediana preparación técnica y teórica en el tema de Internetworking. En particular, se dirige el trabajo a los alumnos de Ingeniería Civil Electricista o de Ingeniería Civil en Computación de la Universidad de Chile, quienes de acuerdo a su malla curricular, poseen los conocimientos y habilidades necesarias para el desarrollo del laboratorio. Es importante destacar que un requisito fundamental para los alumnos es que estén altamente motivados con el tema.

Para un mejor entendimiento y aprovechamiento de los contenidos abordados en las actividades del laboratorio, es necesario que los alumnos posean conocimientos básicos en tecnologías de redes TCP/IP. Por lo cual es altamente recomendable para los candidatos al laboratorio que realicen algún estudio formal o informal sobre redes TCP/IP previo a la realización de los laboratorios.

Para el caso de los alumnos del DIE, se sugiere como requisito previo o simultáneo al laboratorio el curso “Redes de Computadores” (EL64E) y para los alumnos del DCC, se sugiere como requisito previo o simultáneo el curso “Comunicación de Datos” (CC51C), ya que en ambos cursos se muestra la base de conocimientos necesaria para el laboratorio, vale decir el stack de protocolo TCP/IP, y los servicios en Internet.

3.1.2 Infraestructura Necesaria

Para la realización del laboratorio es necesario contar con un conjunto de computadores conectados entre sí formando una pequeña red TCP/IP (con ethernet en la capa 2). El tema de Internetworking propiamente tal no es objetivo del trabajo, por lo que no se ahondará el análisis en tópicos de equipamiento de redes, sino que el foco del trabajo apunta a los servicios que puede suministrar la red.

El esquema del hardware del laboratorio se ve en la Figura 14. Como se aprecia en la figura, desde el punto de vista del hardware de redes el equipamiento es bastante sencillo. Consiste en dos pequeñas

redes, conectadas entre sí por un computador que tiene dos interfaces ethernet mirando a cada una de las dos redes, una tercera interfaz mirando hacia Internet y un modem conectado a la red telefónica conmutada pública (PSTN). Se utilizan dos hubs para implementar las redes ethernet. Para realizar las pruebas de acceso conmutado, se necesita otro computador con modem para poder conectarlo con el computador central, a través de una línea telefónica.

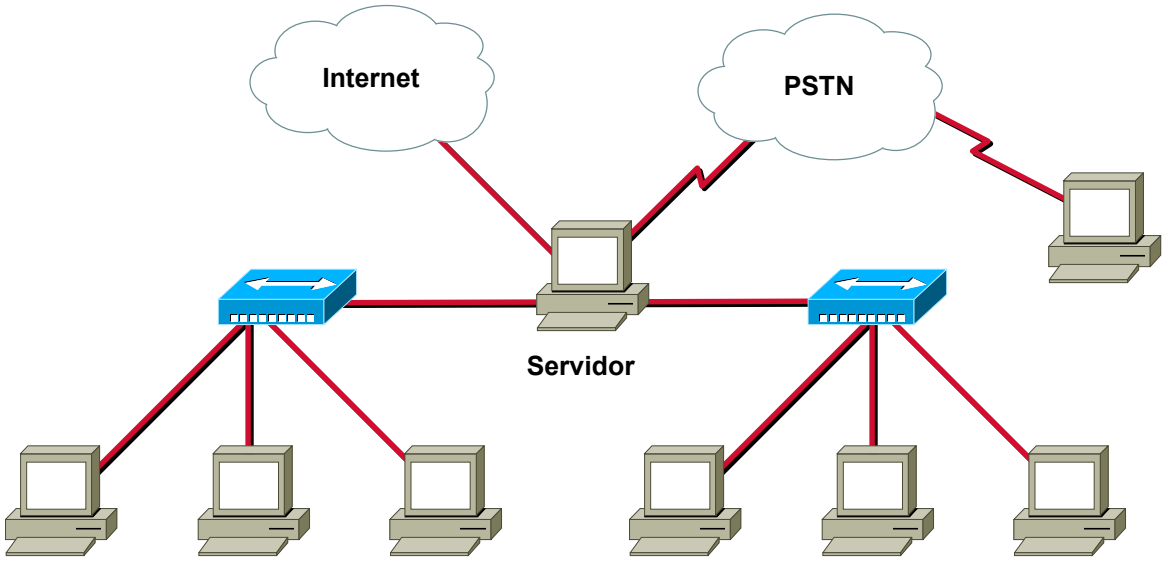


Figura 14. Esquema del laboratorio de ISP

Este esquema puede ser reducido al mostrado en la Figura 15, pero es mucho menos pedagógico. En él se observan dos computadores de similares capacidades, ambos tienen un modem e interfaces ethernet. Desde el punto de vista del hardware no hay diferencia entre los equipos. Desde el punto de vista conceptual sólo el servidor tiene acceso directo a la Internet, y para las pruebas el cliente puede acceder a través del enlace conmutado o del dedicado.

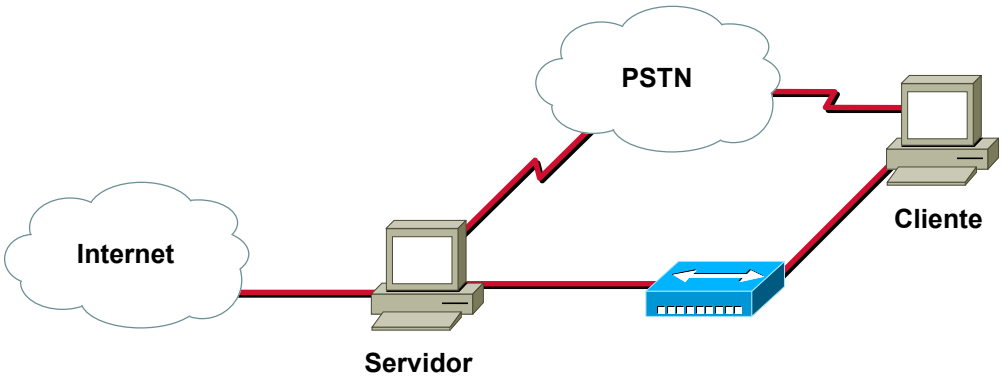


Figura 15. Configuración mínima para el laboratorio

Tanto para los computadores clientes como para los servidores no se exigen grandes requerimientos, pero se recomienda la siguiente configuración mínima:

- Procesador Intel Pentium.
- 32 MB memoria RAM.
- 4 GB disco duro.
- 2 Tarjetas de red 10BaseT.
- Modem externo de 33.6 Kbps.
- Lector de CD-ROM 12x ATAPI IDE.
- Monitor de 14 ‘’.

Claramente con computadores de mayores capacidades se mejoran las condiciones de realización de los laboratorios. En especial se recomienda aumentar la cantidad de memoria de los computadores a 64 MB de RAM o superior y utilizar procesadores Intel Pentium II o AMD K6-2, de modo de mejorar el desempeño de los equipos al realizar las compilaciones de códigos en algunos procesos de instalación de software.

En el Anexo G. Recomendaciones Generales, se indican las consideraciones básicas para el desarrollo de las experiencias. Las recomendaciones apuntan al ámbito experimental, tanto para la manipulación de los equipos, como para el uso de las aplicaciones involucradas.

Por último, es necesario contar con la distribución gratuita de Linux (durante el desarrollo de la memoria se empleó Red Hat 6.2 (www.redhat.com), la que usualmente viene en un CD-ROM, para cada grupo de trabajo en el laboratorio. En general, el resto de los paquetes de software que se utilizarán en el laboratorio pueden ser obtenidos desde sitios de Internet, para esto se disponen sitios tales como www.rpmfind.com, www.redhat.com, u otros.

En términos económicos para el esquema reducido se necesita aproximadamente:

- $ 600.000 pesos para cada computador (mínimo dos computadores).
- $ 100.000 pesos para la instalación de la red.
- $ 35.000 mensuales para los costos de las líneas telefónicas (costo de dos líneas telefónicas residenciales).

3.2 Diseño de Guías del Laboratorio

Para confeccionar las guías se utilizó una estructura definida, la que ya ha sido bastante probada y mejorada en otras memorias en donde el objetivo también es preparar experiencias docentes sobre algún tema en telecomunicaciones, en particular se revisó [Hernández 2000] para construir la estructura de las experiencias.

3.2.1 Estructura de las Guías de Laboratorio

La estructura de las guías está compuesta por los siguientes puntos:

1. Título de la experiencia: Es una frase que identifica fácilmente a la experiencia y su contenido.

2. Índice: Se presenta un índice detallado de la guía de laboratorio.

3. Resumen: En el resumen se muestran cuales son los objetivos generales de la experiencia de modo de entregar al alumno una visión global y una motivación de la sesión.

4. Esquemas generales: Incluye figuras y tablas que ilustran las conexiones físicas que se desea implementar. El esquema debe ser lo más claro posible.

5. Materiales: Se entrega la lista detallada de los materiales que se requieren para desarrollar la experiencia. Incluye equipos, conectores, cables, software, etc.

6. Objetivos: Se detallan los objetivos específicos de la sesión.

7. Requisitos, conceptos y habilidades: Se le informa al alumno cuáles son los conocimientos básicos para llevar a cabo la sesión.

8. Bibliografía y referencias: Se entregan las fuentes de información utilizadas para la realización de las experiencias y otras fuentes de información adicionales para apoyar el entendimiento de los

contenidos estudiados. A los alumnos que realicen las actividades propuestas en el laboratorio, se les recomienda revisar estas referencias para adquirir los conocimientos necesarios para realizar los experimentos.

9. Plan de acción: Se muestra un resumen de las secciones y pasos a seguir. Es la agenda de trabajo de la sesión.

10. Secciones: El conjunto de secciones es el núcleo de la sesión experimental, y su objetivo es detallar las tareas mostradas en el plan de acción. Estas actividades se traducen en una serie de comandos agrupados por secciones, que se deben ejecutar uno tras otro. Esta técnica se conoce como "paso a paso". Cada bloque de comandos contiene una explicación detallada de cada paso y las funciones que cumple cada comando dentro de la configuración global.
    Para que el alumno pueda verificar si ha comprendido los pasos realizados hasta el momento, se incorporan "puntos de control" en donde se plantea un pequeño cuestionario.
    Por último, cada sección debe poseer un nombre que indique el objetivo que se desea conseguir.

11. Cuestionario Final: En este cuestionario se realiza la evaluación de la experiencia, tanto desde el punto de vista teórico como práctico.

3.2.2 Validación de las Guías de Laboratorio

Se realizaron las experiencias sólo con la información que aporta la guía. Los errores encontrados fueron corregidos, y en los casos en que no fue sencilla la corrección por de la cantidad de acciones a tomar, se documentó el mecanismo de solución de errores en el Anexo J. Resolviendo Problemas.

3.3 Metodología de Construcción de un ISP Mínimo

Dentro de los aspectos a considerar en el ISP mínimo está la red interna del ISP, que es el lugar en donde se ubican los equipos que prestarán los servicios a los usuarios. Para el diseño de la red interna se puede considerar el modelo jerárquico de redes, que es un marco de referencia que facilita el diseño de la plataforma de hardware, separando las funciones en unidades bien diferenciadas. También es importante considerar la colección de servicios que prestarán, puesto que de este modo se puede planificar las funcionalidades que ofrecerá a los usuarios.

3.3.1 Modelo Jerárquico de Redes

Este modelo permite dividir una red de computadores en módulos autónomos de funcionalidades bien diferenciadas. De este modo se puede separar el problema del diseño de la red en subproblemas de mayor facilidad de solución.

La Figura 16 muestra el Modelo Jerárquico de Redes [Cisco IDB]. Está compuesto por las siguientes capas:

- Capa de Núcleo: Provee un transporte óptimo entre los sitios.
- Capa de Distribución: Provee y administra las políticas de conexión.
- Capa de Acceso Local: Provee el acceso a usuarios y grupos de trabajo a la red.

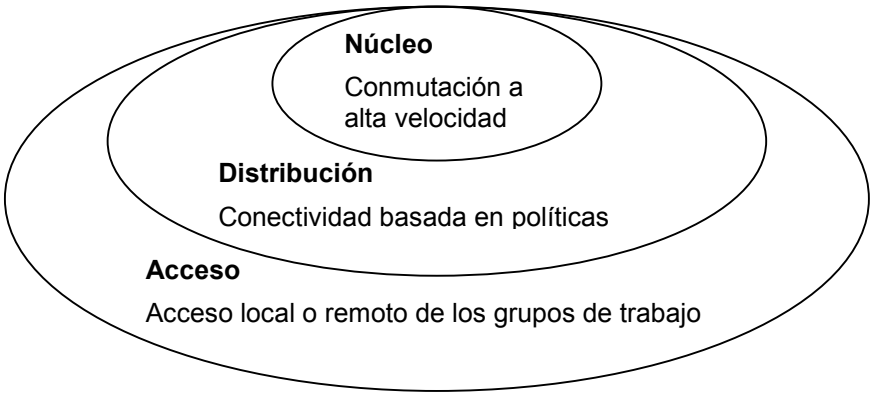


Figura 16. Modelo jerárquico de redes

Las funciones de las capas son:

- Capa de núcleo: Constituye el esqueleto de la red (el backbone), y se debe diseñar de manera que sea capaz de conmutar los paquetes a la mayor velocidad posible. Esta capa de la red no realiza ninguna manipulación sobre los paquetes (tales como listas de acceso o filtraje) pues esto disminuiría la velocidad en la conmutación de los paquetes.
- Capa de distribución: Establece la delimitación entre la capa de acceso y la de núcleo. El propósito de esta capa es proveer una definición clara de los límites de las capas y es aquí donde toma lugar la manipulación de los paquetes. En ambientes que no son del tipo campus, la capa de distribución puede constituirse como el punto de redistribución de los dominios de ruteo, o la zona de demarcación entre los protocolos de ruteo estático y dinámico. También puede ser el punto en el cual los sitios remotos pueden acceder a la red corporativa.
  Un ambiente tipo campus es uno de extensión geográfica mediana en donde se tienen varias LAN pertenecientes a diferentes departamentos de una institución, por ejemplo una facultad.
  La función de la capa de distribución se puede resumir como la capa que provee las bases de las políticas de conectividad.
- Capa de acceso: Es el punto en el cual se permite el acceso dentro de la red a los usuarios finales locales. Esta capa puede emplear listas de acceso o filtros para optimizar la atención a algún conjunto particular de usuarios. En los ambientes que no son del tipo campus, la capa de acceso puede entregar acceso a sitios remotos a la red corporativa, vía alguna tecnología de área ancha, tales como Frame Relay, ISDN, o líneas arrendadas y herramientas para la autentificación de los usuarios.

Algunas consideraciones al modelo jerárquico de redes:

A menudo se piensa erróneamente que las tres capas (núcleo, distribución y acceso) deben existir en entidades físicas claras y distinguibles, pero esto no tiene por qué ser así. Las capas son definidas para apoyar a un diseño exitoso de la red y para representar las funcionalidades que deben existir en una red. La instanciación de cada capa puede ser en distintos routers o switches, puede ser representado por algún medio físico, pueden ser combinados en un único dispositivo, o pueden ser omitidas completamente. Note, sin embargo, que para que la funcionalidad de la red sea óptima, la jerarquía debe ser mantenida.

3.3.2 Estructura de un ISP

La estructura y los servicios básicos de un ISP se muestran en la Figura 17. Observe la correspondencia entre el modelo jerárquico de redes y la estructura del ISP.

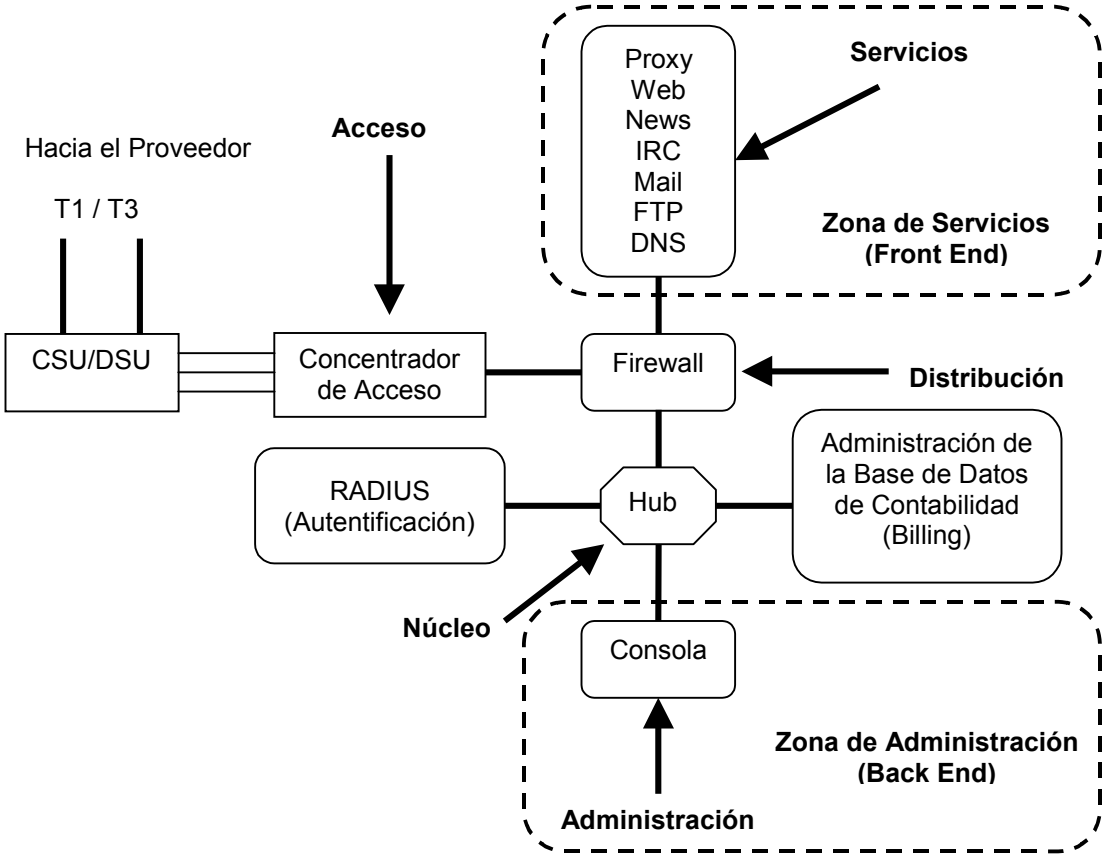


Figura 17. Estructura de un ISP mínimo

Es importante indicar que en la estructura del ISP se contemplan dos zonas importantes, una que está dedicada a los servicios, y otra dedicada a la administración. La zona dedicada a los servicios es la más frágil desde el punto de vista de la seguridad, puesto que está expuesta a todos los usuarios de la Internet que quieran acceder o utilizar un servicio determinado, en la jerga esta área se conoce como la zona desmilitarizada (DMZ). En cambio, la zona de administración debe ser la más protegida, de modo no recibir ataques de hackers.

En efecto, las estaciones que están en la zona de administración están facultadas a ingresar al resto de la plataforma ISP, de modo que si alguien puede tomar el control de las máquinas de administración, puede controlar el ISP completo.

Para los efectos del laboratorio, todas componentes mostradas en la Figura 17 serán implementados en sólo un PC, emulando la mayor cantidad de hardware de redes con aplicaciones desarrolladas para Linux. En particular en el laboratorio se implementará el proxy (en versión web caching), web, e-mail, FTP, DNS, un firewall a nivel de la capa de aplicación y mecanismos de acceso conmutado y dedicado, tal como se ve en la Figura 14 y en la Figura 15.

3.3.3 Implementación de ISP de Pruebas

Para los efectos del desarrollo de las experiencias durante el trabajo realizado en la memoria, la implementación del ISP se lleva a cabo utilizando la menor cantidad posible de equipamiento. El esquema lógico del ISP de pruebas se aprecia en Figura 18. Adicionalmente se utilizaron clientes con acceso conmutado o dedicado para realizar las pruebas de los servicios. Durante la ejecución de los laboratorios será necesario disponer tanto del computador destinado para ser el servidor como de los clientes para realizar las pruebas del servicio.

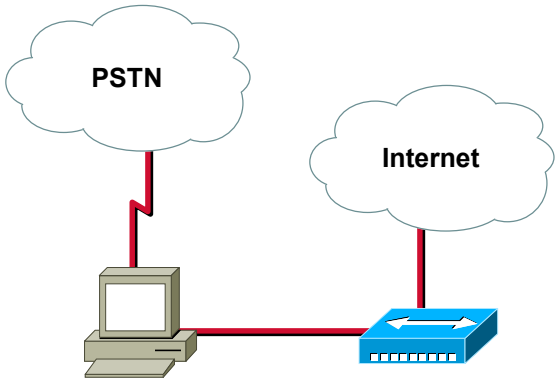


Figura 18. ISP de pruebas

Esta configuración mínima permite cumplir con una gran parte de los servicios que provee un ISP a una escala reducida.

El sistema operativo que se emplea en el ISP de pruebas es Linux. Para fines de administración de redes e implementación de servicios, Linux tiene una gran variedad de software para implementar los servicios del ISP y además posee demonios que permiten simular dispositivos de hardware, con lo cual se puede reducir notablemente la cantidad de equipos a emplear en la red.

Los servicios habilitados en el ISP de pruebas son los servicios mínimos de un ISP, vale decir DNS, Telnet, FTP, WWW, correo electrónico y web caching. Respecto a la emulación de hardware de red se implementó enrutamiento, acceso conmutado y firewall.

3.4 Planificación de las Experiencias

Una vez definido el ISP mínimo, se realizó una segmentación de las etapas de su implementación, de modo de definir los temas a abordar en cada experimento. Con esta segmentación se definen 5 grandes bloques, que constituyen las experiencias 1 a la 5.

En la experiencia 0 se muestra el ISP mínimo operando completamente, de modo de motivar al alumno y comenzar el proceso de familiarización en el tema de los ISP. Esta experiencia se ve complementada con las experiencias 1 y 2. Por último en las experiencias 3, 4 y 5 se construye paso a paso el ISP mínimo.

La planificación de las experiencias se ve en la Tabla 7. La experiencia 0 será expositiva. En ella, junto con mostrar el ISP operativo se mostrarán los casos de uso indicados.

Tabla 7. Planificación de las experiencias

	Exp. 0	**Exp. 1**	**Exp. 2**	**Exp. 3**	**Exp. 4**	**Exp. 5**
ISP operativo	**X**					
Instalación de Linux sin servicios		**X**				
Administración básica de Linux:			**X**			
Comandos útiles			**X**			
Recompilación del kernel			**X**			
Administración de usuarios			**X**			
Instalación de servicios ISP I:				**X**		
DNS	**X**			**X**		
WWW	**X**			**X**		
Telnet	**X**			**X**		
FTP	**X**			**X**		
FTP anónimo	**X**			**X**		
Servicios de conectividad:					**X**	
Modem (ppp)	**X**				**X**	
Enrutamiento	**X**				**X**	
Servicios de servicios ISP II:						**X**
Firewall	**X**					**X**
Correo electrónico	**X**					**X**
Cache engine						**X**

Los experimentos fueron diseñados considerando aspectos tales como dificultad creciente, y la secuencia necesaria para poner en marcha los servicios. Se debe considerar que existen servicios que suponen que otros ya estén operando.

Con la división propuesta se consigue poner en marcha el ISP mínimo, ya que logra habilitar los servicios básicos necesarios que debe prestar un ISP.

Respecto al tiempo que dura cada sesión experimental se espera que no supere las 3 horas.

Capítulo 4: Resultados

En el presente capítulo se muestra un resumen de las seis experiencias desarrolladas para el laboratorio docente de ISP.

En el resumen de cada experiencia se muestra:

- El objetivo general de la experiencia.
- Una breve descripción de los temas que considera la experiencia.
- Los objetivos específicos de la experiencia.
- El esquema lógico y físico de la experiencia.
- Referencias consultadas, duración estimada y la referencia al anexo que corresponde a la guía completa de la experiencia.

Para la realización de las experiencias se utilizó la principalmente la documentación en formato electrónico que se provee para Linux en los sitios metalab.unc.edu y www.hispalinux.es, desarrolladas para el Proyecto de Documentación de Linux (LDP) en inglés y español respectivamente.

Se agregan recomendaciones generales para todas las experiencias en el Anexo G. “Recomendaciones Generales”. Es importante que los alumnos consideren estas indicaciones para que puedan enfrentar mejor las actividades a desarrollar. El autor considera necesario que en la experiencia 0 junto con entregar la guía de laboratorio respectiva, se entregue una copia del Anexo G.

Para la implementación de las experiencias se utilizaron varios computadores, cuyas configuraciones se muestran en las tablas Tabla 16, Tabla 17, Tabla 18, y Tabla 19, en el Anexo H. “Configuración de los Computadores de Pruebas”.

Se anexan a la memoria en medios ópticos la distribución de Red Hat 6.2 y todo el material preparado para las experiencias.

4.1 Experiencia 0: Sitio Proveedor de Servicios Internet Mínimo

El objetivo de la primera experiencia es introducir a los alumnos la noción de lo que es un ISP. Para ello entrega una visión general de un ISP, sus funcionalidades y los requerimientos mínimos para poder realizar la implementación. Además, en esta experiencia se pretende realizar una nivelación de los conocimientos mínimos para realizar las experiencias siguientes.

A diferencia de las otras experiencias, la primera es esencialmente expositiva, y pretende entregar la motivación y los lineamientos básicos para el resto del laboratorio.

Los objetivos de la experiencia 0 son:

1. Introducir la noción de computador y sus componentes de hardware.
2. Introducir la noción de un computador de propósito general o computador cliente.
3. Introducir la noción de un computador servidor.
4. Introducir la noción de red LAN.
5. Mostrar el sistema operativo LINUX.
6. Introducir la noción de un ISP mínimo y su estructura interna.
7. Mostrar los servicios que presta un ISP mínimo a través de casos de uso típicos.

El esquema lógico de la sesión se muestra en Figura 19. En la experiencia se emplea un computador como servidor y los clientes haciéndole consultas tanto en la red del servidor, como a través de un acceso conmutado telefónico. En la Figura 20 se muestra el esquema físico. Sólo en esta oportunidad se detallarán explícitamente las conexiones en la parte posterior de los equipos. Las fotos de los computadores fueron obtenidas de [Cekit 1998]. La duración estimada de la sesión es de 2.5 horas.

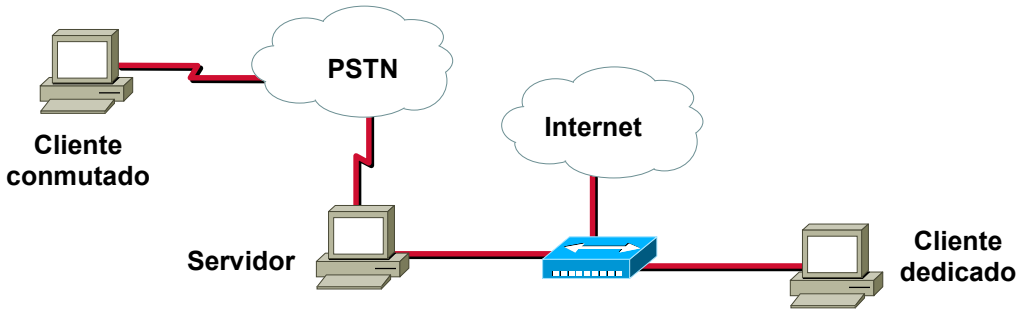


Figura 19. Esquema lógico del laboratorio 0

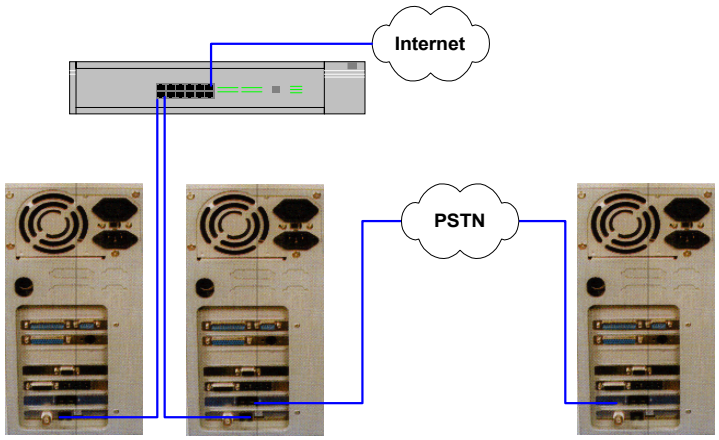


Figura 20. Esquema físico del laboratorio 0

La guía de laboratorio de esta experiencia se encuentra en el Anexo A.

4.2 Experiencia 1: Instalación de Linux

El objetivo de esta experiencia es instalar Linux sin ningún servicio habilitado.

La instalación se puede realizar a través del modo de texto o en el modo gráfico. El modo gráfico es más amigable para usuarios sin experiencia en Linux por lo que será el modo utilizado.

La selección de opciones en la instalación toma aproximadamente 50 minutos, y el proceso de copia de archivos, toma desde 25 minutos a 2 horas, dependiendo de la cantidad de paquetes a instalar y la velocidad del computador, motivo por el cual se agregará una breve clase expositiva en donde se abordarán tópicos de las próximas experiencias.

Los objetivos de la experiencia 1 son:

1. Instalar Linux sin ningún servicio habilitado.
2. Verificar el estado de la instalación.

En esta experiencia interesa mostrar el proceso de instalación de Linux. Para que los alumnos puedan compartir recursos una vez instalado Linux se considera la red mostrada en la Figura 21 y Figura 22. Desde el punto de vista del alumno, sólo considera su computador conectado a un hub, y por otra puerta del hub (aquella que acepta cross-over, que es un mecanismo para habilitar la conexión en cascada de hubs evitando utilizar cables UTP cruzados) un cable mirando hacia la Internet. La duración estimada de la sesión es de 3 horas.

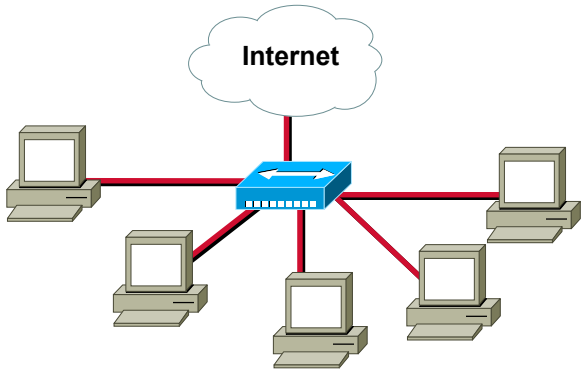


Figura 21. Esquema lógico del laboratorio 1

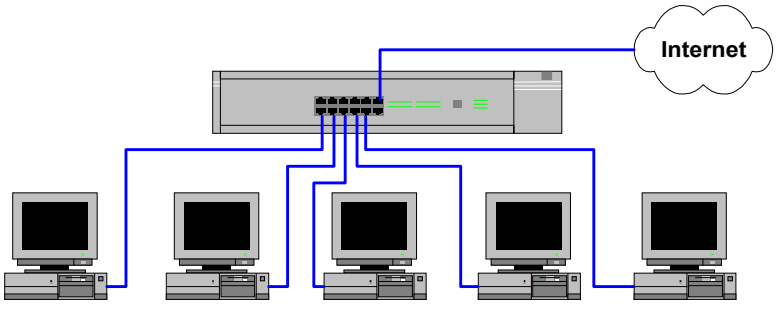


Figura 22. Esquema físico del laboratorio 1

La guía de laboratorio de esta experiencia se encuentra en el Anexo B.

4.3 Experiencia 2: Administración Básica de Linux

El objetivo de esta experiencia es que los alumnos adquieran cierta destreza en el sistema operativo Linux, esto es de vital importancia en el laboratorio, pues permitirá a los alumnos adquirir las habilidades mínimas en el uso de Linux. En ella se mostrarán:

- Algunos comandos útiles de Linux (algunos son comunes a todas las distribuciones de Linux, y otros son parte de Red Hat 6.2): `ls`, `cd`, `mkdir`, `rmdir`, `crontab`, etc.
- Mecanismos de administración de usuarios: `useradd`, `userdel`, etc.
- El proceso de recompilación del kernel.

Linux provee muchas herramientas gráficas para la administración del sistema, pero en esta sesión se utilizarán las herramientas de línea de comando ya que permiten una mejor comprensión de la situación.

Los objetivos de la experiencia 2 son:

1. Mostrar comandos básicos de Linux, en particular los asociados al sistema de archivos.
2. Mostrar comandos básicos de visualización de archivos.
3. Mostrar comandos de administración de Linux.
4. Mostrar comandos básicos de administración de redes.
5. Mostrar comandos de administración de usuarios.
6. Mostrar el proceso de recompilación del kernel.
7. Mostrar modos de ejecución de procesos en segundo plano.

El esquema de conexión es igual al de la experiencia uno. El esquema lógico de conexión se ve en la Figura 23 y el esquema físico en la Figura 24. Para preparar la sección de compilación del kernel se consultó [howto kernel]. La duración estimada de la sesión es de 4.5 horas.

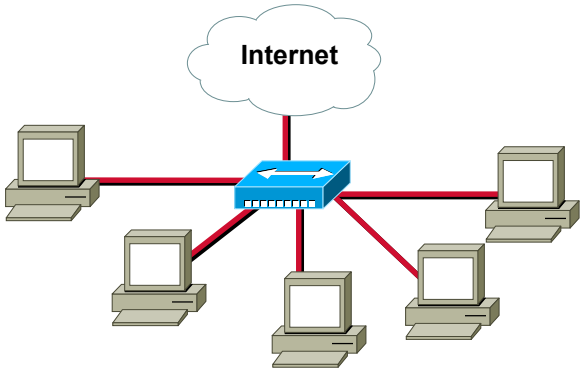


Figura 23. Esquema lógico del laboratorio 2

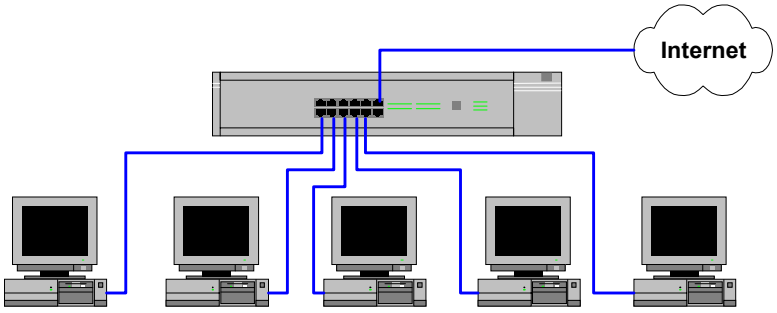


Figura 24. Esquema físico del laboratorio 2

La guía de laboratorio de esta experiencia se encuentra en el Anexo C.

4.4 Experiencia 3: Habilitación de Servicios Internet I

El objetivo de esta experiencia es poner en marcha algunos de los servicios fundamentales de un ISP. El primer servicio que se instalará será el DNS, que es el eje rector del resto de los servicios Internet. Adicionalmente se instalará el servicio WWW, Telnet, FTP y FTP anónimo.

Los objetivos de la experiencia 3 son:

1. Instalación y configuración del servicio DNS.
2. Instalación y configuración del servicio WWW.
3. Instalación y configuración del servicio Telnet.
4. Instalación y configuración del servicio FTP y FTP anónimo.

En esta experiencia interesa mostrar algunos de los servicios de Internet. Para mostrar el esquema de cliente servidor, para esta experiencia se separarán los computadores en pares, donde uno de ellos será el ISP y el otro solicitará servicios. La nube Internet se refiere a los otros pares de computadores, esto para hacer más interesante la experiencia. El esquema de conexión se ve en la Figura 25. El esquema físico de la experiencia se ve en la Figura 26. En esta experiencia se consultaron [howto DNS], [howto ISP2] y [Kirch 1999] entre otros. La duración estimada de la sesión es de 4 horas.

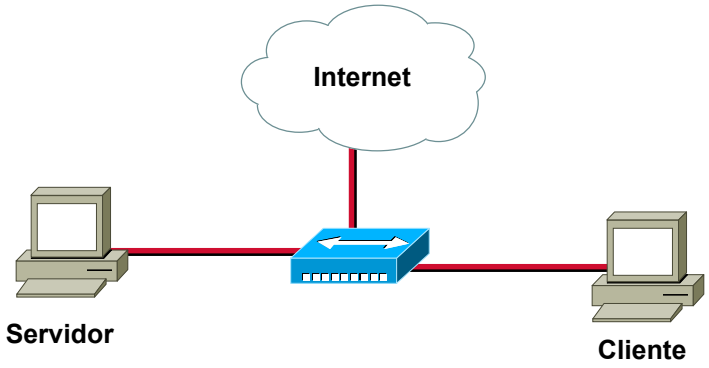


Figura 25. Esquema lógico experiencia 3

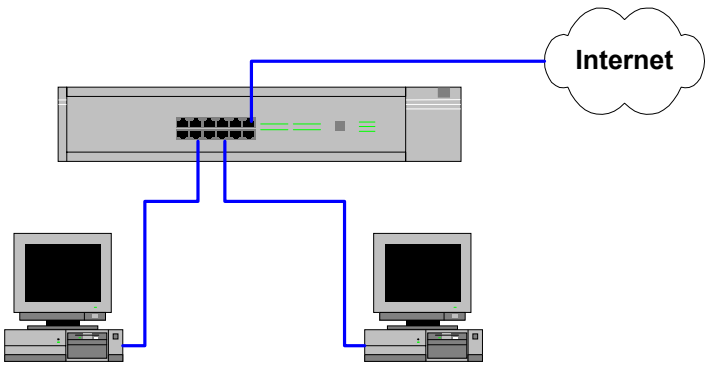


Figura 26. Esquema físico experiencia 3

La guía de laboratorio de esta experiencia se encuentra en el Anexo D.

4.5 Experiencia 4: Habilitación de los Servicios de Conectividad

El objetivo de esta experiencia es habilitar los servicios de conectividad. En la experiencia pasada se implementaron algunos de los servicios de un ISP, en ésta se mostrarán las capacidades de conectividad que ofrecen los sistemas Unix, en particular de Linux, de modo de mostrar como emular los equipos de redes (routers y servidores de acceso) con el software proveído en el sistema.

Para la emulación de routers, existe un protocolo llamado `routed` que es capaz de implementar RIP. Routed fue mejorado por `gated`, otra aplicación diseñada para habilitar servicios de enrutamiento, que implementa RIP, OSPF, BGP y otros. Mayor información de gated se puede obtener en www.gated.org. En esta experiencia sólo se mostrará una introducción a estos tópicos.

Los objetivos de la experiencia 4 son:

1. Mostrar el servicio de enrutamiento directo.
2. Mostrar el mecanismo de conexión conmutada en lado servidor y cliente.

En esta experiencia interesa mostrar los requerimientos mínimos de interconectividad que se necesitan para el ISP. Note que los computadores, a través de la interfaz ethernet, están conectados a puertas del hub, y por otra puerta del hub (aquella que acepta cross-over) se conectará un cable hacia la Internet. También existe un computador conectado con acceso conmutado. El esquema de conexión se ve en la Figura 27. En el esquema se ve a un computador como servidor, y clientes haciéndole consultas tanto en la red del servidor, como a través de un acceso conmutado telefónico. En la Figura 28 se muestra el esquema físico. En la experiencia se consultaron [Gentry 1999], [howto ISP1] y [Kirch 1999]. La duración estimada de la sesión es de 2.5 horas.

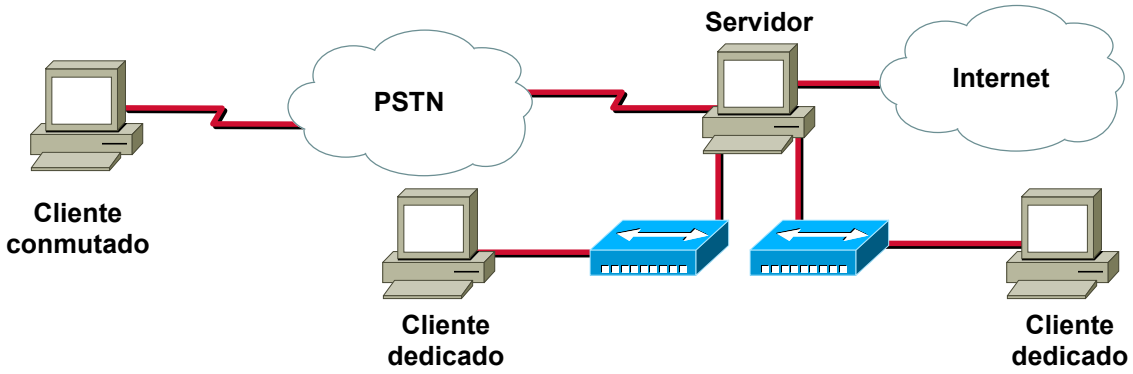


Figura 27. Esquema lógico del laboratorio 4

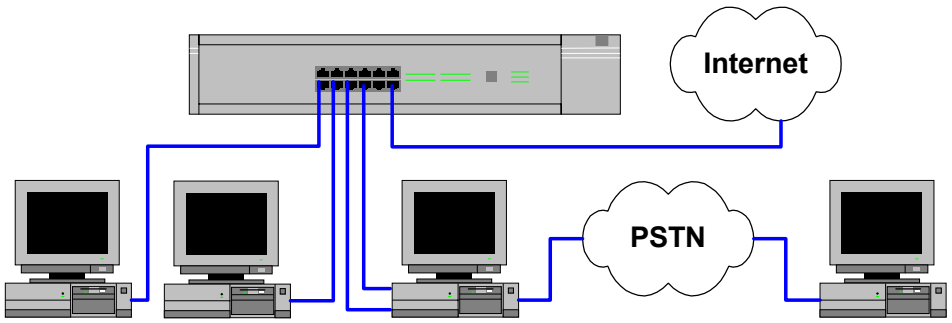


Figura 28. Esquema físico del laboratorio 4

La guía de laboratorio de esta experiencia se encuentra en el Anexo E.

4.6 Experiencia 5: Habilitación de Servicios Internet II

En esta experiencia se pretende terminar la instalación de los servicios de un ISP mínimo, y mostrar una introducción al tema de la seguridad.

- Para hacer una introducción al tema de seguridad en redes se muestra una implementación de firewall para Linux a nivel de aplicación.
- Respecto a los servicios, se mostrará la instalación de sendmail y POP3. También se muestra el servicio proxy en las versiones de acelerador httpd (con lo que se consigue bajar la carga al servidor httpd) y como proxy-caching.

Los objetivos de la experiencia son:

1. Instalación y configuración del firewall.
2. Instalación y configuración del servicio SMTP.
3. Instalación y configuración del servicio POP3.
4. Instalación y configuración del proxy.

En esta experiencia interesa continuar con los servicios de Internet. Los esquemas son iguales a los de la experiencia tres. El esquema de conexión se ve en la Figura 29. El esquema físico de la experiencia se ve en la Figura 30. En esta experiencia se consultaron [howto firewall & proxy], [howto ipchains] y [howto ISP2] entre otros. La duración estimada de la sesión es de 3 horas.

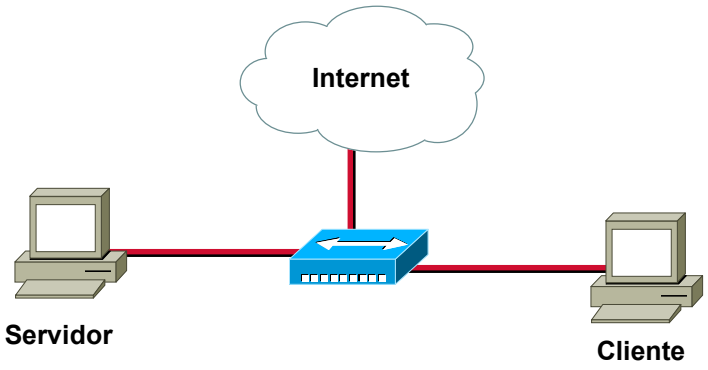


Figura 29. Esquema lógico experiencia 5

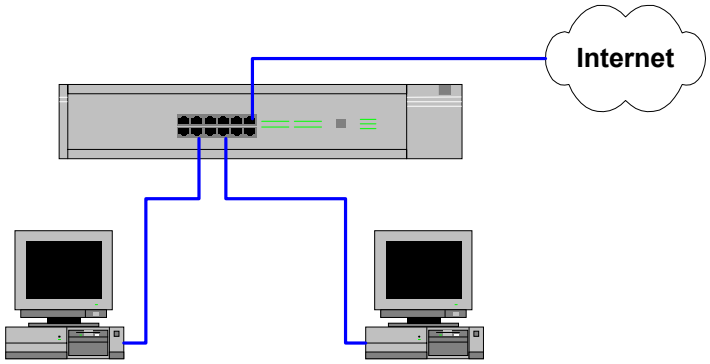


Figura 30. Esquema físico experiencia 5

La guía de laboratorio de esta experiencia se encuentra en el Anexo F.

Capítulo 5: Discusión

En la actualidad, el análisis y diseño de las redes de computadores considera con mayor intensidad a los servicios ofrecidos por la *"red"*, por ejemplo: web, correo electrónico, etc. De este modo, cobra relevancia el conocimiento y comprensión de estos servicios y sus mecanismos de implementación.

Los servicios (e-mail, web, etc.) constituyen el corazón de un ISP, debido a esto cualquier implementación de un ISP debe contemplar a los servicios como un eje rector en la especificación del software y el hardware a emplear.

Esta memoria aborda el tema de los servicios Internet a través de un conjunto de seis guías de laboratorio, en donde propone un plan sistemático con el cual se consigue la puesta en marcha de un ISP a pequeña escala. En las primeras tres experiencias se familiariza al alumno con los tópicos asociados a un ISP, y en las restantes experiencias se muestra como implementar el ISP en cuestión.

En la elaboración de las guías del laboratorio se contemplan tres etapas: Diseño, Implementación y Validación. Las primeras dos fueron cubiertas completamente, en cambio, sólo se validó la corrección técnica de las guías, queda para futuras mejoras la validación pedagógica de las mismas.

La metodología de planificación de las experiencias fue analizar el ISP en su totalidad, y a partir de esto definir la segmentación presentada en la Tabla 7 "Planificación de las experiencias". Con esta planificación se consigue poner en operación los servicios mínimos que presta un ISP.

Las guías de laboratorio consisten en una colección de pasos necesarios para la implementación de las actividades. Los pasos se separan en grupos temáticos o secciones. También se incluyen puntos de control intermedios y un cuestionario final, de modo que el alumno pueda controlar el grado de entendimiento de las actividades realizadas. Además se acompaña material de apoyo para las guías de laboratorio.

Las guías experimentales fueron desarrolladas de modo que la presentación de los contenidos sea lo más completa posible desde el punto de vista técnico. Para obtener un conocimiento mayor de la teoría envuelta en los temas mostrados, se tiene disponible en Internet una gran variedad de documentación en formato electrónico. Para ello se cuentan sitios tales como www.cisco.com, www.redhat.com, metalab.unc.edu, www.hispalinux.es, etc., por lo cual se recomienda una revisión de esta documentación, en especial la bibliografía indicada para cada sesión, al momento de desarrollar las guías, si se desea profundizar en los contenidos.

Para apoyar al profesor encargado de las experiencias se prepararon un conjunto de transparencias de modo de facilitar la entrega de contenidos a los alumnos y realizar las experiencias de modo más fluido. También se anexa una copia de la distribución de Linux utilizada.

En los puntos de control, se plantean mecanismos de verificación de las actividades desarrolladas en la guía, y preguntas fundamentales de modo que el alumno evalúe personalmente su grado de entendimiento de las actividades. Esto es sumamente importante, puesto que permite al alumno analizar y mejorar su dominio en el tema.

Los cuestionarios finales plantean una serie de consultas de corte fundamental y de integración de contenidos, que muestran como a través de herramientas simples se pueden construir poderosos mecanismos para administración y verificación del estado de la red. Esta facilidad está soportada principalmente por el sistema operativo Linux, ya que provee herramientas de automatización de tareas, y una filosofía de entrada y salida de procesos uniforme, lo que permite que con la concatenación de comandos sencillos se puedan construir herramientas de mayor poder.

El laboratorio docente se diseñó pensando en ocupar la menor infraestructura de hardware posible, de modo de poder ser implementado en las instalaciones del laboratorio de Internetworking que actualmente dispone el DIE, Universidad de Chile.

Se validó con usuarios expertos en el tema, lo que garantiza la corrección de las guías desde el punto de vista técnico, pero falta la validación con un grupo de beta tester sin experiencia en el tema, con lo que se mejorará la validez pedagógica de las experiencias. Esta realimentación mejoraría la forma de cómo se presentan los contenidos en las guías experimentales.

Como resultado de esta memoria se diseñaron seis guías experimentales que tratan los siguientes temas:

- Introducción a los ISP.
- Instalación de Linux y verificación inicial del sistema operativo.
- Administración básica de Linux.
- Habilitación de los servicios DNS, HTTP, TELNET y FTP.
- Habilitación de los servicios de conectividad.
- Habilitación de mecanismos de seguridad, servicios de Correo Electrónico y PROXY.

Con los mecanismos propuestos en las guías de laboratorio se logra poner en correcta operación los servicios del ISP mínimo, lo que prueba la validez técnica de las experiencias.

Las guías desarrolladas para el laboratorio están en los anexos, además se incluyen un anexo de recomendaciones generales, otro en donde se indica la configuración de los computadores utilizados en las pruebas y otro donde se explica con mayor detalle en que consiste un ISP.

Las recomendaciones indicadas en el Anexo G. “Recomendaciones Generales” son válidas para el conjunto de las experiencias. En ellas se señalan detalles a considerar desde el punto de vista técnico-experimental, puesto que este es el foco de las guías.

Como se ve en el Anexo H. “Configuración de los Computadores de Pruebas”, para los experimentos no se utilizaron computadores muy sofisticados o de elevado valor, que es uno de los objetivos que se plantearon para el laboratorio.

En el Anexo I. “¿Qué es un ISP?”, se explica con mayor detalle en que consiste un ISP, y se orienta el análisis a los ISP pequeños, tanto desde el punto de vista del hardware como del software. Esta información será relevante para los alumnos, ya que permitirá inducirlos en el tema de forma gradual.

Desde el punto de vista de las conexiones y el hardware, salvo en la “Experiencia 4: Habilitación de los Servicios de Conectividad”, son bastante reducidas.

En las experiencias se muestran las direcciones IP empleadas durante su fase de desarrollo, pero durante la ejecución de las experiencias el esquema de direccionamiento IP se deja a libre elección del profesor encargado de la sesión. Para las experiencias demostrativas se pueden utilizar direcciones válidas, en cambio en las experiencias de instalación y configuración de servicios se recomienda utilizar direcciones privadas del segmento 192.168.0.0/16 en una red cerrada hacia la Internet, de modo de no propagar los eventuales errores a la Internet.

Debido a que estas experiencias están orientadas a los servicios, el tiempo necesario para ellas puede ser muy variable dependiendo de las habilidades de los alumnos. Inicialmente fueron diseñadas para un lapso de tiempo de 3 horas, pero dado que se privilegió la completitud de las experiencias frente a ajustarlas en el tiempo, se considera necesario realizar las experiencias 2 y 3 en dos etapas. Para la experiencia 2 se recomienda en la primera etapa realizar las secciones 0 a la 8, y en la segunda el resto de las secciones. Para la experiencia 3 se recomienda realizar en la primera etapa las secciones 0 a la 3, y en la segunda, el resto de las secciones.

Las experiencias están orientadas a alumnos que posean un nivel medio de conocimientos en redes de computadores y que estén interesados en las aplicaciones que se implementan sobre la plataforma de hardware disponible. Es importante que los alumnos estén motivados con el tema, puesto que durante la

instalación de los servicios será frecuente que los alumnos se enfrenten a procesos de configuración de dificultad creciente, sujeta a errores en la manipulación de los archivos de inicialización.

La dificultad teórica de las sesiones es de nivel bajo a medio, en cambio en el aspecto práctico se tienen muchos factores que podrían artificialmente entorpecer el desarrollo de las experiencias. Se recomienda tener cuidado con los errores tipográficos.

La secuencia de pasos mostrada en las guías no es única, pero si no se conoce con detalle los servicios a instalar, se recomienda respetarla.

Durante el desarrollo de las experiencias fueron utilizadas herramientas de dominio público considerando los siguientes elementos de decisión:

- Las herramientas de dominio público son gratuitas.
- Las herramientas de dominio público están bien documentadas.
- Las herramientas de dominio público en general cumplen los estándares propuestos para los servicios.
- Existe una gran variedad de grupos de discusión orientados a las herramientas de dominio público.
- Las herramientas de dominio público están en constante evolución y desarrollo, por lo cual en general es posible esperar que aparezca una nueva versión que satisfaga los requerimientos solicitados.
- Las herramientas de dominio público utilizadas cubren las necesidades del laboratorio.

Se consiguió obtener un mecanismo sistemático para la instalación de los servicios del ISP, comenzando con el servicio rector en Internet, el DNS, luego el resto de los servicios básicos del ISP, una introducción a los servicios de seguridad y finalizando con herramientas de optimización y administración de redes. Con las guías desarrolladas y un buen acuerdo con el ISP proveedor se puede llevar a cabo la configuración mostrada en la Figura 1, en donde se tiene a un ISP cliente, proveyendo servicios dentro de una red pequeña, conectado a un ISP mayor (ISP proveedor) con lo que obtiene la salida a Internet y el resto de los servicios.

Con los servicios mostrados en las experiencias 3 y 5 se consigue implementar lo que se conoce como ISP virtual (VISP). Un VISP está formado por la granja de servidores, y no provee servicios de conectividad, puesto que los arrienda a otras instituciones. Esta opción es utilizada por empresas pequeñas, que están interesadas en proveer servicios (sitios web, correo electrónico, FTP, etc.) pero no están en la capacidad de instalar la infraestructura necesaria para ofrecer los servicios de conectividad.

La metodología mostrada en las experiencias se conserva en el tiempo, en cambio los programas a instalar pueden ir cambiando, en particular se aconseja revisar el número de la versión que está siendo instalado. Por otro lado, las aplicaciones utilizadas en los experimentos podrían quedar obsoletas, de modo que es conveniente estar atento a las nuevas versiones y reimplementaciones de los servicios.

Las experiencias están enfocadas para un ISP de pequeña escala. A continuación se nombran algunos parámetros a considerar al dimensionar un ISP:

- Dadas las razones de concentración usuales, 1 modem es capaz de atender de 8 a 10 usuarios.
- Frecuentemente se calcula que un usuario utiliza 5 a 6 Kbps de enlace hacia la Internet, para una red con 10 usuarios el enlace de salida debiera ser de 50 a 60 Kbps.
- El espacio utilizado en disco para los correos de los usuarios se debiera dimensionar considerando de 10 MB por cuenta.
- Dependiendo del tipo de usuario (usuario sólo de correo electrónico, usuario desarrollador, etc.), se debe dimensionar como mínimo 20 MB de espacio de disco para los archivos personales en el servidor.
- Para alojar un sitio web pequeño a mediano se necesitan 50 MB en espacio de disco.
- Para obtener un buen desempeño del servidor y considerando el actual estado del hardware desarrollado para computadores, se recomienda usar procesadores Pentium III 600 o superiores, K7 650 o superiores u otras arquitecturas de similares prestaciones (Alpha, Ultra SPARC, etc.).
- Tan importante como el procesador es la memoria principal con que cuente el sistema, se recomienda mínimo 128 MB.

- Cuando la cantidad de usuarios supere a 100, es recomendable separar los servicios intensos en uso de disco con los intensos en procesamiento, vale decir, es necesario dejar en una máquina separada del servidor principal los servicios de correos, web hosting, proxy y ftp. Para esto se recomienda que el computador más poderoso administre DNS, la conectividad hacia Internet y el resto de los servicios. Esto se indica puesto que los servicios intensos en disco usualmente no son exigentes en capacidad de procesamiento.

Dependiendo de qué tipos de servicio se desea proveer y su escala, será necesario utilizar las versiones profesionales de las aplicaciones utilizadas en los experimentos. Por supuesto, también será necesario utilizar computadores con mayor capacidad. Esto debido a que en general las versiones públicas son limitadas.

Para una implementación profesional de un ISP es necesario realizar una revisión más profunda de los siguientes aspectos:

- Seguridad del sitio.
- Autentificación, autorización y tasación (AAA).
- Administración del ancho de banda.
- Dimensionamiento de los enlaces.
- Disponibilidad de los enlaces.
- Dimensionamiento de los servidores.
- Disponibilidad de los servidores.
- Balanceo de la carga de los servidores.
- Protocolos de ruteo interno y externo.
- Administración del espacio de disco.
- Plataforma de acceso remoto (RAS).
- Diseño de la red interna del ISP considerando el modelo jerárquico de redes.

El tema de ISP profesionales no es el foco de esta memoria. En [Neira 1998] se detalló la instalación un ISP a nivel profesional y se muestra una metodología para la instalación de ISP comerciales de alta disponibilidad. Ciertamente han cambiado las tecnologías empleadas en la implementación de dicho ISP respecto de las actuales, pero es un buen punto de partida.

Ya no hay discusión sobre el hecho de que las empresas utilizarán o no Internet. Actualmente, la explosión de popularidad que viven las tecnologías de telecomunicaciones muestran la gran utilidad prestada por los servicios Internet. Es en este contexto donde esta memoria cobra un mayor valor aún, convirtiéndose en una guía para los profesionales que quieran integrarse en el desarrollo de Internet.

En lo inmediato, las guías propuestas en esta memoria sirven de apoyo a los cursos EL64E: “Redes de Computadores” y EL54B: “Sistemas de Procesamiento de la Información” y son complementarias para el curso EL717: “Seminario de Sistemas Digitales”, impartidos en el Departamento de Ingeniería Eléctrica, Universidad de Chile.

Capítulo 6: Conclusiones

Con la segmentación de las actividades utilizada se consiguió plantear una metodología sistemática para la implementación y puesta en marcha del ISP mínimo, a un bajo costo.

La segmentación de las actividades se materializó en las guías experimentales, en donde a través de una serie de pasos el alumno será capaz de poner en marcha los servicios que presta el ISP.

Los servicios constituyen el corazón de un ISP, debido a esto, cualquier implementación de un ISP debe contemplarlos como un eje rector en la especificación del software y el hardware a emplear.

Se diseñó e implementó completamente el plan propuesto de las seis experiencias, con las cuales se cubren los servicios mínimos que presta un ISP. Los temas cubiertos por las experiencias son los siguientes:

- La experiencia 0 muestra el ISP operando, a modo de introducción y motivación para los alumnos.
- La experiencia 1 muestra el proceso de instalación de Linux y verificación inicial del sistema operativo.
- La experiencia 2 muestra los comandos básicos de administración de Linux.
- La experiencia 3 muestra la instalación y configuración de los servicios DNS, WWW, Telnet y FTP.
- La experiencia 4 muestra la instalación y configuración de los servicios de conectividad conmutada y dedicada.
- La experiencia 5 muestra la instalación y configuración de los servicios de firewall, correo electrónico, proxy.

Se utilizó la metodología de construcción de las guías mostrada en [Hernández 2000], debido a que ya ha sido probada mostrando buenos resultados en las sesiones experimentales del Postítulo de Internetworking, dictado en el Departamento de Ingeniería Eléctrica.

La validación de las experiencias se realizó desde el punto de vista técnico, consiguiendo todos los objetivos planteados.

Es importante destacar el valor docente de un laboratorio, en donde se permite un alto grado de entendimiento de las actividades e interacción de los alumnos.

Las experiencias están diseñadas para alumnos con mediana preparación en el tema de redes, pero altamente motivados. Esto es importante destacarlo, puesto que será usual en el desarrollo de las sesiones la corrección de errores o malas maniobras por parte de los alumnos.

Este laboratorio ofrece a sus alumnos, sean ellos profesionales o estudiantes, la posibilidad de desarrollarse y mejorar sus conocimientos relacionados a Internet. Esto ofrece una excelente posibilidad de distinguirse positivamente del resto de sus colegas.

Este trabajo está inmerso en el área de desarrollo de Internetworking, constituyéndose como un aporte en la realización de un gran curso llamado “Laboratorio Docente de Redes de Computadores”, en donde se cubrirán una gran variedad de tecnologías de telecomunicaciones, con lo que se potenciaría enormemente la docencia en el Departamento de Ingeniería Eléctrica. A corto plazo, los contenidos cubiertos por las experiencias propuestas apoyan a los contenidos cubiertos en los cursos EL64E: “Redes de Computadores” y EL54B: “Sistemas de Procesamiento de la Información” y son complementarios al curso EL717: “Seminario de Sistemas Digitales”, impartidos en el DIE, Universidad de Chile.

Actualmente ya se están realizando esfuerzos incipientes en el DIE para abordar la docencia experimental en Internetworking a nivel de pregrado. A nivel de postítulo, ya se realizó la primera versión de sesiones experimentales, con lo cual se ha obtenido un valioso aporte tanto para planificar los tópicos a cubrir, como para mejorar la metodología necesaria para entregar los contenidos.

En la actualidad es frecuente el uso de VISP por parte de algunas empresas que desean obtener un mayor control sobre sus recursos informáticos, pero dado que la inversión en mecanismos de acceso es elevada prefieren arrendarlos a terceros. Estos requerimientos también son cubiertos en esta memoria, puesto que con las actividades de las experiencias 3 y 5 se consigue poner en marcha un VISP.

Como una continuación directa del trabajo realizado está la validación pedagógica de las experiencias, con lo que se conseguirá una realimentación que será útil para mejorar la calidad docente la exposición de los contenidos en las guías, y también será para útil fijar los tiempos necesarios para la realización de las actividades propuestas en el laboratorio.

En el capítulo de discusión se nombran una serie de aspectos necesarios para la implementación de ISP profesionales. Estos tópicos también se pueden abordar desde la perspectiva de laboratorios docentes, enfocados a temas tales como implementación de servicios de alta disponibilidad, planificación de redes, servidores de acceso, seguridad en redes, sistemas de administración y calidad de servicio. Estos laboratorios serán sumamente atractivos para los profesionales orientados al área de Internetworking, potenciando el ámbito de cobertura en la docencia de postítulo.

Capítulo 7: Referencias y Acrónimos

7.1 Bibliografía

[Cekit 1998] Manuel Felipe González, “Curso Práctico sobre Mantenimiento, Reparación, Actualización e Instalación de Computadoras”, fascículos 1+2 y 3, CEKIT S.A., Colombia, 1998.

[Hernández 2000] Luis Eduardo Hernández Astudillo, “Diseño e Implementación de un Laboratorio Docente de LAN Switching y ATM”, memoria para optar al título de Ingeniero Civil Electricista, Universidad de Chile, 2000.

[Neira 1998] José Arturo Neira Quiroga, "Diseño e Implementación de un Sitio Proveedor de Servicios Internet", memoria para optar al título de Ingeniero Civil Electricista, Universidad de Chile, 1998.

[Piquer 1997] José M. Piquer, “CC51C Comunicación de Datos Apuntes”, Departamento de Ciencias de la Computación, Universidad de Chile, 1997.

[Schwartz 1997] Randal L. Schwartz and Tom Christiansen, “Learning Perl”, Second Edition, O’Reilly & Associates Inc, Estados Unidos, 1997.

[Spohn 1997] Darren L. Spohn, "Data Network Design", Second Edition, McGraw-Hill, Estados Unidos, 1997.

[Tanenbaum 1997] Andrew S. Tanenbaum, "Redes de Computadoras", Tercera Edición, Prentice-Hall Hispanoamericana S.A., México, 1997.

[Welsh et al 1999] Matt Welsh, Matthias Kalle Dalheimer & Lar Kaufman, “Running Linux”, Third Edition, O’Reilly & Associates Inc, Estados Unidos, 1999.

7.2 Referencias Electrónicas

[Cisco EIGRP] Cisco Systems Inc, “Enhanced IGRP”, http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/en_igrp.htm, 23 de Mayo de 2000.

[Cisco IGRP] Cisco Systems Inc, “Interior Gateway Routing Protocol”, http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/igrp.htm, 23 de Mayo de 2000.

[Cisco IDB] Cisco Systems Inc., "Internetworking Design Basics", http://www.cisco.com/univercd/cc/td/doc/cisintwk/idg4/nd2002.htm, 21 de Febrero de 2000.

[Gentry 1999] Josh Gentry, “Linux Dialin Server Setup Guide”, http://ftp.the-gc.net/lg/issue38/gentry.html, 02 de Julio de 2000.

[howto DNS] LDP, Nicolai Langfeldt, “DNS HOWO”, http://metalab.unc.edu/pub/Linux/docs/HOWTO/other-formats/pdf/DNS-HOWTO.pdf, 07 de Junio de 2000.

[howto firewall & proxy] LDP, Mark Grennan, “Firewall and Proxy Server HOWTO”, http://metalab.unc.edu/pub/Linux/docs/HOWTO/other-formats/pdf/Firewall-HOWTO.pdf, 07 de Junio de 2000.

[howto ipchains] LDP, Paul Russell, “Linux IPCHAINS-HOWTO”, http://metalab.unc.edu/pub/Linux/docs/HOWTO/other-formats/pdf/IPCHAINS-HOWTO.pdf, 07 de Junio de 2000.

[howto ISP1] LDP, Egil Kvaleberg, “ISP-Hookup-HOWTO”, http://metalab.unc.edu/pub/Linux/docs/HOWTO/other-formats/pdf/ISP-Hookup-HOWTO.pdf, 07 de Junio de 2000.

[howto ISP2] LDP, Anton Chuvakin, “”Pocket” ISP based on RedHat Linux”, http://metalab.unc.edu/pub/Linux/docs/HOWTO/other-formats/pdf/ISP-Setup-RedHat.pdf, 07 de Junio de 2000.

[howto kernel] LDP, Brian Ward, “The Linux Kernel HOWTO”, http://metalab.unc.edu/pub/Linux/docs/HOWTO/other-formats/pdf/Kernel-HOWTO.pdf, 07 de Junio de 2000.

[ISOC] Internet Society, "Internet Society" (ISOC): Welcome Internet Society (ISOC) Web Site”, http://www.isoc.org/, 27 de Julio 2000.

[Kirch 1999] Olaf Kirch (Traducción Proyecto LuCAS), “Guía de Administración de Redes con Linux”, http://lucas.hispalinux.es/htmls/manuales.html, 20 de Mayo de 2000.

[RFC 821] Postel B. Jonathan, “Simple Mail Transfer Protocol”, http://www.ietf.org/rfc/rfc0821.txt, 24 de Mayo de 2000.

[RFC 822] D. Crocker, “Standard for the format of ARPA Internet text messages”, http://www.ietf.org/rfc0822.txt, 24 de Mayo de 2000.

[RFC 0959] J. Postel, J.K. Reynolds, “File Transfer Protocol”, ftp://ftp.isi.edu/in-notes/rfc959.txt, 17 de Julio de 2000.

[RFC 977] Brian Kantor, Phil Lapsley, “Network News Transfer Protocol”, http://info.internet.isi.edu/in-notes/rfc/files/rfc977.txt, 24 de Mayo de 2000.

[RFC 1034] P. Mockapetris, “DOMAIN NAMES - CONCEPTS AND FACILITIES”, ftp://ftp.isi.edu/in-notes/std/std13.txt, 24 de Mayo de 2000.

[RFC 1035] P. Mockapetris, “DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION”, ftp://ftp.isi.edu/in-notes/rfc1035.txt, 24 de Mayo de 2000.

[RFC 1112] S. Deering, “Host Extensions for IP Multicasting”, http://www.ietf.org/rfc/rfc1112.txt, 22 de Mayo de 2000.

[RFC 1519] Fuller, Li, Yu & Varadhan, “Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy“, ftp://ftp.isi.edu/in-notes/rfc1519.txt, 23 de Mayo de 2000.

[RFC 1725] Myers J., Rose M., “Post Office Protocol – Version 3”, http://www.ietf.org/rfc/rfc1725.txt, 24 de Mayo de 2000.

[RFC 1771] Rekhter & Li, “A Border Gateway Protocol 4 (BGP-4)“, ftp://ftp.isi.edu/in-notes/rfc1771.txt, 23 de Mayo de 2000.

[RFC 1918] Y. Rekhter et al, “Address Allocation for Private Internets”, http://www.ietf.org/rfc/rfc1918.txt, 22 de Mayo de 2000.

[RFC 2328] J. Moy, “OSPF Version 2“, ftp://ftp.isi.edu/in-notes/rfc2328.txt, 23 de Mayo de 2000.

[RFC 2453] G. Malkin, “RIP Version 2”, ftp://ftp.isi.edu/in-notes/rfc2453.txt, 23 de Mayo de 2000.

7.3 Acrónimos

AAA: Authentication, Authorization and Accounting.
ACK: Acknowledge.
ARP: Address Resolution Protocol.
AS: Autonomous System.
ASCII: American Standard Code for Information Interchange.
ATAPI: AT Attachment Packet Interface.
ATM: Asynchronous Transfer Mode.
BIOS: Basic Input Output System.
BGP: Border Gategay Protocol.
CD-ROM: Compact Disc Read-Only Memory.
CIDR: Classless Inter-Domain Routing.
CSLIP: Compressed SLIP.
CSMA/CD: Carrier Sense Multiple Access with Collision Detection.
DIE: Departamento de Ingeniería Electrica.
DMZ: Demilitarized Zone.
DNS: Domain Name Server.
DQDB: Distributed Queue Dual Bus.
EGP: Exterior Gateway Protocol.
EIGRP: Enhanced IGRP.
ext2fs: Second Extended Filesystem.
FDDI: Fiber Distributed Data Interface.
FQND: Fully Qualified Domain Name.
FR: Frame Relay.
FTP: File Transfer Protocol.
HTML: HyperText Markup Language.
HTTP: Hiper Text Markup Protocol.
ICMP: Internet Control Message Protocol.
IDE: Integrated Drive Electronics.
IEEE: Institute of Electrical and Electronics Engineers.
IEEE 802.3: Protocolo LAN conocido como Ethernet.
IEEE 802.5: Protocolo LAN Token Ring.
IEEE 802.6: Protocolo MAN DQDB.
IETF: Internet Engineering Task Force.
IGP: Interior Gateway Protocol.
IGRP: Interior Gateway Routing Protocol.
IP: Internet Protocol.
IRC: Internet Relay Chat.
ISO: International Organization for Standardization.
ISOC: Internet Society.
ISP: Internet Service Provider
LAN: Local Area Network.
LILO: Linux Loader.
LDP: Linux Documentation Project.
MAN: Metropolitan Area Network.
Mbps: Megabit / segundo.
MTA: Message Transfer Agent.
NFS: Network File System.
NIS: Network Information Service
NNTP: Network News Transfer Protocol.
OSI: Open Systems Interconnection.
OSPF: Open Shortest Path First.
PAM: Pluggable Authentication Modules.
Perl: Practical Extraction and Report Language.
PLIP: Paralel Line Internet Protocol.

POP3: Post Office Protocol – Version 3.
PPP: Point to Point Protocol.
PSTN: Public Switched Telephony Network.
RADIUS: Remote Authentication Dial-In User Service.
RAM: Random Access Memory.
RAS: Remote Access Server.
RFC: Request For Comment (IETF Document Series).
RIP: Routing Information Protocol .
RPC: Remote Procedure Call.
SLIP: Serial Line Internet Protocol.
SMTP: Simple Mail Transfer Protocol.
TCP: Transmission Control Protocol.
TELNET: Remote Terminal Protocol.
UDP: User Datagram Protocol.
URL: Uniform Resource Locator.
UTP: Unshielded Twiested Pair.
UUCP: Unix to Unix Copy.
VISP: Virtual Internet Service Provider.
VoIP: Voice Over IP.
WAN: Wide Area Network.
WWW: World Wide Web.

ANEXOS

Anexo A. Experiencia 0: Sitio Proveedor de Servicios Internet Mínimo

A.1. Resumen

El objetivo de esta experiencia es introducir a los alumnos la noción de lo que es un sitio Proveedor de Servicios Internet (ISP). Para ello se mostrará una visión general de lo que es un ISP mínimo, sus funcionalidades y los requerimientos mínimos para poder realizar la implementación.

En esta experiencia se pretende realizar una nivelación de los conocimientos necesarios para realizar las experiencias siguientes.

Esta experiencia es esencialmente expositiva, y pretende entregar la motivación y los lineamientos básicos para el resto del laboratorio. En las siguientes sesiones se mostrará como se puede construir el ISP mínimo mostrado en esta oportunidad.

En esta experiencia y en las siguientes es importante considerar las recomendaciones del Anexo G. Recomendaciones Generales.

A.2. Esquemas generales

En esta experiencia interesa mostrar como los equipos clientes solicitan y reciben los servicios del ISP. Note que todos los computadores a través de la interfaz ethernet están conectados a puertas del hub, y por otra puerta del hub (aquella que acepta cross-over) se conectará un cable mirando hacia la Internet. El esquema de conexión se ve en la Figura 31. En él se ve a un computador como servidor y clientes haciéndole consultas tanto en la red del servidor, como a través de un acceso conmutado telefónico. En la Figura 32 se muestra el esquema físico, en donde se muestran explícitamente las conexiones en la parte posterior de los computadores. En las próximas experiencias se asumirá que el alumno sabe realizar las conexiones.

El objetivo de utilizar el hub con puerta de cross-over es para no utilizar cables UTP cruzados, sino que sólo utilizar cables UTP derechos.

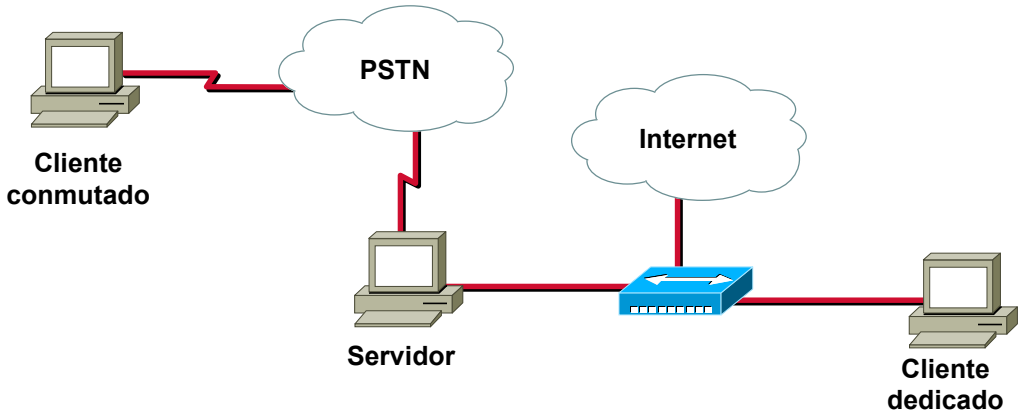


Figura 31. Esquema lógico del laboratorio 0

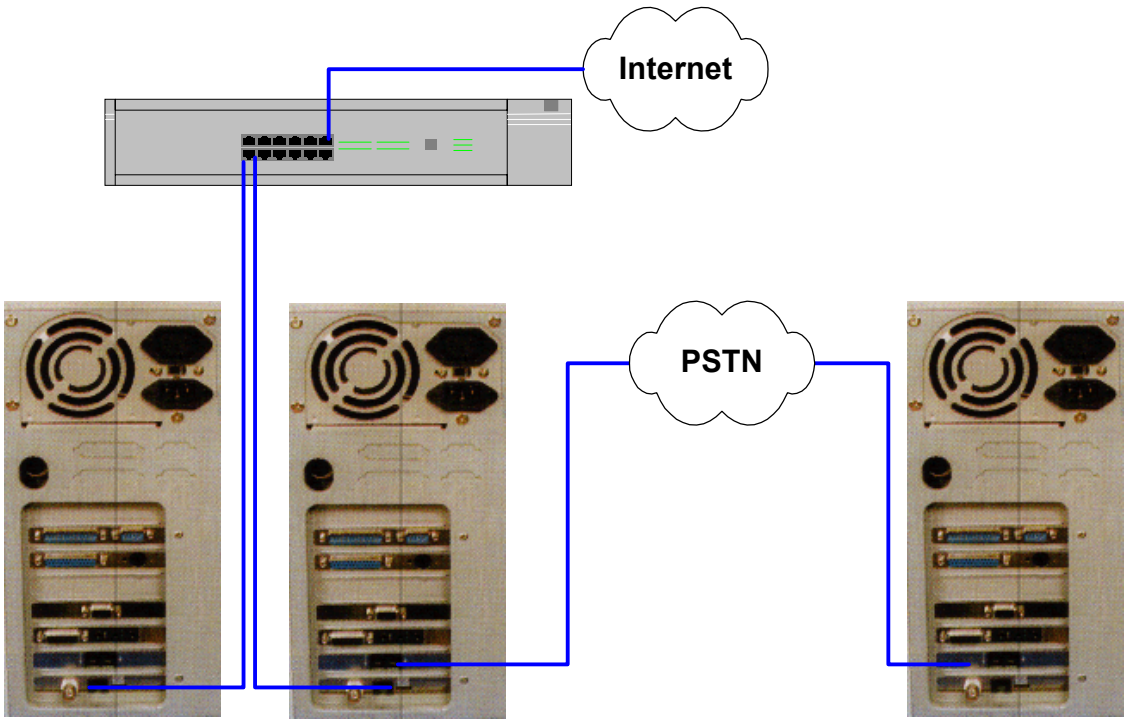


Figura 32. Esquema físico del laboratorio 0

A.3. Materiales

Para esta experiencia se necesita lo siguiente:

- ✓ 1 Computador habilitado como ISP mínimo.
- ✓ 1 Computador habilitado como cliente dedicado.
- ✓ 1 Computador habilitado como cliente conmutado.
- ✓ 1 Computador abierto para fines de mostrar sus componentes de hardware.
- ✓ 2 líneas telefónicas habilitadas.
- ✓ 3 Cables UTP con conectores machos.
- ✓ 1 Cable UTP cruzado con conectores machos (respaldo si falla la puerta cross-over del hub).
- ✓ 1 Hub que soporte cross-over en alguna puerta.

A.4. Objetivos

1. Introducir la noción de computador y sus componentes de hardware.
2. Introducir la noción de un computador de propósito general o computador cliente.
3. Introducir la noción de un computador servidor.
4. Introducir la noción de red LAN.
5. Mostrar el sistema operativo LINUX.
6. Introducir la noción de un ISP mínimo y su estructura interna.
7. Mostrar los servicios que presta un ISP mínimo a través de casos de uso típico.

A.5. Requisitos, conceptos y habilidades necesarias

- ✓ Conocimientos básicos de arquitectura de hardware, en particular el modelo Von Neumann.
- ✓ Conocimientos básicos de sistemas operativos.
- ✓ Noción de computador.
- ✓ Noción de red de computadores.
- ✓ Paradigma cliente/servidor.
- ✓ Noción de diseño modular.
- ✓ Modelos de referencia OSI y TCP/IP.
- ✓ Conocimientos básicos de direccionamiento IP.
- ✓ Las recomendaciones del Anexo G. Recomendaciones Generales.

A.6. Bibliografía y referencias

1. Apuntes del curso el54b: “Sistemas de Procesamiento de la Información”.
2. Apuntes del curso el64e: “Redes de Computadores”.
3. Apuntes del curso el647: “interfaces digitales y Periféricos”.
4. Apuntes del curso el649: “Programación y Operación de Computadores”.
5. Apuntes del curso cc51c: “Comunicación de Datos”.
6. Andrew S. Tanenbaum, "Redes de Computadoras", Tercera Edición, Prentice Hall, 1997.

A.7. Plan de acción

Los pasos a seguir en esta experiencia son:

1. Describir las componentes de hardware de un computador y sus funciones.
2. Describir las características de un equipo cliente.
3. Describir las características de un equipo servidor.
4. Describir las características de una red.
5. Mostrar el sistema operativo LINUX.
6. Verificar las funcionalidades de un ISP mínimo.

A.8. Sección 0: Conexiones

Paso 1 Se debe verificar todo el material.

Paso 2 Realice las conexiones tal como se muestran en el diagrama físico.

A.9. Sección 1: Computador abierto

Paso 1 Abrir el computador destinado para esta actividad y mostrar las componentes de interés para los fines del experimento:

- Tarjeta Madre: Este dispositivo ofrece el soporte para todas las funcionalidades que posea el computador. A través de los buses de comunicaciones permite la conexión de otros dispositivos de hardware tales como tarjetas de video, de red, de módem, etc. Está directamente ligada con el procesador del equipo, y es la que se encarga de entregarle un ambiente apropiado de trabajo.
- Procesador: También conocido como la unidad central de procesamiento (CPU) se constituye como el principal motor de cálculo del computador. En algunos computadores la CPU realiza todos los cálculos necesarios para resolver las actividades, incluyendo cálculos de entrada y salida, gráficos, análisis digital de señales de audio y video, etc. El sistema operativo que resida en la máquina interactúa con la CPU (a través de la tarjeta madre) mediante el uso de instrucciones de control y de cálculo, y de este modo resuelve los requerimientos de las aplicaciones.
- Tarjeta de red: Es un dispositivo que se encarga de proveer la conectividad del equipo a una red local, en un medio dedicado para este fin. De este modo, el equipo puede compartir sus recursos o utilizar recursos de otros equipos de la red permanentemente. En general ofrece velocidades de comunicación bastante altas, del orden de los Mbps o superiores.
- Tarjeta de módem telefónico: Al igual que la tarjeta de red, la de módem permite conectarse con otros equipos, pero esta vez a través de un medio conmutado, la red telefónica pública. Debido a esto es tiene una capacidad de comunicación mucho más disminuida que la de la tarjeta de red.
- Disco duro: Es una unidad magnética de almacenamiento de información. Tiene la característica de que permite un acceso aleatorio a los datos, tanto para lecturas como para escrituras.

En la Figura 33 se muestra la parte posterior de un computador, mientras en la Figura 34 se muestra el interior de un computador.

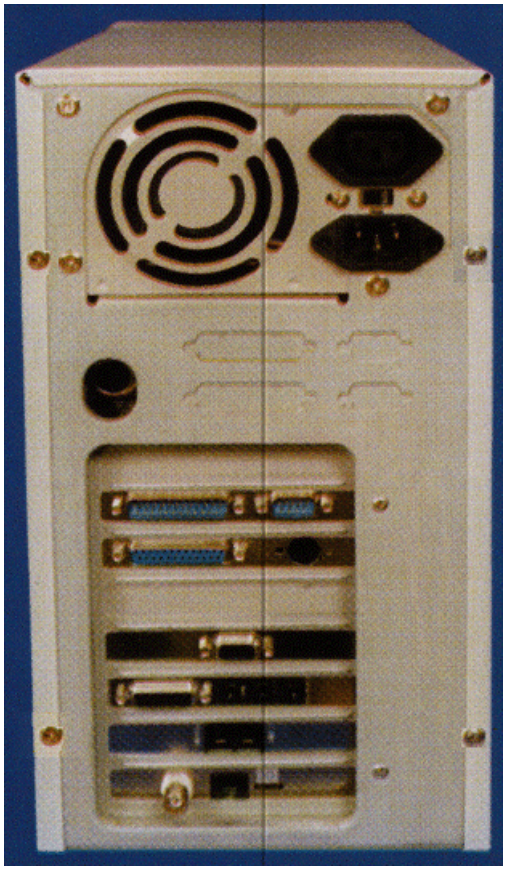


Figura 33. Vista posterior de un computador

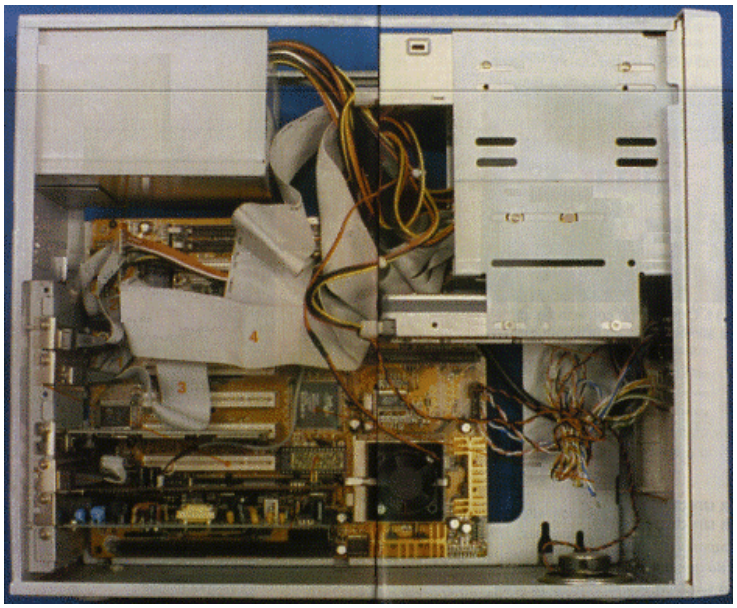


Figura 34. Vista Interior de un computador

A.10. Sección 2: Características de un equipo cliente

Paso 1 Verificar la operación de computador cliente:

- Verificar que sistema operativo tiene residente.
- Verificar que aplicaciones prácticas satisface (computador como estación de trabajo).
- Verificar que aplicaciones tiene incorporada la máquina.

A.11. Sección 3: Características de un equipo servidor

Paso 1 Verificar las funcionalidades de computador servidor:

- Verificar que sistema operativo tiene residente.
- Verificar que aplicaciones prácticas satisface (computador como servidor).
- Verificar que aplicaciones tiene incorporada la máquina.

Punto de Control 1: Verifique si existen diferencias en el hardware entre el equipo cliente y el equipo servidor. Anote aquí las diferencias. Explique por qué se tienen esas diferencias:

_____
_____
_____
_____

A.12. Sección 4: Redes de conexión dedicada

Paso 1 Verificar el equipamiento de redes presente:

- Verificar el Hub.
- Verificar las diferencias entre los cables UTP directos y cruzados.

Paso 2 Funcionalidad de la tarjeta de red.

En esta etapa interesa saber cual es la función del conjunto tarjeta de red / hub, en el contexto del laboratorio. Un ejemplo práctico para observar esto es realizar lo siguiente:

En una ventana de consola DOS ejecute el siguiente comando con su computador conectado al hub.

Nota: En el caso del ejemplo se utiliza el servidor `ftp.dcc.uchile.cl` desde `anakena.dcc.uchile.cl`, consulte al profesor el servidor que corresponda:

```
[0:05 anakena:~/]% ftp ftp.dcc.uchile.cl
```

El servidor debería responder lo siguiente:

```
Connected to ftp.dcc.uchile.cl.
220 sunsite FTP server ready.
Name (ftp.dcc.uchile.cl:raparede):
```

Ahora el servidor le está solicitando su nombre de usuario (login name), responda con el nombre `ftp`, el cual esta asociado al usuario público, es decir, un usuario que no tiene una cuenta asignada en el servidor.

```
Name (ftp.dcc.uchile.cl:raparede): ftp
```

El servidor responde lo siguiente:

```
331 Guest login ok, send your complete e-mail address as password.
Password:
```

Ahora el servidor le está solicitando su contraseña (password), debido a que empleó el nombre `ftp`, el servidor le solicita su dirección de correo electrónico como contraseña, digítela, cuando la digite no verá ninguna letra en la pantalla, está bien, se supone que la contraseña es secreta.

```
230 Guest login ok, access restrictions apply.
ftp>
```

En este instante usted esta dentro del sistema y puede obtener (enviar) información desde (hacia) la máquina.

Para salir ejecute el comando `quit`.

```
ftp> quit
221-You have transferred 0 bytes in 0 files.
221-Total traffic for this session was 1157 bytes in 0 transfers.
221-Thank you for using the FTP service on sunsite.
221 Goodbye.
```

Paso 3 Repita el comando (ftp) anterior pero en esta oportunidad desconecte el cable UTP correspondiente a su computador del hub.

Punto de Control 2: Explique porque el comando en esta oportunidad es infructuoso:

Explique intuitivamente la función del conjunto tarjeta de red / hub.

A.13. Sección 5: Redes de conexión dedicada

Paso 1 Levante una conexión conmutada.

```
[root@almendra /etc]# ifup ppp0
```

Paso 2 Ejecute las mismas instrucciones de la Sección 4, Paso 2.

A.14. Sección 6: Casos de uso

Dentro de los servicios típicos que presta un ISP están:

- Servicio de conectividad.
- Servidor TELNET.
- Servidor DNS.
- Servidor WWW.

- Servidor Correo.
- Selector de rutas, es decir operar como un router.

Para apreciar las funcionalidades de un ISP y tener una primera aproximación de LINUX (que es uno de los sabores de Unix) ejecute los siguientes comandos:

Paso 1 Inicio de una sesión TELNET.

Ejecute el comando `telnet gorrion.die.uchile.cl`

```
[0:17 anakena:~/]% telnet gorrion.die.uchile.cl
```

El servidor responde con:

```
Trying 10.0.25.99...
Connected to gorrion.die.uchile.cl.
Escape character is '^]'.

Red Hat Linux release 6.0 (Hedwig)
Kernel 2.2.5-15 on an i686
login:
```

Ahora el servidor le solicita su login, en el ejemplo se utiliza la cuenta `test`, con password `test`:

```
login: test
Password:
Last login: Wed Jun 28 23:35:42 from anakena.dcc.uchile.cl

[gorrion.die.uchile.cl:~/]%
```

Paso 2 Utilizando el servicio de resolución de nombres.

Ejecute el comando `nslookup`

```
[gorrion.die.uchile.cl:~/]% nslookup
```

El servidor responde con:

```
Default Server:  ict.cec.uchile.cl
Address:  200.9.100.1

>
```

Consulte la dirección de `gorrion.die.uchile.cl`

```
> gorrion.die.uchile.cl
```

El servidor responde con:

```
> gorrion.die.uchile.cl
Server:  ict.cec.uchile.cl
Address:  200.9.100.1

Name:    gorrion.die.uchile.cl
Addresses:  10.0.25.99, 146.83.6.74
```

Para salir utilice el comando `exit`

```
> exit
```

Punto de Control 3: Consulte nuevamente la dirección de gorrión.die.uchile.cl, nota alguna diferencia, por qué:

_____
_____
_____
_____

Paso 3 Utilizando el servidor web.

Nota: En el caso del ejemplo se emplea e servidor abril.firstcom.cl, consulte al profesor la dirección del servidor que corresponda.

Ejecute el comando `lynx www.die.uchile.cl`

```
[test@abril test]$ lynx www.die.uchile.cl
```

El servidor responde con:

```
Test Page for Red Hat Linux's Apache Installation

                                   It Worked!

   If you can see this, it means that the installation of the Apache software
   on this Red Hat Linux system was successful. You may now add content to
   this directory and replace this page.

                        ________________________________________

     If you are seeing this instead of the content you expected, please
     contact the administrator of the site involved. If you send mail about
     this to the authors of the Apache software or Red Hat Software, who
     almost certainly have nothing to do with this site, your message will
     be ignored.

                        ________________________________________

   The Apache documentation has been included with this distribution.

   For documentation and information on Red Hat Linux, please visit the web
   site of Red Hat Software. The manual for Red Hat Linux is available here.

   You are free to use the image below on an Apache-powered web server.
   Thanks for using Apache!

                              [ Powered by Apache ]
   You are free to use the image below on a Red Hat Linux-powered web server.
   Thanks for using Red Hat Linux!

                           [ Powered by Red Hat Linux ]

Commands: Use arrow keys to move, '?' for help, 'q' to quit, '<-' to go back.
  Arrow keys: Up and Down to move.  Right to follow a link; Left to go back.
 H)elp O)ptions P)rint G)o M)ain screen Q)uit /=search [delete]=history list
```

Para salir utilice el comando `q`, y luego `y`.

Paso 4 Uso del agente de correos.

Para enviarle un correo al usuario `test`, ejecute el comando `mail test`

```
[gorrion.die.uchile.cl:~/]% mail test
```

El servidor responde con:

```
Subject:
```

Escriba el tema (subject) del correo:

```
Subject: prueba de correo
```

Escriba el siguiente correo:

```
Esta es una prueba de correo
Saludos
.
```

Cuando el programa le pregunte por `Cc:` (courtesy copy) sólo presione <Enter>.

```
Cc:
```

Punto de Control 4: Verifique que le llegó el correo con el comando `mail`.

Paso 5 Uso del servidor FTP.

Esto ya se vio en la Sección 4, paso 2.

Paso 6 Finalización de una sesión TELNET.

Para finalizar la sesión TELNET, ejecute el comando `exit`

```
[gorrion.die.uchile.cl:~/]% exit
```

El servidor responde con:

```
logout
Connection closed by foreign host.
```

Paso 7 Verificación de rutas.

Para esto se pueden verificar varios casos de uso, en este caso se mostrará el comando `tracert` de DOS, análogo al `traceroute` de Unix.

```
C:\>tracert 146.83.8.200
```

El servidor responde con:

```
Traza a la dirección dgf.uchile.cl [146.83.8.200]
sobre un máximo de 30 saltos:

  1   127 ms    97 ms    93 ms  192.168.0.12
  2   116 ms   100 ms    97 ms  10.40.20.1
  3   133 ms   107 ms   106 ms  200.9.98.98
  4   109 ms    97 ms    93 ms  dgf.uchile.cl [146.83.8.200]
```

```
Traza completa.
```

A.15. Cuestionario final

1. Indique las diferencias entre un computador cliente y un servidor (analice el hardware, el software y sus funcionalidades).
2. Indique las diferencias entre la conexión conmutada y dedicada.
3. Cuál es la función principal del ISP.
4. Qué otras funciones cumple un ISP.
5. Construya un diagrama modular de las funcionalidades de un ISP.
6. Describa la función del DNS.

Anexo B. Experiencia 1: Instalación de Linux

B.1. Resumen

El objetivo de esta experiencia es instalar Linux sin ningún servicio habilitado.

La instalación se puede realizar a través del modo de texto o en el modo gráfico. El modo de texto ofrece una interfaz pobre, y para usuarios sin experiencia en Linux esto puede hacer más difícil el proceso, por esta razón se escoge el modo gráfico, que es más intuitivo y natural.

La selección de opciones en la instalación toma aproximadamente 50 minutos, y el proceso de copia de archivos, toma desde 25 minutos a 2 horas, dependiendo de la cantidad de paquetes a instalar, y la velocidad del computador, motivo por el cual se agregará una breve clase expositiva en donde se abordarán tópicos de las próximas experiencias.

B.2. Esquemas generales

En esta experiencia interesa mostrar el proceso de instalación de Linux. Desde el punto de vista del alumno, usted sólo considerará su computador conectado a un hub a través de la interfaz ethernet, y por otra puerta del hub (aquella que acepta cross-over) se conectará un cable mirando hacia la Internet. El esquema de conexión se ve en la Figura 35. En el esquema se ven los computadores de los alumnos y la Internet conectados a un hub. El esquema físico de la experiencia se ve en la Figura 36.

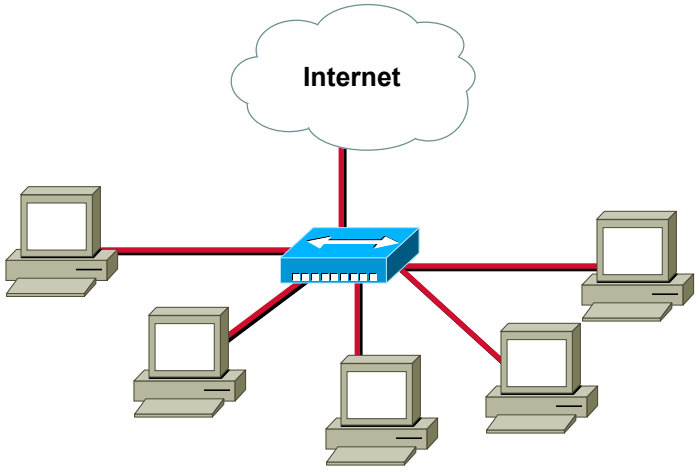


Figura 35. Esquema lógico del laboratorio 1

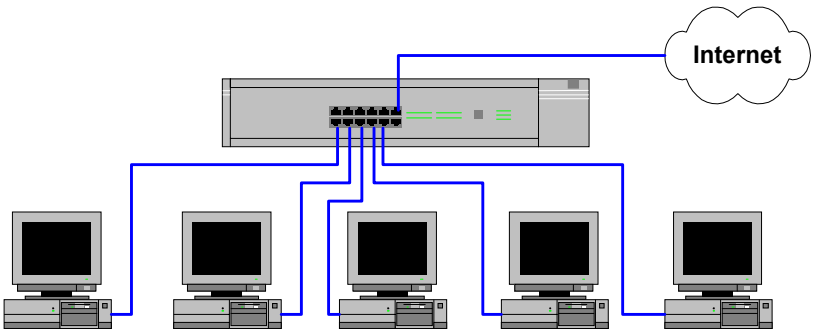


Figura 36. Esquema físico del laboratorio 1

B.3. Materiales

Para esta experiencia se necesita lo siguiente:

- ✓ 1 computador con 2 GB en disco duro libre (mínimo).
- ✓ 1 Hub que soporte cross-over en alguna puerta.
- ✓ 1 cable UTP con conectores machos (para conectar su PC al hub).
- ✓ 1 cable UTP con conectores machos (para el hub a la Internet).
- ✓ 1 CD-ROM con la distribución de Linux Red Hat 6.2 o superior.

B.4. Objetivos

1. Instalar Linux sin ningún servicio habilitado.
2. Verificar el estado de la instalación.

B.5. Requisitos, conceptos y habilidades necesarias

- ✓ Conocimientos básicos en sistemas operativos.
- ✓ Conocimientos básicos en redes ethernet.
- ✓ Modelos de referencia OSI y TCP/IP.
- ✓ Conocimientos básicos de direccionamiento IP.
- ✓ Las recomendaciones del Anexo G. Recomendaciones Generales.

B.6. Bibliografía y referencias

1. Apuntes del curso el54b: “Sistemas de Procesamiento de la Información”.
2. Apuntes del curso el64e: “Redes de Computadores”.
3. Apuntes del curso el647: “interfaces digitales y Periféricos”.
4. Apuntes del curso el649: “Programación y Operación de Computadores”.
5. Apuntes del curso cc51c: “Comunicación de Datos”.
6. Andrew S. Tanenbaum, "Redes de Computadoras", Tercera Edición, Prentice Hall, 1997.

B.7. Plan de acción

Los pasos a seguir en esta experiencia son:

1. Selección del método de Instalación.
2. Configuración inicial de la instalación (idioma, teclado, mouse, tipo de instalación).
3. Establecimiento y formateo de las particiones.
4. Instalación de LILO.
5. Configuración de tarjeta de red y de hora.
6. Establecimiento la password del administrador del sistema, y cuentas de usuario.
7. Selección de paquetes.
8. Instalación de paquetes.

B.8. Sección 0: Conexiones

Paso 1 Se debe verificar todo el material.

Paso 2 Realice las conexiones tal como se muestran en el diagrama físico.

B.9. Sección 1: Selección del método de Instalación

En este documento se explica la instalación desde CD-ROM, que es el método más sencillo de instalación. Los otros métodos de instalación son: NFS, FTP, SMB Shared Volume, Hard Drive o PCMCIA. Para mayor información refiérase al manual.

Es importante destacar que para instalar Linux, es necesario tener cierto conocimiento del hardware del computador en donde se efectuará la instalación. En particular es necesario conocer el nombre del fabricante y el modelo de las componentes del equipo, esto debido a que el asistente de instalación podría realizar consultas al usuario relativas al hardware del equipo.

El asistente de instalación, intenta descubrir cual es la opción correcta, dependiendo del sistema en donde se realiza la instalación, y cuando no descubre esta opción, ofrece la opción por defecto. Es en estas ocasiones en donde el usuario manualmente debe especificar cual es la opción correcta.

Paso 1 Preparación inicial.

Previo a la instalación del sistema, se deben tomar ciertas consideraciones iniciales. El asistente de instalación de Linux es una aplicación que corre sobre Linux. De este modo, es necesario estar en este ambiente previo a la instalación. Esto se puede conseguir de tres maneras distintas:

Paso 2 *Opción 1.-* Disco de Inicio: Se debe utilizar el programa rawrite.exe para crear el disco de inicio. Esta aplicación viene en la distribución de Linux, en el directorio `d:\dosutils` (donde `d:` corresponde al drive asignado al CD-ROM). Para esta opción es necesario tener un disco 3.5' de alta densidad formateado y en blanco. A continuación se muestra un ejemplo de uso suponiendo que la unidad CD-ROM tiene asociada la letra d:

```
D:\>cd \dosutils
D:\dosutils>rawrite.exe
Enter disk image source file name: ..\images\boot.img
Enter target diskette drive: a
Please insert a formatted diskette into drive A: and press -ENTER- :
```

Una vez que se tiene el disco de inicio, se reinicia el computador con el disco de inicio de Linux en la disquetera.

Paso 2 *Opción 2.-* Desde ambiente MS-DOS: En el directorio `d:\dosutils` (donde `d:` corresponde al drive asignado al CD-ROM), se cuenta con el programa `autoboot.bat` que es un archivo batch, que carga el kernel de Linux desde el ambiente MS-DOS.

Para utilizar esta opción, es necesario que el ambiente de trabajo sea MS-DOS puro, no una consola MS-DOS en un ambiente Windows 95. Para conseguir el ambiente MS-DOS puro, al arrancar el computador presione la tecla <F8>, y luego la opción de *Sólo símbolo de sistema a modo a prueba de fallos*. Luego cámbiese al directorio de `d:\dosutils` y ejecute el programa `autoboot.bat`.

Para esto ejecute:

```
C:\>cd d:\dosutils
D:\dosutils>autoboot.bat
```

Paso 2 *Opción 3.-* Utilizando el CD-ROM: Para utilizar este método, la tarjeta madre del computador debe ser sea capaz de utilizar el lector de CD-ROM como unidad de arranque, afortunadamente, la mayoría de las BIOS actuales soportan esta característica.

Para esto, es necesario ingresar a la configuración de la BIOS del equipo, y seleccionar al lector de CD-ROM como unidad de arranque. Dependiendo del tipo de BIOS con que cuente el equipo, esto se puede hacer en la opción del menú principal *"Advanced CMOS Setup"*, o en "*BIOS Feature Setup"* (u otra, que en general es la segunda opción del menú principal). En el menú que corresponda también hay que configurar el lector como primera unidad de arranque. Luego, con el CD-ROM de Linux dentro del lector de CD-ROM, reiniciar el equipo. Un ejemplo de BIOS se ve en la Figura 37.

Punto de Control 1: De acuerdo a la opción escogida, indique una evaluación personal del proceso, en particular, indique el tiempo empleado, y la facilidad de uso:

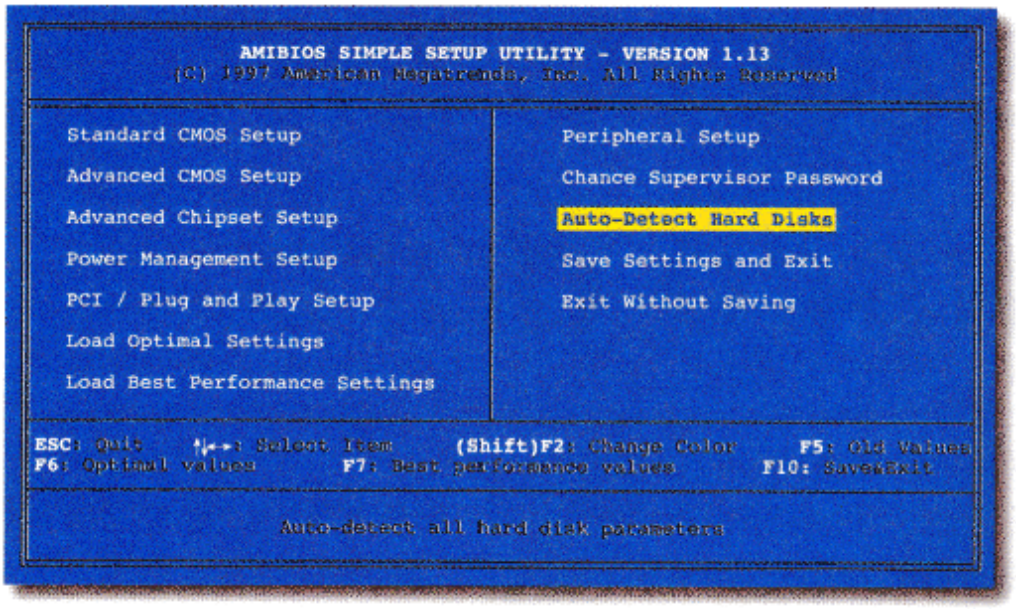


Figura 37. Bios de un computador

B.10. Sección 2: Configuración inicial de la instalación (idioma, teclado, mouse, tipo de instalación)

Paso 1 Selección del idioma.

El asistente de instalación de Linux, permite utilizar varios idiomas para los diálogos que aparecen durante la instalación, se recomienda escoger como idioma el inglés.

Luego presione el botón <next> (<siguiente>).

Paso 2 Selección del teclado.

El asistente ofrece la opción genérica (teclado en inglés, 101 teclas), y el usuario, dependiendo de que tipo de teclado disponga, debe indicar cual es la alternativa correcta. Si su teclado tiene la distribución española o latinoamericana (se reconocen porque poseen la letra “Ñ”) indíquelo al instalador.

Luego presione el botón <next> (<siguiente>).

Paso 3 Selección del mouse.

El asistente ofrece la opción genérica (mouse serial, 2 botones), y el usuario, dependiendo de que tipo de mouse disponga, debe indicar cual es la alternativa correcta. Note que si su mouse es de dos botones debe activar la emulación del tercer botón.

Punto de Control 2: Verifique que la selección del teclado es la correcta. Si escogió teclado en español verifique el uso de la tecla “Ñ” y de los acentos.

Luego presione el botón <next> (<siguiente>).

Paso 4 Tipo de Instalación.

El asistente de instalación, en principio ofrece dos opciones: Instalación (Installing) o Actualización (Upgrading). La opción Actualización es útil en equipos que ya tienen instalados una versión antigua de Linux, puesto que permite actualizar el Sistema Operativo, sin borrar los archivos de datos previos. La opción Instalación, se usa para equipos que no tengan Linux, o cuando no interesa conservar los archivos de versiones previas.

Si se escoge la opción instalación, el asistente de instalación ofrece los siguientes tipos de instalación: Servidor, Estación de Trabajo, o Custom. La opción que permite mayor libertad para el usuario es Custom.

Para los efectos del laboratorio, escoja la opción de Instalación Personalizada (Custom Installing).

Luego presione el botón <next> (<siguiente>).

B.11. Sección 3: Establecimiento y formateo de las particiones

Paso 1 Estableciendo las particiones.

Todos los sistemas operativos son instalados en alguna partición del Disco Duro, de modo que Linux también debe ser instalado en una partición que este dedicada sólo para el sistema operativo.

Para su buen funcionamiento, se necesitan al menos dos particiones, una partición que aloje el sistema operativo (partición principal) y otra partición que se usa para la memoria virtual (partición swap).

Para el caso de dos particiones, la partición principal, o partición *root*, se monta en la raíz del sistema de archivos (filesystem /), y es una partición de tamaño mediano a grande (sobre 1.5 GB). En esta partición se instala el Sistema Operativo, las aplicaciones, las cuentas de los usuarios, etc.

La partición *swap*, se utiliza para emular la memoria RAM del computador, permitiendo así tener una mayor capacidad de procesamiento. Cuando el computador tiene menos de 16 MB de memoria RAM, se recomienda que el tamaño de esta partición sea de al menos 16 MB, para computadores con más memoria, se recomienda que la partición tenga al menos el mismo tamaño que la memoria del computador, y como máximo el doble de la memoria RAM (por ejemplo si el equipo tiene 32 MB de RAM, la partición swap será entre 32 a 64 MB de disco).

También se pueden generar otras particiones, por ejemplo:

- La partición `/boot`, que aloja los archivos necesarios para arrancar la máquina en Linux, para esta partición se recomienda como máximo 16MB.
- La partición `/tmp`, que aloja los archivos y datos temporales de los usuarios, el tamaño de esta partición depende de cada sistema en particular (de 500 MB hacia arriba).
- La partición `/home`, que aloja las cuentas de los usuarios. Para calcular el tamaño de la partición se debe considerar las políticas de la institución sobre espacio en disco para sus usuarios y cantidad de usuarios a mantener. Por ejemplo, 100 usuarios con 50 MB cada uno requiere una partición de 5 GB.
- La partición `/usr/local` que aloja a las aplicaciones. Depende de la cantidad de aplicaciones a instalar, en general mientras más grande mejor.
- La partición `/var/mail` que aloja a los correos de los usuarios, etc. Al igual que la partición `/home`, depende de las políticas de la institución, para el ejemplo (100 usuarios) si se considera que cada usuario conserva 10 MB en correos se necesita 1 GB para la partición.

A menudo, Linux es instalado en computadores que ya poseen un sistema operativo, en efecto, generalmente en cualquier computador IBM compatible, está instalado Windows, en alguno de sus sabores. Debido esto, Linux tiene la capacidad de montar particiones NO-Linux, por ejemplo las particiones FAT 16 o FAT 32 de Windows.

Para establecer las particiones en el modo gráfico debe seleccionar el disco que alojará las particiones, y luego presionar el botón <New>. Esto abre un cuadro de dialogo, en donde se debe especificar el tamaño de la partición y el punto de montaje (esto se refiere a si es la partición `root`, que se denota por un `/`, la partición `swap`, o alguna otra).

En Linux (y también en otros sabores de Unix) el punto de montaje consiste en un directorio libre (sin archivos anidados) en donde se inserta una partición dada al sistema de archivos de Linux.

Para las particiones NO-Linux sólo indique el punto de montaje. Para esto, escoja la partición NO-Linux, presione el botón <Edit> e indique en la opción *Punto de Montaje (mounting point)* cual el directorio en donde se montará la partición.

Luego presione el botón <next> (<siguiente>).

Paso 2 Formateo de las particiones.

En esta etapa se le indica al asistente que particiones se deben formatear. Hay que tener el cuidado de sólo formatear las particiones de Linux, es decir las particiones `/`, `/boot`, `/home`, etc. La partición `swap`, se formatea automáticamente, y las particiones de otros sistemas operativos NO deben ser formateadas.

Punto de Control 3: Verifique que las particiones a formatear. ¿Por qué no se deben formatear las particiones NO-Linux?

_____

_____

_____

_____

Luego presione el botón <next> (<siguiente>).

B.12. Sección 4: Instalación de LILO

Este paso aunque es muy sencillo, es importante hacerlo con cuidado, si falla podría tener problemas en la recuperación de los archivos contenidos en el disco duro.

LILO es el cargador de sistemas operativos que se incluye en Linux, tiene la capacidad de cargar Linux, MS-DOS, Windows 95, Windows NT. En general se instala en el Master Boot Record (MBR) del disco duro principal.

Usted tiene la opción de utilizar o no LILO, se recomienda su uso.

Paso 1 Instalación de LILO.

Seleccione el uso de LILO.

Luego presione el botón <next> (<siguiente>).

Paso 2 Indique donde se instalará LILO.

Puede ser en la partición de Linux que ofrezca el instalador, o en el MBR del disco duro principal. Se recomienda instalar en el MBR.

Luego presione el botón <next> (<siguiente>).

B.13. Sección 5: Configuración de tarjeta de red y de hora

Paso 1 Configuración de red.

Los datos para la configuración de Redes TCP/IP, deben ser proveídos por el administrador de la red. Se necesita conocer lo siguiente:

Tabla 8. Parámetros típicos para redes TCP/IP

IP Address:	Es la dirección IP de la máquina.
Netmask:	Es la máscara de red.
Default Gateway:	Dirección IP del router de la red.
Primary Nameserver:	Dirección IP del servidor de nombres de la red.
Domain Name:	Nombre del dominio de la red.
Host Name:	Nombre de la máquina.

Indique estos valores en el cuadro de diálogo.

Punto de control 4: ¿Qué sucede si no configura la tarjeta de red?

_____
_____
_____
_____

Luego presione el botón <next> (<siguiente>).

NOTA: Si el instalador no le consulta por estos datos, significa que no fue detectada automáticamente la tarjeta de red. Esto puede suceder con algunas tarjetas 3com. Si le sucede esto, realice este paso luego de instalar Linux en el equipo y solicite ayuda al encargado de la sesión. En general el esquema de solución es similar al descrito en el Anexo J. Resolviendo Problemas en la sección J.1. No se reconoce la tarjeta de red 3Com Etherlink III 3c509b bajo Linux.

Paso 2 Selección de hora regional.

Dependiendo de la zona geográfica, se debe establecer el huso horario que corresponda. Por ejemplo, para el caso Chile, se debe escoger Chile/Continental, o Chile/Santiago.

Para esto puede hacerlo escogiendo el huso correspondiente de modo manual, o con el mouse posicionarse sobre el mapa que se muestra cerca de Santiago de Chile, y hacer un clic.

Luego presione el botón <next> (<siguiente>).

B.14. Sección 6: Establecimiento la password del administrador del sistema, y cuentas de usuario

Paso 1 Password de root.

Se debe indicar la password de root (administrador) del sistema. Note que debe indicar la password de root en ambas cajas de texto, una para indicar la password, y en la segunda para confirmarla.

Para fines de laboratorio escriba la password `labISP2000`, en un caso real debe escoger con cuidado la password de root. Se recomienda como mínimo 6 caracteres, y que en ellos se tengan letras mayúsculas y minúsculas, números, y caracteres como `*`, `!`, `%`, etc.

En esta etapa, también se pueden agregar las cuentas de los otros usuarios que utilizaran el sistema.

Para los usuarios debe indicar su login name (nombre de usuario en el sistema), su nombre real, y la password. Al igual que con la password de root, debe indicar la password en la primera caja de texto, y su confirmación en la segunda, y luego presionar el botón <add> (<agregar>)

Se recomienda, agregar al menos un usuario para realizar pruebas y otro para administrar remotamente el equipo.

NOTA: Si el botón <next> (<siguiente>) no está habilitado, puede ser que existe alguna diferencia entre las password indicadas en la caja password y la de verificación.

Luego presione el botón <next> (<siguiente>).

Paso 2 Especificación de identificación de acceso.

Si la red en que se trabaja, cuenta con NIS, consultar al administrador de red, sobre el servidor y los datos necesarios. Si no cuenta con NIS, habilitar la encriptación con MD5, y shadow passwords, con esto será un poco más difícil que los hackers puedan robar las passwords de los usuarios del sistema, o de root.

Luego presione el botón <next> (<siguiente>).

B.15. Sección 7: Selección de paquetes

Paso 1 Selección de paquetes disponibles en la distribución básica de LINUX.

De acuerdo a lo que se requiera, selecciones los paquetes a instalar. Para una selección más fina, escoja la opción “selección individual de paquetes”.

Recuerde que interesa NO instalar los servicios, sólo lo mínimo para utilizar Linux.

En B.20. Anexo: Paquetes que se pueden instalar en la distribución Red Hat 6.2, se muestran las opciones principales que ofrece el instalador.

B.16. Sección 8: Configuración de X Windows

Si el equipo se ocupará como estación de trabajo es recomendable instalar X Windows, si lo ocupará como servidor, puede no ser necesario.

En general con el botón <autoprobe> se puede realizar fácilmente la instalación de X Windows. Se debe determinar el tipo de monitor y la tarjeta de video. Para el monitor es importante indicar las características de velocidad de refresco en la vertical y la horizontal, y para la tarjeta de video el tipo, la marca y la cantidad de memoria.

Paso 1 Primero escoja el monitor de los ofrecidos en la lista.

Paso 2 Escoja la tarjeta de video.

Paso 3 Indique la cantidad de memoria de video.

Paso 4 Presione el botón de selección de modo gráfico y seleccione la resolución deseada.

Si no dispone de la información suficiente para la instalación de X Windows, tendrá que probar varias configuraciones, hasta llegar con la correcta. Si el equipo en que instala Linux tiene Windows 95/98/NT, puede obtener información de la tarjeta de video del *Panel de Control*, haciendo doble clic en *Sistema* y

en la lengüeta *Administrador de dispositivos*, luego haga clic sobre *Adaptadores de pantalla*, escoja el controlador de video que tenga y vea sus *propiedades*.

IMPORTANTE: Recuerde probar la configuración escogida, si esta no funciona, vuelva atrás y pruebe una nueva configuración.

B.17. Sección 9: Instalación de paquetes

Una vez hecho todo lo anterior, presione el botón <siguiente> (<next>). Espere mientras escucha y toma apuntes de la clase.

Cuando termine la copia e instalación de los paquetes el instalador le solicitará que retire las unidades de disco del equipo. En particular retire el CD-ROM y el disco de 3.5' (si es que usó esta opción de instalación). El equipo se reiniciará.

B.18. Sección 10: Verificación inicial

Paso 1 Una vez que arranque el equipo, cuando aparezca la señal

```
LILO:
```

Indique `linux`, si quiere arrancar en Linux, y `dos` para Windows. Escriba "`linux`".

Observe el arranque de la máquina.

Cuando el equipo le solicite el login, escriba root, y luego la password que escogió para root (`labISP2000`).

```
Login: root
Password:
```

Ya ingresó a la máquina por primera vez, tiene instalado Linux, y ahora hay que configurar todos los servicios.

B.19. Cuestionario Final

1. Cuántas particiones necesita Linux para ser instalado, y cuáles son sus funciones.
2. Cuál es la función de LILO.
3. Qué es un punto de montaje de particiones.
4. Cuál es la función de los puntos de montaje.
5. Cuál es el objetivo de indicar los parámetros TCP/IP a la interfaz ethernet.
6. Cuál es la función del usuario root de un sistema Linux (Unix en general).

B.20. Anexo: Paquetes que se pueden instalar en la distribución Red Hat 6.2

- Printer Support: Permite configurar y utilizar una gran cantidad de impresoras.
- X Window System: Ambiente de trabajo gráfico de Unix.
- GNOME: Administrador de ventanas, corre sobre X Windows.
- KDE: Administrador de ventanas, corre sobre X Windows.
- Mail/WWW/News Tools: Herramientas para leer correos electrónicos, ver páginas web, y leer noticias USENET en la red.
- DOS/Windows Connectivity: Permite montar las particiones de DOS y Windows 3.1/95/98.
- Graphics Manipulation: Aplicaciones para gráficos.
- Games: Juegos.

- Multimedia Support: Soporte para tarjetas de sonido, CD-ROM, etc.
- Networked Workstation: Soporte de aplicaciones de red.
- Dialup Workstation: Soporte para conexión por modem.
- News Server: Servidor de Noticias USENET.
- NFS Server: Servidor de NFS, sirve para compartir sistemas de archivos Unix por la red.
- SMB (Samba) Server: Servidor de Samba, ofrece una interfaz transparente al sistema de archivos para estaciones de trabajo Microsoft Windows.
- IPX/Netware (tm) Connectivity: Conectividad para IPX/Netware.
- Anonymous FTP Server: Servidor de FTP anónimo.
- Web Server: Servidor de páginas web.
- DNS Name Server: Servidor de nombres de Internet.
- Postgres (SQL) Server: Motor de bases de datos.
- Network Management Workstation: Herramientas de administración de la red.
- TeX Document Formatting: Lenguaje de macros para producir texto.
- Emacs: Editor de texto.
- Development: Herramientas de desarrollo.
- Kernel Development: Herramientas de desarrollo para el kernel.
- Extra Documentation: Más documentación.
- Utilities: Utilitarios comunes.
- Everything: Instala toda la distribución en el equipo.

Anexo C. Experiencia 2: Administración Básica de Linux

C.1. Resumen

El objetivo de esta experiencia es que los alumnos adquieran cierta destreza en el sistema operativo Linux.

La sesión está completamente orientada al software. En ella se mostrarán:

- Algunos comandos útiles de Linux (algunos son comunes a todas las distribuciones de Linux, y otros son parte de Red Hat 6.2): `ls`, `cd`, `mkdir`, `rmdir`, `crontab`, etc.
- Mecanismos de administración de usuarios: `useradd`, `userdel`, etc.
- El proceso de recompilación del kernel.

Linux provee herramientas gráficas para la mayoría de los procedimientos de administración del sistema, pero en esta experiencia se utilizarán en lo posible las herramientas de línea de comando, que si bien es cierto son más engorrosas, permiten una mejor comprensión de la situación.

Esta experiencia puede resultar tediosa, pero es útil para tener un mínimo conocimiento de las herramientas de Linux. Debe ser realizada en modo superusuario (root).

C.2. Esquemas generales

En esta experiencia interesa mostrar algunas herramientas de administración de Linux. Desde el punto de vista del alumno, usted sólo considerará su computador conectado a un hub a través de la interfaz ethernet, y por otra puerta del hub (aquella que acepta cross-over) se conectará un cable mirando hacia la Internet. El esquema de conexión se ve en la Figura 38. En el esquema se ven los computadores de los alumnos y la Internet conectados a un hub. El esquema físico de la experiencia se ve en la Figura 39.

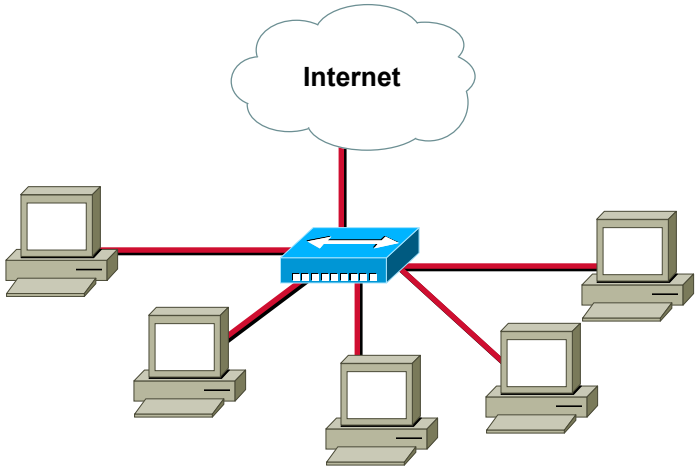


Figura 38. Esquema lógico del laboratorio 2

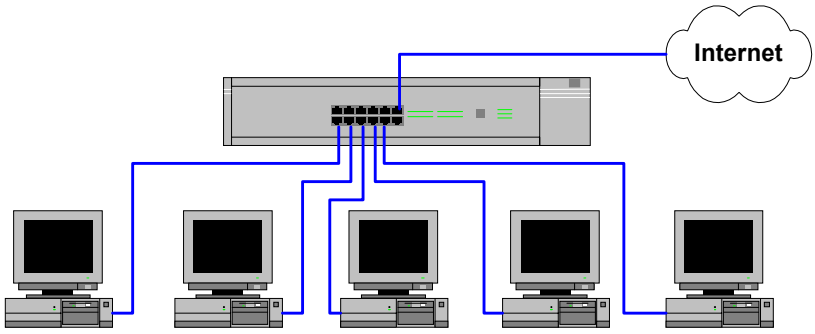


Figura 39. Esquema físico del laboratorio 2

C.3. Materiales

Para esta experiencia se necesita lo siguiente:

- ✓ 1 computador Linux instalado.
- ✓ 1 Hub que soporte cross-over en alguna puerta.
- ✓ 1 cable UTP con conectores machos (para conectar su PC al hub).
- ✓ 1 cable UTP con conectores machos (para el hub a la Internet).
- ✓ 1 CD-ROM con la distribución de Linux Red Hat 6.2 o superior.

C.4. Objetivos

1. Mostrar comandos básicos de Linux, en particular los asociados al sistema de archivos.
2. Mostrar comandos básicos de visualización de archivos.
3. Mostrar comandos de administración de Linux.
4. Mostrar comandos básicos de administración de redes.
5. Mostrar comandos de administración de usuarios.
6. Mostrar el proceso de recompilación del kernel.
7. Mostrar modos de ejecución de procesos en segundo plano.

C.5. Requisitos, conceptos y habilidades necesarias

- ✓ Conocimientos básicos en sistemas de archivos.
- ✓ Conocimientos básicos en sistemas operativos.
- ✓ Conocimientos básicos en redes ethernet.
- ✓ Conocimientos básicos en redes TCP/IP.
- ✓ Conocimientos básicos en resolución de nombres directa y inversa.
- ✓ Las recomendaciones del Anexo G. Recomendaciones Generales.

C.6. Bibliografía y referencias

1. Apuntes del curso el54b: “Sistemas de Procesamiento de la Información”.
2. Apuntes del curso el64e: “Redes de Computadores”.
3. Apuntes del curso el647: “interfaces digitales y Periféricos”.
4. Apuntes del curso el649: “Programación y Operación de Computadores”.
5. Apuntes del curso cc51c: “Comunicación de Datos”.
6. Olaf Kirch (Traducción Proyecto LuCAS), “Guía de Administración de Redes con Linux”, http://lucas.hispalinux.es/htmls/manuales.html, 20 de Mayo de 2000.
7. LDP, Brian Ward, “The Linux Kernel HOWTO”, http://metalab.unc.edu/pub/Linux/docs/HOWTO/other-formats/pdf/Kernel-HOWTO.pdf, 07 de Junio de 2000.

C.7. Plan de acción

Los pasos a seguir en esta experiencia son:

1. Mostrar los comandos básicos de navegación y visualización en el sistema de archivos.
2. Mostrar los comandos de creación y eliminación de directorios.
3. Mostrar los comandos básicos de ayuda en línea.
4. Mostrar los comandos de búsqueda de archivos.
5. Mostrar los comandos básicos de manipulación de archivos.
6. Mostrar los comandos para ver y ajustar la fecha y hora.
7. Mostrar los comandos básicos para administración de redes.
8. Mostrar los comandos básicos de creación y eliminación de cuentas de usuarios.
9. Mostrar los comandos básicos para modificar los atributos de los archivos.
10. Mostrar los comandos básicos de automatización de tareas.
11. Mostrar el mecanismo de compilación de programas.
12. Mostrar el mecanismo de recompilación del kernel.

C.8. Sección 0: Conexiones

Paso 1 Se debe verificar todo el material.

Paso 2 Realice las conexiones tal como se muestran en el diagrama físico.

C.9. Sección 1: Navegación y visualización en el sistema de archivos

Paso 1 Para ver el directorio actual escriba el comando `pwd`

```
[root@almendra /home]# pwd
/home
```

Paso 2 Para ver los archivos del directorio actual escriba el comando `ls`, el comando `ls -l` permite ver algunos atributos de los archivos y con `ls -la` junto con ver los atributos, se ven todos los archivos, es decir, también se ven los archivos ocultos.

```
[root@almendra /home]# ls
httpd  raparede
[root@almendra /home]# ls -l
total 8
drwxr-xr-x    5 root     root         4096 May  6 16:06 httpd
drwx------    4 raparede raparede     4096 May 26 03:20 raparede
[root@almendra /home]# ls -la
total 16
drwxr-xr-x    4 root     root         4096 May  6 16:27 .
drwxr-xr-x   17 root     root         4096 May  6 16:03 ..
drwxr-xr-x    5 root     root         4096 May  6 16:06 httpd
drwx------    4 raparede raparede     4096 May 26 03:20 raparede
```

Punto de Control 1: ¿Para qué sirve el comando `ls -a`?, ¿Cuál es la característica de los archivos ocultos?

Paso 3 Para navegar por los directorios se utiliza el comando `cd`, cámbiese al directorio `/tmp`, y liste los archivos. Note que la salida del `ls` puede ser distinta.

```
[root@almendra /home]# cd /tmp
[root@almendra /tmp]# ls
install.log  orbit-root
```

C.10. Sección 2: Creación y eliminación de directorios

Paso 1 Para crear directorios se utiliza el comando `mkdir` y para eliminarlos el comando `rmdir`. Siga los pasos mostrados en el ejemplo.

```
[root@almendra /tmp]# mkdir directorio
[root@almendra /tmp]# ls
directorio  install.log  orbit-root
[root@almendra /tmp]# cd directorio
 [root@almendra directorio]# mkdir prueba
[root@almendra directorio]# ls -la
total 12
drwxr-xr-x    3 root     root         4096 Jun  4 17:52 .
drwxrwxrwt    9 root     root         4096 Jun  4 17:50 ..
drwxr-xr-x    2 root     root         4096 Jun  4 17:52 prueba
[root@almendra directorio]# rmdir prueba/
```

```
[root@almendra directorio]# ls -la
total 8
drwxr-xr-x    2 root     root         4096 Jun  4 17:52 .
drwxrwxrwt    9 root     root         4096 Jun  4 17:50 ..
```

Punto de Control 2: Intente eliminar un directorio que no esté vacío, ¿Qué sucede?

C.11. Sección 3: Ayuda en línea

Paso 1 Para obtener ayuda en línea se puede utilizar el comando `man`. Este comando se invoca con un argumento que indica sobre que comando se quiere obtener ayuda, en el ejemplo se pide ayuda para el comando `ls`

```
[root@almendra directorio]# man ls
Formatting page, please wait...


LS(1)                           FSF                             LS(1)

NAME
       ls - list directory contents

SYNOPSIS
       ls [OPTION]... [FILE]...

DESCRIPTION
```

C.12. Sección 4: Comandos de búsqueda de archivos

Paso 1 Actualice la base de datos del localizador de archivos. Para dejar el comando corriendo en background, escriba un "`&`" luego del comando `updatedb`. El sistema le informará cuando termine de ejecutar el comando.

```
[root@almendra directorio]# updatedb &

 [1]+  Done                    updatedb
```

Paso 2 Una vez actualizada la base de datos localice todos los archivos que estén relacionados con `localtime`

```
[root@almendra directorio]# locate localtime
/usr/lib/perl5/5.00503/Time/localtime.pm
/usr/lib/perl5/5.00503/i386-linux/auto/POSIX/localtime.al
/usr/lib/perl5/man/man3/Time::localtime.3.gz
/usr/man/man3/localtime.3.gz
/etc/localtime
```

C.13. Sección 5: Comandos de manipulación de archivos

Paso 1 Para copiar archivos se utiliza el comando `cp`. Se debe indicar el archivo de origen y el destino. En el ejemplo se copia el archivo `/mnt/dosc/@tmp/resp2`, usted puede hacer el ejercicio con cualquier archivo. El destino se indica con el carácter punto (`.`), el que se interpreta como el directorio actual.

```
[root@almendra directorio]# cp "/mnt/dosc/@tmp/resp2" .
[root@almendra directorio]# ls -la
total 12
drwxr-xr-x    2 root     root         4096 Jun  4 17:57 .
drwxrwxrwt    9 root     root         4096 Jun  4 17:50 ..
-rwxr-xr-x    1 root     root         1675 Jun  4 17:57 resp2
```

Paso 2 Para mover el archivo a otra posición o cambiarle el nombre se usa el comando `mv`. Se debe indicar el archivo de origen y el destino. En el ejemplo se renombra el archivo `resp2` como `hola`.

```
[root@almendra directorio]# mv resp2 hola
[root@almendra directorio]# ls -la
total 12
drwxr-xr-x    2 root     root         4096 Jun  4 17:57 .
drwxrwxrwt    9 root     root         4096 Jun  4 17:50 ..
-rwxr-xr-x    1 root     root         1675 Jun  4 17:57 hola
```

Paso 3 Para borrar el archivo se usa el comando `rm`. Se debe indicar el archivo o los archivos que se van a eliminar.

```
[root@almendra directorio]# rm hola
rm: remove `hola'? y
[root@almendra directorio]# ls -la
total 8
drwxr-xr-x    2 root     root         4096 Jun  4 17:57 .
drwxrwxrwt    9 root     root         4096 Jun  4 17:50 ..
```

Paso 4 Para ver el contenido de un archivo se usa el comando `more` o el comando `cat`. Se debe indicar el archivo o los archivos que se van a mostrar. La diferencia entre los comandos es que el primero muestra el archivo por páginas, en cambio el segundo lo muestra de sin detenciones, esto se aprecia bien con archivos grandes.

```
[root@almendra directorio]# cd /etc
[root@almendra /etc]# more ytalkrc
turn scrolling on
turn rering on
turn prompt-rering on

[root@almendra /etc]# cat ytalkrc
turn scrolling on
turn rering on
turn prompt-rering on
```

Punto de Control 3: En el directorio `/etc` muestre algún archivo de más de 10 KB con el comando `cat archivo`. Luego ejecute el comando `cat archivo | more`. ¿Cuál es la función del `more`?. ¿Cuál es la función del pipe (`|`)?

Paso 5 Para ver el final de un archivo se usa el comando `tail`, y para ver las últimas n líneas de un archivo el comando `tail -n`. En el ejemplo se muestra el final del archivo `/etc/passwd`, y luego las últimas 5 líneas de `/etc/passwd`. Con `tail -f` se ve como crece un archivo en tiempo real.

```
[root@almendra /etc]# tail passwd
operator:x:11:0:operator:/root:
games:x:12:100:games:/usr/games:
gopher:x:13:30:gopher:/usr/lib/gopher-data:
ftp:x:14:50:FTP User:/home/ftp:
nobody:x:99:99:Nobody:/:
xfs:x:43:43:X Font Server:/etc/X11/fs:/bin/false
gdm:x:42:42::/home/gdm:/bin/bash
piranha:x:60:60::/home/httpd/html/piranha:/dev/null
pvm:x:24:24::/usr/share/pvm3:/bin/bash
raparede:x:500:500:Rodrigo A. Paredes Moraleda:/home/raparede:/bin/bash

[root@almendra /etc]# tail -5 passwd
xfs:x:43:43:X Font Server:/etc/X11/fs:/bin/false
gdm:x:42:42::/home/gdm:/bin/bash
piranha:x:60:60::/home/httpd/html/piranha:/dev/null
pvm:x:24:24::/usr/share/pvm3:/bin/bash
raparede:x:500:500:Rodrigo A. Paredes Moraleda:/home/raparede:/bin/bash
```

C.14. Sección 6: Modificación de atributos de un archivo

Paso 1 Para modificar los atributos de un archivo se usa el comando `chmod`. En Unix y en Linux un archivo puede poseer tres atributos:

- Lectura, atributo r, en decimal es `4` y en binario es `0100`
- Escritura, atributo w, en decimal es 2 y en binario es `0010`
- Ejecución, atributo x, en decimal es 1 y en binario es `0001`

Estos atributos se deben especificar para tres tipos de usuarios:

- Usuario dueño del archivo, caracteres 2, 3 y 4 contando de izquierda a derecha
- Grupo, caracteres 5, 6 y 7 contando de izquierda a derecha
- Otros, caracteres 8, 9 y 10 contando de izquierda a derecha

Para esto cree el archivo de prueba `hola`, utilizando el comando `echo`, que permite imprimir en la salida estándar el argumento del `echo`. Con el caracter `>` se redirecciona la salida estándar del `echo` al archivo `hola`.

```
[root@accounting tmo]# echo hola > hola
[root@accounting tmo]# ls -la
total 12
drwxr-xr-x   2 root     root         4096 Jun  5 11:55 .
drwxr-x--x  24 root     root         4096 Jun  5 11:55 ..
-rw-r--r--   1 root     root            5 Jun  5 11:55 hola
```

Para obtener la ayuda rápida de `chmod`, simplemente escriba el comando con el argumento `--help`

```
[root@accounting tmo]# chmod --help
Usage: chmod [OPTION]... MODE[,MODE]... FILE...
  or:  chmod [OPTION]... OCTAL_MODE FILE...
  or:  chmod [OPTION]... --reference=RFILE FILE...
```

```
  -c, --changes           like verbose but report only when a change is made
  -f, --silent, --quiet   suppress most error messages
  -v, --verbose           output a diagnostic for every file processed
      --reference=RFILE   use RFILE's mode instead of MODE values
  -R, --recursive         change files and directories recursively
      --help              display this help and exit
      --version           output version information and exit

Each MODE is one or more of the letters ugoa, one of the symbols +-= and
one or more of the letters rwxXstugo.

Report bugs to <bug-fileutils@gnu.org>.
```

Paso 2 Para modificar varios atributos a la vez, se combinan los atributos mediante la operación OR. En el ejemplo para el usuario se especifican todos los atributos (r, w y x = 0100_2 OR 0010_2 OR 0001_2 = 0111_2 = 7_{10}), para el grupo se especifican atributos de escritura y ejecución (w y x = 0010_2 OR 0001_2 = 0011_2 = 3_{10}) y para otros sólo se especifica el atributo ejecución (x = 0001_2 = 0001_2 =1_{10})

```
[root@accounting tmo]# chmod 731 hola
[root@accounting tmo]# ls -l
total 4
-rwx-wx--x   1 root     root            5 Jun  5 11:55 hola
```

Para negar los atributos, simplemente en la posición que corresponda coloque un `0`.

Punto de control 4: Como se asigna al archivo `hola` los atributos de lectura para todos, lectura/escritura para el usuario y lectura para el grupo. Verifique con `ls -l` los cambios.

```
[root@almendra /root]# ls -l
total 4
-rw-r--r--    1 root     root            5 Jun  4 19:20 hola
```

Paso 4 Para cambiar el dueño de un archivo se utiliza el comando `chown`. El primer argumento es el nombre del usuario, y el segundo es el archivo o la lista de archivos a modificar. Para verificar el cambio utilice el comando `ls -l`

```
[root@almendra /root]# chown raparede hola
[root@almendra /root]# ls -l
total 4
-rw-r--r--    1 raparede root           5 Jun  4 19:20 hola
```

Paso 5 Para cambiar el grupo de un archivo se utiliza el comando `chgrp`. El primer argumento es el grupo, y el segundo el archivo a modificar, si se indica una lista de archivos, el comando opera sobre toda la lista. Para verificar el cambio utilice el comando `ls -l`

```
[root@almendra /root]# chgrp user hola
[root@almendra /root]# ls -l
total 4
-rw-r--r--    1 raparede user           5 Jun  4 19:20 hola
```

C.15. Sección 7: Visualización y ajuste de fecha y hora

Paso 1 Para visualizar la fecha y hora se usa el comando `date`

```
[root@almendra directorio]# date
Sun Jun  4 17:58:18 CLT 2000
```

Paso 2 Para cambiar la hora se usa el comando `date -s STRING`

```
[root@almendra directorio]# date -s 8:00:00
Sun Jun  4 08:00:00 CLT 2000
```

Paso 3 Para cambiar la fecha se usa el comando `date -s STRING`. Luego de cambiar la fecha se debe ajustar la hora. Luego verifique todo con `date`

```
[root@almendra /root]# date -s 06/04/2000
Sun Jun  4 00:00:00 CLT 2000
[root@almendra /root]# date -s 19:03:31
Sun Jun  4 19:03:31 CLT 2000
[root@almendra /root]# date
Sun Jun  4 19:03:41 CLT 2000
```

C.16. Sección 8: Comandos básicos para administración de redes

Paso 1 Para el estado de las interfaces activas se usa el comando `ifconfig`

```
[root@accounting radacct]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:04:6D:24:4D
          inet addr:200.27.17.35  Bcast:200.27.17.47  Mask:255.255.255.240
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:4594963 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1181 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          Interrupt:9 Base address:0xdc00

eth1      Link encap:Ethernet  HWaddr 00:10:4B:06:18:F9
          inet addr:10.254.0.20  Bcast:10.254.0.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1161808 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3902702 errors:0 dropped:0 overruns:0 carrier:0
          collisions:31 txqueuelen:100
          Interrupt:5 Base address:0x320

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:3924  Metric:1
          RX packets:11965 errors:0 dropped:0 overruns:0 frame:0
          TX packets:11965 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
```

El comando `ifconfig` tiene otros usos, para verlos ejecute `man ifconfig`. Dentro de las funciones de `ifconfig` se tienen las de configurar las interfaces.

Paso 2 Un comando muy utilizado para verificar el estado de otros computadores es el comando `ping`. Siga el ejemplo, la salida debiera ser similar.

```
[root@accounting radacct]# ping gorrion.die.uchile.cl
PING gorrion.die.uchile.cl (146.83.6.74) from 10.254.0.20 : 56(84) bytes of
data.
64 bytes from 146.83.6.74: icmp_seq=0 ttl=245 time=13.8 ms
64 bytes from 146.83.6.74: icmp_seq=1 ttl=245 time=26.5 ms
64 bytes from 146.83.6.74: icmp_seq=2 ttl=245 time=22.0 ms
64 bytes from 146.83.6.74: icmp_seq=3 ttl=245 time=24.9 ms
64 bytes from 146.83.6.74: icmp_seq=4 ttl=245 time=20.4 ms
64 bytes from 146.83.6.74: icmp_seq=5 ttl=245 time=8.7 ms
64 bytes from 146.83.6.74: icmp_seq=6 ttl=245 time=15.2 ms
64 bytes from 146.83.6.74: icmp_seq=7 ttl=245 time=21.7 ms

--- gorrion.die.uchile.cl ping statistics ---
8 packets transmitted, 8 packets received, 0% packet loss
round-trip min/avg/max = 8.7/19.1/26.5 ms
```

Para detener la salida de `ping` presione simultáneamente las teclas <Control> y <C>, esto en la jerga se ve como Ctrl-C.

Note el contenido de las últimas tres líneas. Se muestran las estadísticas del comando. Para el ejemplo se ve que de los 8 paquetes enviados, 8 fueron recibidos y no hubo pérdidas. El valor de `round-trip` indica el tiempo de ida y vuelta de los paquetes mínimo, promedio y máximo.

Paso 3 Para ver la tabla de enrutamiento se utiliza el comando `route`. Siga el ejemplo, la salida debiera ser similar, pero con los valores de la red local.

```
[root@accounting radacct]# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use
Iface
10.254.0.20     0.0.0.0         255.255.255.255 UH    0      0        0 eth1
200.27.17.35    0.0.0.0         255.255.255.255 UH    0      0        0 eth0
200.27.17.32    0.0.0.0         255.255.255.240 U     0      0        0 eth0
10.254.0.0      0.0.0.0         255.255.255.0   U     0      0        0 eth1
127.0.0.0       0.0.0.0         255.0.0.0       U     0      0        0 lo
0.0.0.0         10.254.0.1      0.0.0.0         UG    0      0        0 eth1
```

Punto de Control 5: Pruebe con `route` y compare la salida de `route -n`, ¿cuál es la diferencia?

Paso 4 Para detectar la ruta desde una máquina a otra se utiliza el comando `traceroute`. Siga el ejemplo, la salida debiera ser similar, pero con los valores de la red local.

```
[root@accounting radacct]# traceroute gorrion.die.uchile.cl
traceroute: Warning: gorrion.die.uchile.cl has multiple addresses; using
146.83.6.74
traceroute to gorrion.die.uchile.cl (146.83.6.74), 30 hops max, 38 byte
packets
 1  telephony-adm-gw (10.254.0.1)  2.099 ms  3.320 ms  3.570 ms
 2  172.17.1.2 (172.17.1.2)  7.185 ms  7.053 ms  7.239 ms
 3  200.27.20.90 (200.27.20.90)  7.195 ms  7.073 ms  7.239 ms
 4  net2win-atm-BVI09-gw.firstcom.cl (200.27.18.1)  7.197 ms  6.974 ms
7.236 ms
 5  core1-net2win.firstcom.cl (200.27.101.38)  7.543 ms  7.001 ms  7.238 ms
 6  nap-rdc-atm-0-102-macul.ctc-mundo.net (200.10.224.18)  21.786 ms  21.518
ms  10.878 ms
```

```
 7  200.10.224.254 (200.10.224.254)  10.839 ms  18.014 ms  40.050 ms
 8  ra-uchile.reuna.cl (146.83.240.98)  14.480 ms  18.148 ms  10.881 ms
 9  146.83.17.1 (146.83.17.1)  10.836 ms  14.456 ms  25.466 ms
10  146.83.38.156 (146.83.38.156)  18.130 ms  14.351 ms  10.880 ms
11  200.9.98.129 (200.9.98.129)  149.530 ms *  118.328 ms
12  gorrion.die.uchile.cl (146.83.6.74)  69.175 ms  61.653 ms  50.983 ms
```

Paso 5 Con el comando `nslookup` se puede encontrar la dirección IP dado nombre de host, y el nombre de host dado un número IP. Siga el ejemplo, la salida debiera ser similar. Para salir utilice la palabra clave "`exit`".

```
[22:09 anakena:~/]% nslookup
Default Server:  anakena.dcc.uchile.cl
Address:  192.80.24.83

> gorrion.die.uchile.cl
Server:  anakena.dcc.uchile.cl
Address:  192.80.24.83

Non-authoritative answer:
Name:    gorrion.die.uchile.cl
Addresses:  10.0.25.99, 146.83.6.74

> 146.83.6.74
Server:  anakena.dcc.uchile.cl
Address:  192.80.24.83

Name:    gorrion.die.uchile.cl
Address:  146.83.6.74

> exit
```

C.17. Sección 9: Creación y eliminación de cuentas de usuarios

Paso 1 Para crear un usuario usa el comando `useradd`. Se pueden indicar una gran cantidad de parámetros en la creación del usuario, para ver una ayuda básica, ejecute `useradd` sin parámetros, luego cree el usuario test según el ejemplo.

En el ejemplo se ejecuta `ls -la` en el directorio `/home` previo a la creación del usuario, para enfatizar que el usuario `test` no esta presente en `/home`, que es el directorio por defecto en donde las cuentas de usuario son almacenadas.

```
[root@almendra /root]# useradd
usage: useradd    [-u uid [-o]] [-g group] [-G group,...]
            [-d home] [-s shell] [-c comment] [-m [-k template]]
            [-f inactive] [-e expire ] [-p passwd] [-n] [-r] name
       useradd    -D [-g group] [-b base] [-s shell]
            [-f inactive] [-e expire ]

[root@almendra /home]# ls -la
total 16
drwxr-xr-x    4 root     root         4096 May  6 16:27 .
drwxr-xr-x   17 root     root         4096 May  6 16:03 ..
drwxr-xr-x    5 root     root         4096 May  6 16:06 httpd
drwx------    4 raparede raparede     4096 May 26 03:20 raparede

[root@almendra /root]# useradd -g user -s /bin/tcsh test
```

Paso 2 Verifique la creación del usuario con el comando `ls -la` en el directorio `/home`

```
[root@almendra /home]# ls -la
total 20
drwxr-xr-x    5 root     root         4096 Jun  4 19:13 .
drwxr-xr-x   17 root     root         4096 May  6 16:03 ..
drwxr-xr-x    5 root     root         4096 May  6 16:06 httpd
drwx------    4 raparede user         4096 May 26 03:20 raparede
drwx------    4 test     user         4096 Jun  4 19:13 test
```

Punto de Control 5: Esto también se podría hacer manualmente, y para ello se debe modificar el archivo `/etc/passwd`. Verifique que en el archivo se agrega la línea para el usuario `test`. ¿Qué significan los campos mostrados en el directorio?

Paso 3 Para asignar la password se usa el comando `passwd`

```
[root@almendra /root]# passwd test
Changing password for user test
New UNIX password:
Retype new UNIX password:
passwd: all authentication tokens updated successfully
```

Como todo buen programa de actualización de password, no muestra lo que se escribe, luego cuando escriba por segunda vez la password, cuide de no cometer errores de tipeo.

Paso 4 Otra forma de verificar la existencia del usuario es con el comando `su`. Ejecute el comando `su - test`. Como está operando en modo superusuario no le solicitará la password de test.

```
[root@almendra /root]# su - test
[test@almendra test]$ ls
Desktop
```

Paso 5 El comando `su` también permite asumir el papel de superusuario, esto es útil cuando administra el servidor desde otra máquina, para esto ejecute el comando `su -`. En este caso, como está operando como usuario normal (en particular como el usuario test) se le solicitara la password del superusuario.

```
[test@almendra test]$ su -
Password:
```

Paso 6 Salga del shell (ambiente) del superusuario, esto se hace con el comando `exit`, y ahora salga del shell de test (nuevamente con `exit`).

```
[root@almendra /root]# exit
[test@almendra test]$ exit
```

Paso 7 Para borrar al usuario test ejecute el comando `userdel`. `userdel` permite dos opciones, tal como se ve en la ayuda rápida. Si se ejecuta sin opciones, sólo elimina al usuario del archivo `/etc/passwd`, cuando se usa con la opción `-r` además de eliminarlo del archivo `/etc/passwd`, borra los archivos del usuario.

```
[root@almendra /root]# userdel
usage: userdel [-r] name

[root@almendra /root]# userdel -r test
```

Punto de Control 7: Esto también se podría hacer manualmente, y para ello se debe modificar el archivo `/etc/passwd`. Verifique que en el archivo se eliminó la línea para el usuario `test`. También verifique que el directorio de test en `/home` fue borrado.

C.18. Sección 10: Comandos básicos de automatización de tareas

Paso 1 Para ver la ayuda del comando utilice `man crontab`, y luego `man 5 crontab`. A continuación se muestra parte del manual.

```
[root@almendra /root]# man 5 crontab
Formatting page, please wait...

             field          allowed values
              -----          --------------
              minute         0-59
              hour           0-23
              day of month   1-31
              month          1-12 (or names, see below)
              day of week    0-7 (0 or 7 is Sun, or use names)

       A  field  may  be an asterisk (*), which always stands for
       ``first-last''.
```

Paso 2 Para ver el estado actual de la tabla `crontab`, ejecute `crontab -l`

```
[root@almendra /root]# crontab -l
no crontab for root
```

Paso 3 Para agregar acciones a la tabla `crontab`, ejecute `crontab -e`. En el ejemplo se agrega el comando `updatedb` a las 02:00 a.m. todos los días, de modo de tener actualizada la base de datos de localización de archivos del sistema de archivos. Note que el carácter **#** se utiliza para indicar comentarios. El carácter ***** se utiliza para indicar a todas las opciones, por ejemplo, el ***** en la tercera posición significa todos los días del mes.

```
[root@almendra /root]# crontab -e
no crontab for root - using an empty one
ccrontab: installing new crontab

# cron a las 2:00 todos los dias del año
0 2 * * * /usr/bin/updatedb
```

Paso 4 Para verificar la modificación del estado actual de la tabla `crontab`, ejecute `crontab -l`

```
[root@almendra /root]# crontab -l
# DO NOT EDIT THIS FILE - edit the master and reinstall.
# (/tmp/crontab.1151 installed on Sun Jun  4 19:10:00 2000)
# (Cron version -- $Id: crontab.c,v 2.13 1994/01/17 03:20:37 vixie Exp $)
# cron a las 2:00 todos los dias del año
0 2 * * * /usr/bin/updatedb
```

C.19. Sección 11: Mecanismo de compilación de programas

Paso 1 Escriba el programa `hola.c`, para eso ejecute `vi hola.c`. Siga las instrucciones indicadas:

```
[root@almendra /root]# vi hola.c
```

Presione la tecla <i> y luego escriba lo siguiente. Cuide de escribir el programa `hola.c` sin errores de tipeo:

```
#include <stdio.h>

main(){
  printf("hola, que tal el laboratorio\n");
}
```

Paso 2 Compile el programa `hola.c`, para eso ejecute `gcc –o hola hola.c`. La opción `–o` sirve para indicar cual es el archivo ejecutable (en la jerga se dice binario) destino.

```
[root@almendra /root]# gcc -o hola hola.c
```

Paso 3 Ejecute programa `hola`, para eso escriba "`hola`".

```
[root@almendra /root]# hola
bash: hola: command not found
```

¿Qué fallo?

1.- Verifique que el programa es ejecutable.
2.- Verifique que el programa esta en el path de programas ejecutables.

1.-
```
[root@almendra /root]# ls -l
total 16
-rwxr-xr-x    1 root     root        11750 Jun  4 19:38 hola
-rw-r--r--    1 root     root           74 Jun  4 19:34 hola.c
```

Es ejecutable (atributo x).

2.-
```
[root@almendra /root]# set
PATH=/usr/kerberos/bin:/usr/kerberos/bin:/sbin:/bin:/usr/sbin:/usr/bin:/usr/X1
1R6/bin:/root/bin
```

No esta el directorio /root en PATH

Paso 3 Ejecute programa `hola`, para eso ejecute `./hola`

```
[root@almendra /root]# ./hola
hola, que tal el laboratorio
```

C.20. Sección 12: Mecanismo de recompilación del kernel

El proceso hay que hacerlo como root. Actualmente no es tan necesario recompilar el kernel, puesto que se pueden cargar módulos en forma independiente y en demanda, pero se muestra el mecanismo como cultura general.

Paso 1 Respaldo del directorio `/boot`. Es importante respaldar este directorio, puesto que si se comete un error en la recompilación del kernel, se puede recuperar el kernel anterior de este directorio. En este caso el kernel se va a respaldar en la partición de Windows 95 del computador. Se puede escoger cualquier otro directorio para realizar el respaldo.

```
[root@almendra /root]# cd /mnt/dosc/
```

Verificando que haya un directorio para respaldo de linux

```
[root@almendra dosc]# ls
@tmp                  autoexec.m01  ffastun.ffl   msdos.sys     system.1st
Apps                  biosid.tmp    ffastun.ffo   netlog.txt    tek
Archivos de programa  bootlog.prv   ffastun0.ffx  recycled      videorom.bin
Lang                  bootlog.txt   install.log   scandisk.log  windows
Mis documentos        command.com   io.sys        setuplog.old  www
Real                  config.sys    liprefs.js    setuplog.txt
Videos                detlog.old    mp3.old       setupxlg.txt
autoexec.001          detlog.txt    msdos.---     suhdlog.---
autoexec.bat          ffastun.ffa   msdos.bak     suhdlog.dat
```

No se encontró el directorio para respaldos de linux, hay que hacer uno. Luego entre al directorio construido, y cree un directorio con nombre `boot`. Esto es para no olvidar de donde vienen los archivos respaldados. Entre al directorio `boot`, y copie los archivos del directorio `/boot`

```
[root@almendra dosc]# mkdir linux
[root@almendra dosc]# cd linux/
[root@almendra linux]# mkdir boot
[root@almendra linux]# cd boot
[root@almendra boot]# cp /boot/* .
cp: /boot/lost+found: omitting directory
```

Si se reporta un error como el mostrado en el ejemplo, no se preocupe. Vuelva a `/boot`. Guarde el listado original (para recuperar los links si corresponde), siga las instrucciones del ejemplo:

```
[root@almendra boot]# cd /boot
[root@almendra /boot]# ls -la > listado
[root@almendra /boot]# mv listado /mnt/dosc/linux/boot/
```

Vuelva a `/mnt/dosc/linux` (el directorio de respaldo de linux). Para recordar la fecha de la generación del kernel renombre el directorio con la fecha que corresponda, y luego verifique el cambio:

```
[root@almendra linux]# mv boot boot.20000606
[root@almendra linux]# ls -la
total 12
drwxr-xr-x    3 root     root         4096 Jun  6 09:10 .
drwxr-xr-x   15 root     root         4096 Jun  6 08:56 ..
drwxr-xr-x    2 root     root         4096 Jun  6 09:05 boot.20000606
```

Paso 2 Respaldo de los módulos que ya están compilados. Para esto cámbiese al directorio `/lib`, consolide los archivos del directorio `/lib/modules` como `modules.fecha_actual`, y comprima el archivo consolidado:

```
[root@almendra /boot]# cd /lib
[root@almendra /lib]# tar -cvf modules.20000606 modules
[root@almendra /lib]# gzip modules.20000606
```

Construya el directorio `/mnt/dosc/linux/lib` y mueva el archivo consolidado al directorio creado.

```
[root@almendra /lib]# mkdir /mnt/dosc/linux/lib
[root@almendra /lib]# mv modules.20000606.gz /mnt/dosc/linux/lib
```

Antes de borrar el contenido del directorio `/modules`, renombre el directorio modules a `modules.fecha`, como medida de seguridad para recuperar rápido los módulos antiguos si ocurre un error.

```
[root@almendra /lib]# mv modules modules.20000606
```

Cree el directorio `/modules` y verifique la situación, para evitar que salgan muchas líneas, filtre la entrada con el comando `grep`.

```
[root@almendra /lib]# mkdir modules
[root@almendra /lib]# ls -la |grep mo
```

Punto de Control 8: ¿Cuál es el riesgo de generar mal el kernel, cómo se puede salvar esta situación?

_____

_____

_____

_____

Paso 3 Ahora viene la parte importante: configurar el kernel. Cámbiese al directorio `/usr/src`, y verifique que estén instaladas las fuentes del kernel.

```
[root@almendra /lib]# cd /usr/src/
[root@almendra src]# ls -la
total 16
drwxr-xr-x    4 root     root         4096 May  6 16:15 .
drwxr-xr-x   22 root     root         4096 May  6 16:15 ..
lrwxrwxrwx    1 root     root           12 May  6 16:15 linux -> linux-2.2.14
drwxr-xr-x   18 root     root         4096 May  6 16:15 linux-2.2.14
drwxr-xr-x    7 root     root         4096 May  6 16:05 redhat
```

Note el link linux, si no lo encuentra baje las fuentes de la Internet y descomprímalas en este directorio. Las fuentes las puede obtener desde ftp.kernel.org/pub/linux/kernel/vx.y donde `x` e `y` son los números de

la versión `x` es el mayor e `y` el menor, ejemplo v2.2, fíjese que numero menor sea par, los impares corresponden a kernels en desarrollo en cambio los pares son para kernels estables.

Cámbiese al directorio linux.

```
[root@almendra src]# cd linux
```

Ahora se puede configurar el kernel de varias maneras distintas, observe la Tabla 9.

Tabla 9. Tipos de configuración de kernels

Llamada a make	Tipo de configuración
`make config`	Configurador manual
`make menuconfig`	Configurador de menú de texto
`make xconfig`	Configurador de menú X windows

Se recomienda `make menuconfig` o `make xconfig`

Si dispone de ambiente X windows, utilice la opción `xconfig` (ver Figura 40), si no utilice la opción `menuconfig`

```
[root@almendra linux]# make xconfig
```

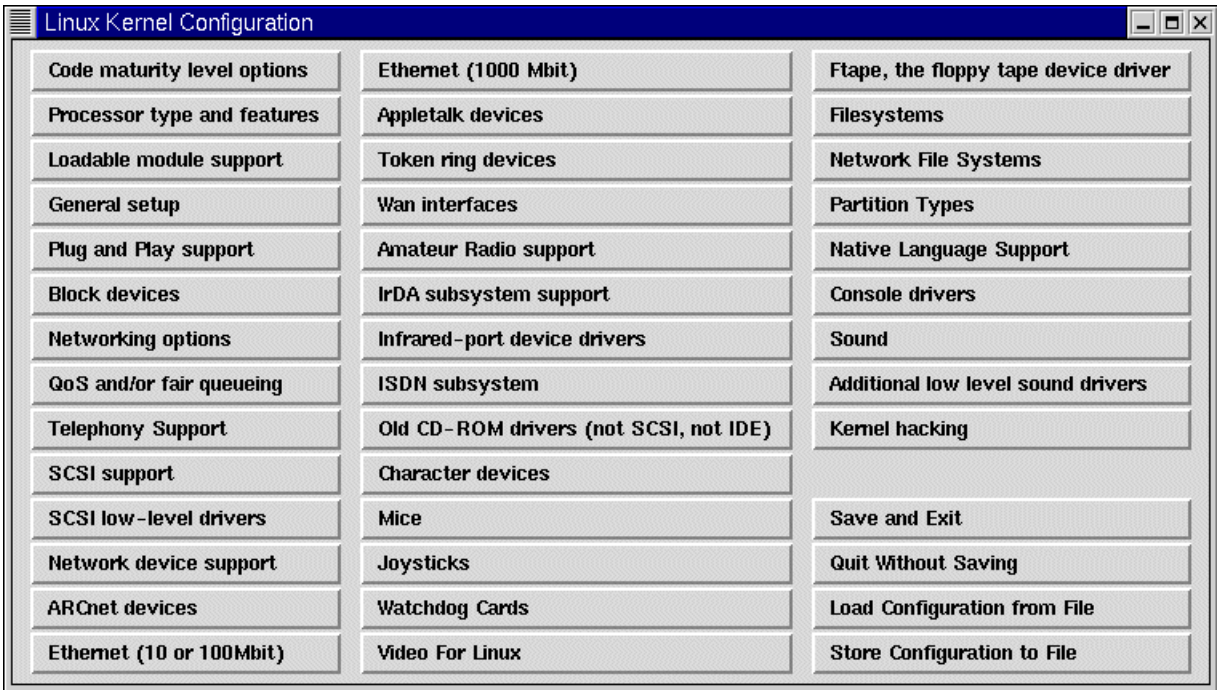


Figura 40. Menú de configuración del kernel, ambiente X windows

Recorra el menú completo y escoja las opciones, de acuerdo a su sistema y necesidades. Recuerde leer la ayuda (help) para entender lo que esta haciendo.

Para la mayoría de las opciones se permite tres opciones: y = Yes, m = Module y n = No.

- Yes significa que la opción se compila y se agrega al kernel.
- Module ignifica que la opción se compila pero no se agrega al kernel, sino que se agrega en demanda.
- No significa que no se compila.

Algunos importantes se ven en la Tabla 10.

Tabla 10. Opciones importantes del configurador de kernel

Processor type and features	Indique su procesador, indique si tiene o no coprocesador matemático.
General support	Habilite la opción Networking support (indique y), habilite TCP/IP.
Networkig options	Habilite IP: Advanced Router, IP:verbose route monitoring, IP: large routing tables.
Network device support	Habilite PPP y SLIP.
Filesystems	Habilite Second extended, msdos, /proc, NFS, ISO9660, y todos los FAT (compatibles con Microsoft Windows).

Una vez hecho el proceso de configuración, hay que configurar las dependencias y limpiar las versiones anteriores.

```
[root@almendra linux]# make dep
[root@almendra linux]# make clean
```

Luego de esto viene la parte más fuerte en cálculo para el computador, compilar el kernel.

```
[root@almendra linux]# make bzImage
```

La última línea es:

```
make[1]: Leaving directory `/usr/src/linux-2.2.14/arch/i386/boot'
```

Cámbiese al directorio donde se genera la imagen del kernel:

```
[root@almendra linux]# cd arch/i386/boot/
```

Mueva la imagen del kernel a la partición de arranque, esta información la puede obtener del archivo `/etc/lilo.conf`. NO borre el kernel anterior. El kernel de linux se indica en el registro cuyo label (etiqueta) es linux.

```
[root@almendra boot]# more /etc/lilo.conf
boot=/dev/hda
map=/boot/map
install=/boot/boot.b
prompt
timeout=50
linear
default=dos

image=/boot/vmlinuz-2.2.14-5.0smp
      label=linux
      read-only
      root=/dev/hda5

image=/boot/vmlinuz-2.2.14-5.0
      label=linux-up
```

```
      read-only
      root=/dev/hda5

other=/dev/hda1
      label=dos
```

Como se aprecia en el archivo, la partición de arranque de linux es `/boot`, esto depende de cada máquina.

```
[root@almendra boot]# mv bzImage /boot/bzImage
```

Edite el archivo `/etc/lilo.conf` para indicar la nueva posición de la imagen del kernel, se recomienda que agregue un nuevo registro para el nuevo kernel, de modo de que si falla el kernel, se pueda recuperar sin problemas. Edite el archivo con el editor de su preferencia, en el ejemplo se editó con `vi`, observe que se agrega el nuevo kernel y se cambia el label del kernel antiguo.

```
[root@almendra boot]# vi /etc/lilo.conf
[root@almendra boot]# more /etc/lilo.conf
boot=/dev/hda
map=/boot/map
install=/boot/boot.b
prompt
timeout=50
linear
default=dos

image=/boot/bzImage
      label=linux
      read-only
      root=/dev/hda5

image=/boot/vmlinuz-2.2.14-5.0smp
      label=linux-old
      read-only
      root=/dev/hda5

image=/boot/vmlinuz-2.2.14-5.0
      label=linux-up
      read-only
      root=/dev/hda5

other=/dev/hda1
      label=dos
```

Instale el nuevo sector de arranque del disco duro, para eso utilice el comando `lilo`

```
[root@almendra boot]# lilo
Added linux
Added linux-old
Added linux-up
Added dos *
```

Note que `lilo` instala todas las imágenes de arranque que dispone el computador, las linux y las no linux.

Paso 5 Reinicie la máquina. Si esta en X windows, presione Ctrl-Alt-Del para salir de X windows, y luego Crtl-Alt-Supr para reiniciar la máquina.

Paso 6 Si dejo alguna opción como módulo, lo que es muy probable, tendrá que compilar los módulos, esto se hace como sigue:

```
[root@almendra /root]# cd /usr/src/linux
[root@almendra linux]# make modules
[root@almendra linux]# make modules_install
```

En algunas distribuciones, tendrá que copiar el directorio de los módulos con otros nombres, para descubrir el nombre del kernel que está ejecutando utilice `uname -r`. En el caso del ejemplo, el kernel tiene la versión 2.2.14-5.0smp, por lo cual se hace el siguiente comando (la opción `-r` de `cp`, es para que los subdirectorios se copien recursivamente):

```
[root@almendra modules]# cp -r 2.2.14-5.0 2.2.14-5.0smp
```

Ahora está completo el proceso, reinicie la máquina. Si luego de esto tiene problemas, tiene dos opciones, repetir el proceso de compilación y corregir los errores, o recuperar las versiones antiguas.

C.21. Cuestionario Final

1. Qué es un sistema de archivos.
2. Diseñe (no implemente, sólo diseñe) un mecanismo para respaldar y eliminar una cuenta.
3. Diseñe (no implemente, sólo diseñe) un mecanismo para recuperar y reconstruir una cuenta eliminada.
4. Diseñe (no implemente, sólo diseñe) un mecanismo que monitoree el estado de una conexión de acuerdo a la siguiente premisa: Después de 20 minutos de que el enlace está caído, envíe un correo al root local. Suponga que conoce al menos una dirección IP al otro lado del enlace.
5. Cuál es la función del kernel.

Anexo D. Experiencia 3: Habilitación de Servicios Internet I

D.1. Resumen

El objetivo de esta experiencia es poner en marcha algunos de los servicios fundamentales de un ISP. El primer servicio que se instalará será el DNS, que es el eje rector del resto de los servicios Internet, y luego debido a su gran popularidad, pondrá en marcha el servicio WWW. Adicionalmente se instalará el servicio Telnet, FTP y FTP anónimo.

D.2. Esquemas generales

En esta experiencia interesa mostrar algunos de los servicios de Internet. Para mostrar el esquema de cliente servidor, para esta experiencia se separarán los computadores en pares, donde uno de ellos será el ISP y el otro solicitará servicios. La nube Internet se refiere a los otros pares de computadores, esto para hacer más interesante la experiencia. El esquema de conexión se ve en la Figura 41. El esquema físico de la experiencia se ve en la Figura 42.

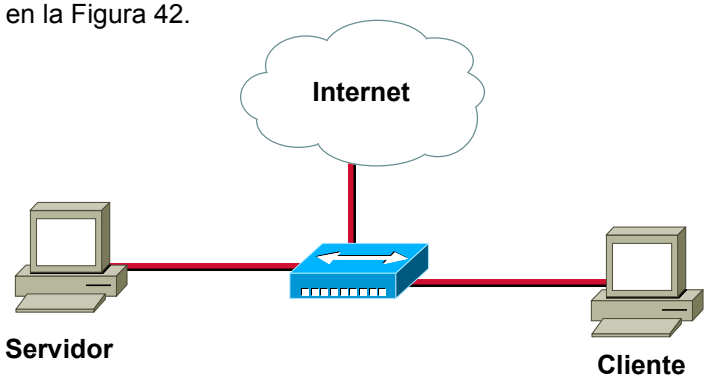


Figura 41. Esquema lógico experiencia 3

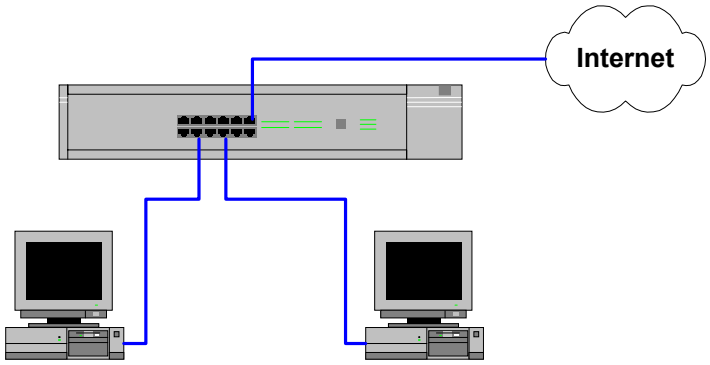


Figura 42. Esquema físico experiencia 3

D.3. Materiales

Para esta experiencia se necesita lo siguiente:

- ✓ 1 Computador para habilitarlo como ISP mínimo.
- ✓ 1 Computador habilitado como cliente dedicado.
- ✓ 3 Cables UTP con conectores machos.
- ✓ 1 Cable UTP cruzado con conectores machos (respaldo si falla la puerta cross-over del hub).
- ✓ 1 Hub que soporte cross-over en alguna puerta.
- ✓ 1 CD-ROM con la distribución de Linux Red Hat 6.2 o superior.

D.4. Objetivos

1. Instalación y configuración del servicio DNS.
2. Instalación y configuración del servicio WWW.
3. Instalación y configuración del servicio Telnet.
4. Instalación y configuración del servicio FTP y FTP anónimo.

D.5. Requisitos, conceptos y habilidades necesarias

- ✓ Conocimientos básicos de sistemas operativos.
- ✓ Noción de red de computadores.
- ✓ Paradigma cliente/servidor.
- ✓ Noción de diseño modular.
- ✓ Modelos de referencia OSI y TCP/IP.
- ✓ Conocimientos básicos de direccionamiento IP.
- ✓ Conocimientos básicos en sistemas de archivos.
- ✓ Conocimientos básicos en redes TCP/IP.
- ✓ Conocimientos básicos en resolución de nombres directa y inversa.
- ✓ Las recomendaciones del Anexo G. Recomendaciones Generales.

D.6. Bibliografía y referencias

1. Apuntes del curso el54b: “Sistemas de Procesamiento de la Información”.
2. Apuntes del curso el64e: “Redes de Computadores”.
3. Apuntes del curso el647: “interfaces digitales y Periféricos”.
4. Apuntes del curso el649: “Programación y Operación de Computadores”.
5. Apuntes del curso cc51c: “Comunicación de Datos”.
6. Andrew S. Tanenbaum, "Redes de Computadoras", Tercera Edición, Prentice Hall, 1997.
7. Olaf Kirch (Traducción Proyecto LuCAS), “Guía de Administración de Redes con Linux”, http://lucas.hispalinux.es/htmls/manuales.html, 20 de Mayo de 2000.
8. LDP, Anton Chuvakin, “”Pocket” ISP based on RedHat Linux”, http://metalab.unc.edu/pub/Linux/docs/HOWTO/other-formats/pdf/ISP-Setup-RedHat.pdf, 07 de Junio de 2000.
9. LDP, Brian Ward, “The Linux Kernel HOWTO”, http://metalab.unc.edu/pub/Linux/docs/HOWTO/other-formats/pdf/Kernel-HOWTO.pdf, 07 de Junio de 2000.

D.7. Plan de acción

Los pasos a seguir en esta experiencia son:

1. Instalación y configuración del DNS en modalidad cache.
2. Configuración del DNS como maestro de zona.
3. Instalación y configuración de httpd.
4. Instalación de sitios virtuales.
5. Instalación de telnet.
6. Instalación del servicio FTP.
7. Instalación del servicio FTP anónimo.

D.8. Sección 0: Conexiones

Paso 1 Se debe verificar todo el material.

Paso 2 Realice las conexiones tal como se muestran en el diagrama físico.

D.9. Sección 1: Algo de seguridad

La experiencia hay que realizarla como usuario root.

Asignando el grupo `wheel` para los comandos sensibles:

Paso 1 Edite el archivo `/etc/group` y modifique o agregue la siguiente línea (donde dice SuLogin indique su login name).

```
wheel:x:10:root,SuLogin
```

Ejemplo:

```
[root@almendra /etc]# vi group

-----------------------------------------------------------------------
wheel:x:10:root,raparede
-----------------------------------------------------------------------
```

Paso 2 Cambie el grupo del comando su a `wheel`

```
[root@almendra /etc]# cd /bin
[root@almendra /bin]# chgrp wheel su
```

Paso 3 Asigne los permisos de ejecución

```
[root@almendra /bin]# chmod 4750 /bin/su
```

Con esto solo los usuarios del grupo wheel pueden ocupar el comando `su`

Restringiendo el uso del comando `cron`

Para que sólo los usuarios root y Usted puedan programar comandos `cron` modifique el archivo `/etc/cron.allow` con los nombres de los usuarios permitidos, en este caso root y Usted.

Paso 4 Edite el archivo `/etc/cron.allow`

```
[root@almendra /bin]# cd /etc
[root@almendra /etc]# vi cron.allow

-----------------------------------------------------------------------
root
raparede
-----------------------------------------------------------------------
```

Paso 5 Verifique el archivo `/etc/cron.allow`

```
[root@almendra /etc]# more cron.allow
root
raparede
```

D.10. Sección 2: Instalación de un DNS en modalidad cache

En el ejemplo se utilizará el dominio `paredesmoraleda.cl`, esto se debe cambiar de a cuerdo al dominio específico con que este trabajando.

Paso 1 Monte el cdrom.

```
[root@almendra /root]# mount /mnt/cdrom/
```

Paso 2 Instalación de los paquetes:

Cámbiese al directorio de los RPMS, e instale los RPM de `bind`.

```
[root@almendra /root]# cd /mnt/cdrom/RedHat/RPMS/
[root@almendra RPMS]# rpm -i bind-8.2.2_P5-9.i386.rpm
[root@almendra RPMS]# rpm -i bind-utils-8.2.2_P5-9.i386.rpm
```

Si sale un mensaje del tipo `package nombre_paquete is already installed` significa que el paquete ya ha sido previamente instalado. Puede dejar esto tal cual está, o desinstalar el paquete con `rpm -e nombre_paquete` y luego volver a instalar con `rpm -i nombre_paquete.i386.rpm`

Configuración:

Paso 3 Escriba el programa `/etc/named.conf`

```
[root@almendra RPMS]# cd /etc
[root@almendra /etc]# vi named.conf

-----------------------------------------------------------------------
// Config file for caching only name server

options {
        directory "/var/named";

        // Uncommenting this might help if you have to go through a
        // firewall and things are not working out:

        // query-source port 53;
};

zone "." {
        type hint;
        file "root.hints";
};

zone "0.0.127.in-addr.arpa" {
        type master;
        file "pz/127.0.0";
};
-----------------------------------------------------------------------
```

La línea "`directory`" indica cual es el directorio donde buscar los archivos. Todos los nombres de archivo son relativos a él. Luego `pz` (que viene del inglés primary zone) es un directorio bajo `/var/named`, es decir es `/var/named/pz`

Paso 4 Escriba el programa `/var/named/root.hints` (si el directorio `/var/named` no existe créelo con `mkdir /var/named`).

```
[root@almendra /etc]# cd /var
[root@almendra /var]# mkdir /var/named
[root@almendra /var]# cd named/
[root@almendra named]# vi root.hints

-----------------------------------------------------------------------
;
; There might be opening comments here if you already have this file.
```

```
; If not don't worry.
;
.                       6D IN NS        G.ROOT-SERVERS.NET.
.                       6D IN NS        J.ROOT-SERVERS.NET.
.                       6D IN NS        K.ROOT-SERVERS.NET.
.                       6D IN NS        L.ROOT-SERVERS.NET.
.                       6D IN NS        M.ROOT-SERVERS.NET.
.                       6D IN NS        A.ROOT-SERVERS.NET.
.                       6D IN NS        H.ROOT-SERVERS.NET.
.                       6D IN NS        B.ROOT-SERVERS.NET.
.                       6D IN NS        C.ROOT-SERVERS.NET.
.                       6D IN NS        D.ROOT-SERVERS.NET.
.                       6D IN NS        E.ROOT-SERVERS.NET.
.                       6D IN NS        I.ROOT-SERVERS.NET.
.                       6D IN NS        F.ROOT-SERVERS.NET.

G.ROOT-SERVERS.NET.     5w6d16h IN A    192.112.36.4
J.ROOT-SERVERS.NET.     5w6d16h IN A    198.41.0.10
K.ROOT-SERVERS.NET.     5w6d16h IN A    193.0.14.129
L.ROOT-SERVERS.NET.     5w6d16h IN A    198.32.64.12
M.ROOT-SERVERS.NET.     5w6d16h IN A    202.12.27.33
A.ROOT-SERVERS.NET.     5w6d16h IN A    198.41.0.4
H.ROOT-SERVERS.NET.     5w6d16h IN A    128.63.2.53
B.ROOT-SERVERS.NET.     5w6d16h IN A    128.9.0.107
C.ROOT-SERVERS.NET.     5w6d16h IN A    192.33.4.12
D.ROOT-SERVERS.NET.     5w6d16h IN A    128.8.10.90
E.ROOT-SERVERS.NET.     5w6d16h IN A    192.203.230.10
I.ROOT-SERVERS.NET.     5w6d16h IN A    192.36.148.17
F.ROOT-SERVERS.NET.     5w6d16h IN A    192.5.5.241
--------------------------------------------------------------------
```

Paso 5 La siguiente sección del archivo `named.conf` es `pz/127.0.0`, escriba el archivo `pz/127.0.0`

```
[root@almendra named]# mkdir pz
[root@almendra named]# cd pz
[root@almendra pz]# vi 127.0.0
```

Tenga cuidado con los errores tipográficos.

El caracter ";" se utiliza para los comentarios, luego cualquier texto que se escriba luego del ";" no se considera.

```
--------------------------------------------------------------------
@                           IN          SOA         ns.paredesmoraleda.cl.
root.paredesmoraleda.cl. (
                              7       ; numero de serie
                              360000  ; refresco cada 100 horas
                              3600    ; reintentos cada 1 hora
                              3600000 ; expiración del sitio en 42 días
                              360000  ; TTL por defecto de las consultas
)
                IN      NS      ns.paredesmoraleda.cl.
1               IN      PTR     localhost.
--------------------------------------------------------------------
```

Cada vez que modifique este archivo incremente el valor del número de serie, de modo que los servidores secundarios vean el aumento en el número de serie y actualicen sus tablas.

Paso 6 Edite el archivo `/etc/resolv.conf`

```
[root@almendra pz]# vi /etc/resolv.conf

-----------------------------------------------------------------
domain paredesmoraleda.cl
search paredesmoraleda.cl
nameserver 127.0.0.1
-----------------------------------------------------------------
```

- La línea `domain` indica el nombre del dominio.
- La línea `search` indica cual es el dominio por defecto en donde se deben buscar las máquinas.
- La línea `nameserver` especifica la dirección IP del servidor de nombres.

Paso 7 Edite la línea `order` del archivo `/etc/host.conf`

```
[root@almendra pz]# vi /etc/host.conf

order hosts, bind
```

Paso 8 Ejecute `named`

Nota: `ndc` es el programa name daemon control.

```
[root@almendra pz]# /usr/sbin/ndc start
```

Para ver el estado de la ejecución, en otra ventana (esto servirá para la depuración de errores) observe el estado del `log` de mensajes.

```
[root@almendra pz]# tail -f /var/log/messages
Jun 14 23:39:26 almendra named[1770]: starting.  named 8.2.2-P5 Mon Feb 28
10:17:53   EST   2000   ^Iroot@porky.devel.redhat.com:/usr/src/bs/BUILD/bind-
8.2.2_P5/src/bin/named
Jun 14 23:39:26 almendra named[1770]: hint zone "" (IN) loaded (serial 0)
Jun 14 23:39:26 almendra named[1770]: Zone "0.0.127.in-addr.arpa" (file
pz/127.0.0): No default TTL set using SOA minimum instead
Jun 14 23:39:26 almendra named[1770]: master zone "0.0.127.in-addr.arpa" (IN)
loaded (serial 7)
Jun 14 23:39:26 almendra named[1770]: listening on [127.0.0.1].53 (lo)
Jun 14 23:39:26 almendra named[1770]: listening on [192.168.3.1].53 (eth0)
Jun 14 23:39:26 almendra named[1770]: listening on [192.168.4.1].53 (eth0:0)
Jun 14 23:39:26 almendra named[1770]: Forwarding source address is
[0.0.0.0].1026
Jun 14 23:39:26 almendra named[1771]: Ready to answer queries.
```

Paso 9 Probando el servicio. Siga los pasos mostrados en la guía.

```
[root@almendra pz]# nslookup
Default Server:  localhost
Address:  127.0.0.1

> www.die.uchile.cl
Server:  localhost
Address:  127.0.0.1

Name:    www.die.uchile.cl
Address:  146.83.12.26

> www.die.uchile.cl
Server:  localhost
```

```
Address:  127.0.0.1

Non-authoritative answer:
Name:    www.die.uchile.cl
Address:  146.83.12.26

> 146.83.12.26
Server:  localhost
Address:  127.0.0.1

Name:    ulises.dic.uchile.cl
Address:  146.83.12.26

> ulises.dic.uchile.cl
Server:  localhost
Address:  127.0.0.1

Non-authoritative answer:
Name:    ulises.dic.uchile.cl
Address:  146.83.12.26
```

Punto de Control 1: ¿Qué entiende por respuesta autorizada y no autorizada?

Paso 10 Se puede mejorar un poco la configuración con lo siguiente:

```
[root@almendra /etc]# more named.conf

---------------------------------------------------------------------
// Config file for caching only name server

options {
        directory "/var/named";

        forward first;
        forwarders {
                200.9.97.3;
                200.9.100.1;
                200.27.2.2;
                200.27.2.7;
        };

        // Uncommenting this might help if you have to go through a
        // firewall and things are not working out:

        // query-source port 53;
};

zone "." {
        type hint;
        file "root.hints";
};

zone "0.0.127.in-addr.arpa" {
        type master;
```

```
        file "pz/127.0.0";
};
-------------------------------------------------------------------
```

Paso 11 Baje y suba el servicio.

```
[root@almendra /etc]# ndc stop
Shutdown initiated.
[root@almendra /etc]# ndc start
new pid is 2258
```

Para una instalación permanente, modifique el archivo `/etc/rc.d/rc.local` agregando al comienzo la línea:

```
/etc/rc.d/init.d/named start
```

Ejemplo:

```
[root@almendra rc.d]# more rc.local
#!/bin/sh
#
# This script will be executed *after* all the other init scripts.
# You can put your own initialization stuff in here if you don't
# want to do the full Sys V style init stuff.

# lanzando el DNS
/etc/rc.d/init.d/named start

if [ -f /etc/redhat-release ]; then
    R=$(cat /etc/redhat-release)
(continua el archivo)
```

D.11. Sección 3: Agregando las zonas locales al DNS

Paso 1 Inserte la zona nueva al archivo `/etc/named.conf`

Agregue la zona al final del archivo.

```
-------------------------------------------------------------------
zone "paredesmoraleda.cl" {
        notify no;
        type master;
        file "pz/paredesmoraleda.cl";
};
-------------------------------------------------------------------
```

El tipo `master` indica que el servidor tiene la copia maestra de la zona, y esta en condiciones de dar respuestas autorizadas sobre la zona.

Paso 2 Ahora cree el archivo `pz/paredesmoraleda.cl`

```
[root@almendra /etc]# cd /var/named/pz/
[root@almendra pz]# vi paredesmoraleda.cl

-------------------------------------------------------------------
@                           IN          SOA         ns.paredesmoraleda.cl.
root.paredesmoraleda.cl. (
```

```
                                200006151; numero de serie: yyyymmdd+version
diaria
                                360000  ; refresco cada 100 horas
                                3600    ; reintentos cada 1 hora
                                3600000 ; expiración del sitio en 42 días
                                360000  ; TTL por defecto de las consultas
)
                IN      NS      ns              ; Inet Address of name server
                IN         MX         10  mail.paredesmoraleda.cl;  Primary  Mail
Exchanger

localhost       IN      A       127.0.0.1
ns              IN      A       192.168.3.1
almendra        IN      CNAME   ns
mail            IN      CNAME   ns
www             IN      CNAME   ns
ftp             IN      CNAME   ns
ganesh          IN      A       192.168.3.2

almendra2       IN      A       192.168.4.1
-----------------------------------------------------------------
```

Baje y suba el servicio:

```
[root@almendra /etc]# ndc stop
Shutdown initiated.
[root@almendra /etc]# ndc start
new pid is 2275
```

Paso 3 Pruebe el cambio.

```
[root@almendra init.d]# nslookup
Default Server:  localhost
Address:  127.0.0.1

> set q=any
> paredesmoraleda.cl
Server:  localhost
Address:  127.0.0.1

paredesmoraleda.cl      preference      =      10,      mail      exchanger      =
mail.paredesmoraleda.cl.paredesmoraleda.cl
paredesmoraleda.cl      nameserver = ns.paredesmoraleda.cl
paredesmoraleda.cl
      origin = ns.paredesmoraleda.cl
      mail addr = root.paredesmoraleda.cl
      serial = 200006153
      refresh = 360000 (4d4h)
      retry   = 3600 (1H)
      expire  = 3600000 (5w6d16h)
      minimum ttl = 360000 (4d4h)
paredesmoraleda.cl      nameserver = ns.paredesmoraleda.cl
ns.paredesmoraleda.cl   internet address = 192.168.3.1
```

Punto de control 2: Note la línea del mail exchanger:

```
paredesmoraleda.cl                  preference    =    10,    mail    exchanger    =
mail.paredesmoraleda.cl.paredesmoraleda.cl
```

Tiene un error, debiera ser:

```
paredesmoraleda.cl                  preference   =   10,   mail   exchanger   =
mail.paredesmoraleda.cl
```

¿A que se debe el error?, ¿Cómo se corrige?, Corríjalo.

Si no encuentra el error, observe el siguiente archivo de zona, en donde se muestra la versión final queda como sigue:

```
[root@almendra /etc]# cd /var/named/pz/
[root@almendra pz]# vi paredesmoraleda.cl
-----------------------------------------------------------------

@                              IN            SOA          ns.paredesmoraleda.cl.
root.paredesmoraleda.cl. (
                                 200006152; numero de serie: yyyymmdd+version
diaria
                                 360000  ; refresco cada 100 horas
                                 3600    ; reintentos cada 1 hora
                                 3600000 ; expiración del sitio en 42 días
                                 360000  ; TTL por defecto de las consultas
)
                IN      NS       ns      ; Inet Address of name server
                IN      MX       10 mail ; Primary Mail Exchanger

localhost       IN      A        127.0.0.1

ns              IN      A        192.168.3.1
                        MX       10 mail
                        HINFO    "K6-2 500" "Linux 2.2"
almendra        IN      CNAME    ns
mail            IN      CNAME    ns
www             IN      CNAME    ns
ftp             IN      CNAME    ns

ganesh          IN      A        192.168.3.2
                        HINFO    "Pentium 133" "Windows 98"

almendra2       IN      A        192.168.4.1
-----------------------------------------------------------------
```

Paso 4 Baje y suba el servicio.

```
[root@almendra /etc]# ndc stop
Shutdown initiated.
[root@almendra /etc]# ndc start
new pid is 2287
```

Paso 5 La zona reversa.

Agregue el archivo `named.conf`

```
-----------------------------------------------------------------
```

```
zone "3.168.192.in-addr.arpa" {
        notify no;
        type master;
        file "pz/192.168.3";
};
-------------------------------------------------------------------
```

Agregue la zona inversa:

```
[root@almendra /etc]# cd /var/named/pz/
[root@almendra pz]# vi /var/named/pz/192.168.3

-------------------------------------------------------------------
@                               IN            SOA         ns.paredesmoraleda.cl.
root.paredesmoraleda.cl. (
                                  7       ; numero de serie
                                  360000  ; refresco cada 100 horas
                                  3600    ; reintentos cada 1 hora
                                  3600000 ; expiración del sitio en 42 días
                                  360000  ; TTL por defecto de las consultas
)
                IN      NS      ns.paredesmoraleda.cl.

1               IN      PTR     ns.paredesmoraleda.cl.
2               IN      PTR     ganesh.paredesmoraleda.cl.
-------------------------------------------------------------------
```

Baje y suba el servicio:

```
[root@almendra /etc]# ndc stop
Shutdown initiated.
[root@almendra /etc]# ndc start
new pid is 2299
```

Paso 6 Verifique el funcionamiento

```
[root@almendra /root]# nslookup
Default Server:  localhost
Address:  127.0.0.1

> 192.168.3.1
Server:  localhost
Address:  127.0.0.1

Name:    ns.paredesmoraleda.cl
Address:  192.168.3.1

> exit
```

Comentarios:

La línea `notify no;` le indica a `named` que no notifique a los servidores secundarios o esclavos cuando se actualizan las tablas de las zonas.

Una zona esclava es una replica de la zona maestra. Las listas maestras especifican una o más direcciones IP que serán la lista de esclavos a contactar para actualizar su copia de la zona. Para definir servidores esclavos de servidores maestros se necesita especificar al menos lo siguiente:

```
     zone domain_name {
```

```
  type slave;
  file path_name;
  masters { ip_addr; [ ip_addr; ... ] };
};
```

Ejemplo: Para indicarle a algún `named` que sea el servidor secundario de `paredesmoraleda.cl`, se debe especificar:

```
zone "paredesmoraleda.cl" {
  type slave;
  file "sz/paredesmoraleda.cl";
  masters { 192.168.3.1};
};
```

Para mayor información consulte `man named`, `man named.conf`, DNS HOWTO y DNS & BIND, C. Liu y P. Albitz, O'Reilly & Associates.

Punto de Control 3: ¿Cuál es la diferencia entre el DNS cache y el DNS usual?

D.12. Sección 4: Servidor Web

Paso 1 Instale el servidor Apache. El cdrom de Linux debe estar montado.

```
[root@almendra /root]# cd /mnt/cdrom/RedHat/RPMS/
[root@almendra RPMS]# ls -la | grep apache
-rw-rw-r--      8 root       root          427362 Mar   8 17:40 apache-1.3.12-
2.i386.rpm-rw-rw-r--     7 root      root         108160 Mar   8 17:40 apache-
devel-1.3.12-2.i386.rpm
-rw-rw-r--     7 root      root        440681 Mar  8 17:40 apache-manual-1.3.12-
2.i386.rpm
[root@almendra RPMS]# rpm -i apache-1.3.12-2.i386.rpm
```

Si lo desea, también puede instalar la documentación:

```
[root@almendra RPMS]# rpm -i apache-manual-1.3.12-2.i386.rpm
```

Si ya está instalado el paquete, déjelo tal cual, o si prefiere desinstale con `rpm -e ...` y vuelva a instalarlo con `rpm –i ....`

Levante el servicio

```
[root@almendra init.d]# ./httpd start
```

Con Netscape pruebe el servicio. Esto se debería ver como en la Figura 43.

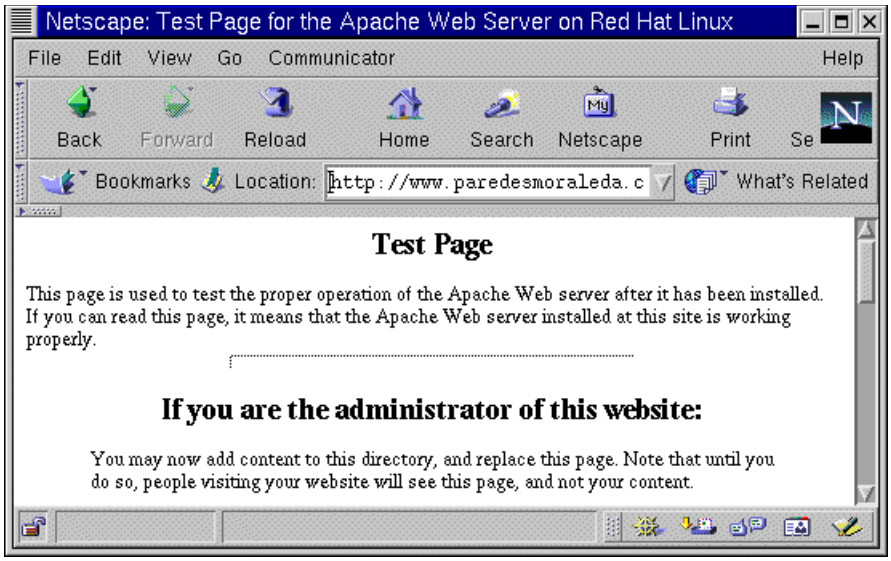


Figura 43. Verificación del servicio Wen en el ISP

Paso 2 Edite el archivo de configuración.

```
[root@almendra /root]# cd /etc/httpd/conf/
[root@almendra conf]# vi httpd.conf
```

En este archivo se indican entre otros parámetros los mostrados en la Tabla 11.

Tabla 11. Parámetros del archivo `httpd.conf`

Parámetro	Explicación
ServerRoot "/etc/httpd"	Directorio de configuración, errores y logs
Timeout 300	Tiempo en segundos antes de enviar o recibir un Timeout
StartServers 8	El numero de servidores que se lanzan al comienzo del sistema
MaxClients 150	Numero máximo de clientes conectado simultaneamente
Port 80	Puerto de servicio Verifiquelo en /etc/services
DocumentRoot "/home/httpd/html"	Direc torio de los documentos del sitio
<Directory "/home/httpd/html">	Inicio del registro para configura el directorio de los documentos del sistema
UserDir public_html	Directorio de los documentos de los usuarios
<Directory /home/*/public_html>	Inicio del registro para configura el directorio de los documentos de los usuarios
AccessFileName .htaccess	Nombre del archivo de control de acceso

Es conveniente que lo revise completo.

D.13. Seccion 5: Agregando sitios web virtuales

Paso 1 Agregue una nueva zona al `/etc/named.conf`

```
---------------------------------------------------------------------
zone "test.cl" {
        notify no;
        type master;
        file "pz/test.cl";
};
---------------------------------------------------------------------
```

construya el archivo `pz/test.cl`

```
[root@almendra /etc]# cd /var/named/pz/
[root@almendra pz]# vi test.cl
```

```
-------------------------------------------------------------------
@               IN      SOA     ns.test.cl. root.test.cl. (
                                200006153; numero de serie: yyyymmdd+version
diaria
                                360000  ; refresco cada 100 horas
                                3600    ; reintentos cada 1 hora
                                3600000 ; expiración del sitio en 42 días
                                360000  ; TTL por defecto de las consultas
)
                IN      NS      ns      ; Inet Address of name server
                IN      MX      10 mail ; Primary Mail Exchanger

localhost       IN      A       127.0.0.1

ns              IN      A       192.168.4.1
                        MX      10 mail
                        HINFO   "K6-2 500" "Linux 2.2"
www             IN      CNAME   ns
-------------------------------------------------------------------
```

Baje y suba el servicio DNS.

Si está corriendo DNS con ndc haga lo siguiente:

```
[root@almendra /etc]# ndc stop
Shutdown initiated.
[root@almendra /etc]# ndc start
new pid is 2299
```

Si esa corriendo DNS como demonio haga lo siguiente:

```
[root@almendra /root]# /etc/rc.d/init.d/named restart
Shutting down named:                                       [  OK  ]
Starting named:                                            [  OK  ]
```

Paso 2 Vaya al final del archivo `httpd.conf` y escriba lo siguiente, siga el ejemplo mostrado en el archivo `httpd.conf`

```
-------------------------------------------------------------------
<VirtualHost 192.168.4.1>
    ServerAdmin root@test.cl
    DocumentRoot /home/httpd/test.cl
    ServerName ns.test.cl
    ErrorLog logs/test.cl.error_log
    CustomLog logs/test.cl.access_log common
</VirtualHost>
-------------------------------------------------------------------
```

Paso 3 Cree directorio `/home/httpd/test.cl/`

```
[root@almendra /root]# cd /home/httpd/
[root@almendra httpd]# mkdir test.cl
```

Paso 4 Escriba la siguiente página:

```
[root@almendra httpd]# cd test.cl/
[root@almendra test.cl]# vi index.html

----------------------------------------------------------------------
<html>
<head>
   <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
</head>
<body>
Archivo de prueba para www.test.cl
</body>
</html>
----------------------------------------------------------------------
```

Paso 5 Baje y suba el servicio.

```
[root@almendra /root]# /etc/rc.d/init.d/httpd restart
Shutting down http:                                        [  OK  ]
Starting httpd:                                            [  OK  ]
```

Pruebe el servicio a www.paredesmoraleda.cl y a www.test.cl. Para www.paredesmoraleda.cl debería ver lo mismo de la Figura 43, y para www.test.cl lo de la Figura 44.

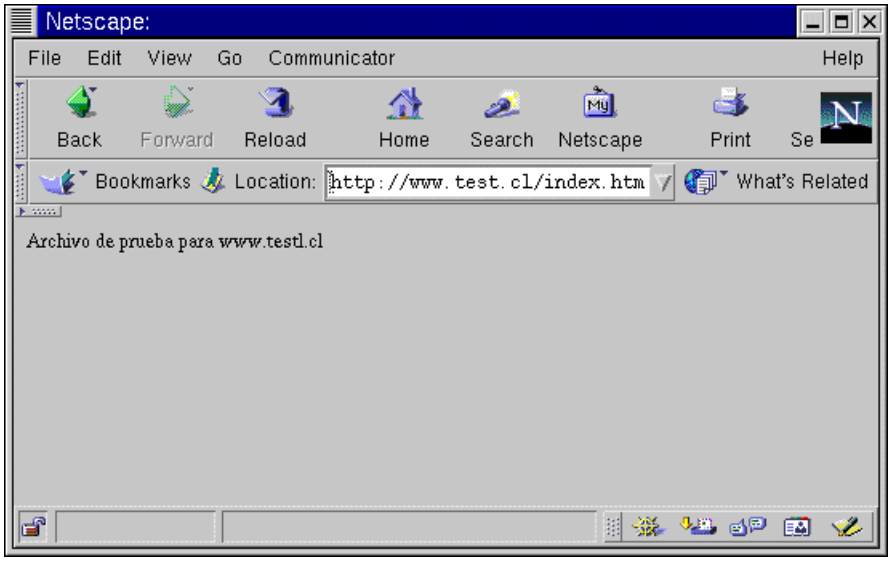


Figura 44. Sitio virtual www.test.cl

Punto de Control 4: ¿Qué ventaja ofrece el hecho de montar sitios web virtuales?, ¿Qué entiende por el concepto de web hosting?

D.14. Sección 6: Instalación de telnet

Paso 1 Instale el telnet cliente y servidor. El cdrom de Linux debe estar montado.

```
[root@almendra /root]# cd /mnt/cdrom/RedHat/RPMS/
[root@almendra RPMS]# rpm -i telnet-server-0.16-6.i386.rpm
[root@almendra RPMS]# rpm -i telnet-0.16-6.i386.rpm
```

Pruebe el servicio.

Recuerde que root no puede entrar por telnet, ingrese a la máquina con su cuenta.

```
[root@almendra RPMS]# telnet ns
Trying 192.168.3.1...
Connected to ns.paredesmoraleda.cl (192.168.3.1).
Escape character is '^]'.

Red Hat Linux release 6.2 (Zoot)
Kernel 2.2.14-5.0smp on an i586
login: raparede
Password:
Last login: Thu Jun 15 13:58:38 from ns
[raparede@almendra raparede]$ su -
Password:
[root@almendra /root]#
```

Punto de Control 5: ¿Por qué razón cree Usted que root no puede entrar por telnet?

_____
_____
_____
_____

D.15. Sección 7: Instalación de servidor FTP

Paso 1 Instale el servidor FTP. El cdrom de Linux debe estar montado.

Se necesitan tener dos terminales abiertos simultáneamente, uno en modo superusuario (root) en donde se realizará a instalación, y el otro como un usuario normal.

```
[root@abril /root]# cd /mnt/cdrom/RedHat/RPMS/
```

Busque los archivos que tengan relación con ftp.

```
[root@abril RPMS]# ls | grep ftp
anonftp-3.0-3.i386.rpm
ftp-0.16-3.i386.rpm
gftp-2.0.6a-3.i386.rpm
ncftp-3.0beta21-4.i386.rpm
tftp-0.16-5.i386.rpm
tftp-server-0.16-5.i386.rpm
wu-ftpd-2.6.0-3.i386.rpm
```

Ejecute el siguiente comando:

```
[root@abril RPMS]# rpm -i wu-ftpd-2.6.0-3.i386.rpm
```

Punto de control 6: En el terminal de usuario verifique que está operando el demonio de ftp, para eso haga un ftp hacia el servidor, como un usuario cualquiera.

NOTA 1: en el archivo /etc/ftpusers se indican los usuarios que NO pueden usar ftp, dentro de ellos está root, luego no intente hacer ftp ingresando como usuario root
NOTA 2: en IP la dirección 127.0.0.1 corresponde a la dirección local de la máquina por defecto.

Punto de Control 7: ¿Por qué razón cree Usted que root no puede entrar por ftp?

_____

_____

_____

_____

Ejecute los siguientes comandos en negrita, ingrese su password cuando corresponda y observe la salida.

```
[raparede@abril ~]$ ftp 127.0.0.1
Connected to 127.0.0.1.
220 abril.firstcom.cl FTP server (Version wu-2.6.0(1) Mon Feb 28 10:30:36
EST 2000) ready.
530 Please login with USER and PASS.
530 Please login with USER and PASS.
KERBEROS_V4 rejected as an authentication type
Name (127.0.0.1:raparede): raparede
331 Password required for raparede.
Password:
230 User raparede logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
200 PORT command successful.
150 Opening ASCII mode data connection for /bin/ls.
total 52
-rw-r--r--    1 raparede usuarios       24 May 11 15:10 .bash_logout
-rw-r--r--    1 raparede usuarios      230 May 11 15:10 .bash_profile
-rw-r--r--    1 raparede usuarios      124 May 11 15:10 .bashrc
-rw-r--r--    1 raparede usuarios      435 May 11 15:10 .kderc
-rw-------    1 raparede usuarios       17 May 12 18:31 .mysql_history
-rw-r--r--    1 raparede usuarios     3394 May 11 15:10 .screenrc
drwx------    2 raparede root         4096 May 11 15:13 .xauth
drwxr-xr-x    5 raparede usuarios     4096 May 11 15:10 Desktop
-rw-r--r--    1 raparede usuarios       59 May 11 15:14 a.c
-rwxr-xr-x    1 raparede usuarios    11731 May 11 15:15 a.out
drwxr-xr-x    3 raparede usuarios     4096 May 16 10:52 programas
226 Transfer complete.
ftp> quit
221-You have transferred 0 bytes in 0 files.
221-Total traffic for this session was 1224 bytes in 1 transfers.
221-Thank you for using the FTP service on abril.firstcom.cl.
221 Goodbye.
```

D.16. Sección 8: Instalación del servidor de FTP anónimo

Paso 1 Instale el servidor FTP anónimo. El cdrom de Linux debe estar montado.

Ejecute el siguiente comando:

```
[root@abril RPMS]# rpm -i anonftp-3.0-3.i386.rpm
```

Punto de control 8: Verifique que está operando el servidor de ftp anónimo, para esto en el terminal de usuario haga un ftp hacia el servidor, como el usuario anónimo (`anonymous`).

Paso 2 Pruebas de ftp anónimo.

Ejecute los comandos en negrita, y cuando le solicite la password, ingrese su dirección de correo electrónico y observe la salida.

```
[raparede@abril ~]$ ftp 127.0.0.1
Connected to 127.0.0.1.
220 abril.firstcom.cl FTP server (Version wu-2.6.0(1) Mon Feb 28 10:30:36
EST 2000) ready.
530 Please login with USER and PASS.
530 Please login with USER and PASS.
KERBEROS_V4 rejected as an authentication type
Name (127.0.0.1:raparede): anonymous
331 Guest login ok, send your complete e-mail address as password.
Password:
230 Guest login ok, access restrictions apply.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
200 PORT command successful.
150 Opening ASCII mode data connection for /bin/ls.
total 16
d--x--x--x   2 root     root         4096 May 16 16:56 bin
d--x--x--x   2 root     root         4096 May 16 16:56 etc
drwxr-xr-x   2 root     root         4096 May 16 16:56 lib
drwxr-sr-x   2 root     ftp          4096 Feb  4 15:06 pub
226 Transfer complete.
ftp> quit
221-You have transferred 0 bytes in 0 files.
221-Total traffic for this session was 801 bytes in 1 transfers.
221-Thank you for using the FTP service on abril.firstcom.cl.
221 Goodbye.
```

Paso 3 Configuración del servicio FTP.

En el directorio `/etc` se ven varios archivos relacionados con FTP, de ellos destacan:

En el archivo `/etc/ftpaccess` está la configuración del servicio.
En el archivo `/etc/ftpusers` están los usuarios que no pueden usar ftp, entre ellos está root.

D.17. Cuestionario Final

1. ¿Para qué sirve el DNS?
2. ¿En qué casos es útil el DNS modalidad cache?
3. En la Escuela de Ingeniería de la U de Chile, la resolución inversa de direcciones generalmente no se realiza en los departamentos, sino que la realiza el CEC, por que razón. Hint: Averigüe la máscara de red que se emplea en la Escuela.
4. Que es web hosting.
5. Diseñe un esquema que semanalmente respalde los documentos web de una máquina.

Anexo E. Experiencia 4: Habilitación de los Servicios de Conectividad

E.1. Resumen

El objetivo de esta experiencia es habilitar los servicios de conectividad. En la experiencia pasada se implementaron algunos de los servicios de un ISP, en ésta se mostrarán las capacidades de conectividad que ofrecen los sistemas Unix, en particular de Linux, de modo de mostrar como emular los equipos de redes (routers y servidores de acceso) con el software proveído en el sistema.

Para la emulación de routers, existe un protocolo llamado routed que era capaz de implementar RIP, routed fue mejorado por gated, otra aplicación diseñada para habilitar servicios de enrutamiento, que implementa RIP, OSPF, BGP y otros, mayor información de gated se puede obtener en www.gated.org. En esta experiencia sólo se mostrará una introducción a estos tópicos.

En resumen los servicios que se considerarán son:

- Conexión dedicada mediante ruteo directo.
- Conexión conmutada vía modem.

E.2. Esquemas generales

En esta experiencia interesa mostrar los requerimientos mínimos de interconectividad que se necesitan para el ISP. Note que todos los computadores, a través de la interfaz ethernet están conectados a puertas del hub, y por otra puerta del hub (aquella que acepta cross-over) se conectará un cable mirando hacia la Internet. El esquema de conexión se ve en la Figura 45. En el esquema se ve a un computador como servidor y clientes haciéndole consultas tanto en la red del servidor, como a través de un acceso conmutado telefónico. En la Figura 46 se muestra el esquema físico.

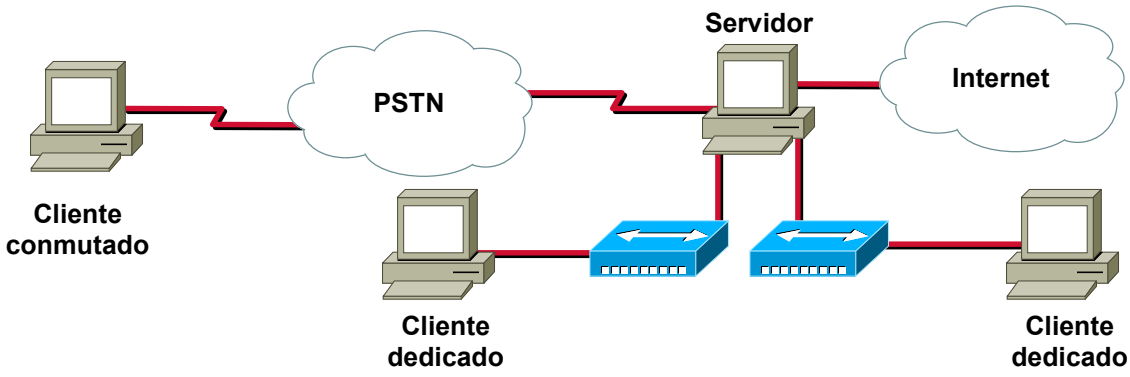


Figura 45. Esquema lógico del laboratorio 4

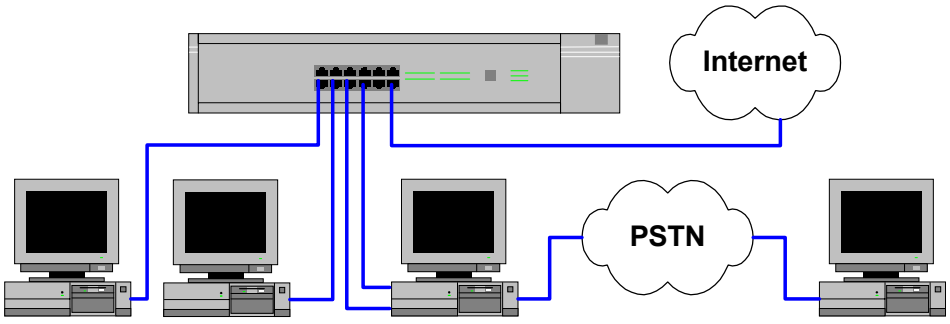


Figura 46. Esquema físico del laboratorio 4

E.3. Materiales

Para esta experiencia se necesita lo siguiente:

- ✓ 1 Computador habilitado como ISP mínimo (200 MB en disco duro libre) y dos tarjetas de red.
- ✓ 2 Computador para realizar las funciones de cliente dedicado.
- ✓ 1 Computador para realizar las funciones conmutado.
- ✓ 2 líneas telefónicas habilitadas.
- ✓ 4 Cables UTP con conectores machos.
- ✓ 1 Cable UTP cruzado con conectores machos (respaldo si falla la puerta cross-over del hub).
- ✓ 1 Hub que soporte cross-over en alguna puerta.
- ✓ 1 CD-ROM con la distribución de Linux Red Hat 6.2 o superior.

E.4. Objetivos

1. Mostrar el servicio de enrutamiento directo.
2. Mostrar el mecanismo de conexión conmutada en lado servidor y cliente.

E.5. Requisitos, conceptos y habilidades necesarias

- ✓ Conocimientos básicos en sistemas operativos.
- ✓ Conocimientos básicos en redes ethernet.
- ✓ Modelos de referencia OSI y TCP/IP.
- ✓ Conocimientos básicos de direccionamiento IP.
- ✓ Conocimientos básicos en protocolos de enrutamiento.
- ✓ Las recomendaciones del Anexo G. Recomendaciones Generales.

E.6. Bibliografía y referencias

1. Apuntes del curso el54b: “Sistemas de Procesamiento de la Información”.
2. Apuntes del curso el64e: “Redes de Computadores”.
3. Apuntes del curso el647: “interfaces digitales y Periféricos”.
4. Apuntes del curso el649: “Programación y Operación de Computadores”.
5. Apuntes del curso cc51c: “Comunicación de Datos”.
6. Olaf Kirch (Traducción Proyecto LuCAS), “Guía de Administración de Redes con Linux”, http://lucas.hispalinux.es/htmls/manuales.html, 20 de Mayo de 2000.
7. Josh Gentry, “Linux Dialin Server Setup Guide”, http://ftp.the-gc.net/lg/issue38/gentry.html, 02 de Julio de 2000.

E.7. Plan de acción

Los pasos a seguir en esta experiencia son:

1. Configuración de Dial Up.
2. Pruebas de acceso conmutado como cliente.
3. Configuración de Dial In.
4. Pruebas de acceso conmutado como servidor.
5. Configuración de interfaces para ruteo directo.
6. Pruebas iniciales de ruteo directo.
7. Habilitación de ruteo directo.
8. Pruebas de ruteo directo.

E.8. Sección 0: Conexiones

Paso 1 Se debe verificar todo el material.

Paso 2 Realice las conexiones tal como se muestran en el diagrama físico.

E.9. Sección 1: Configuración de Dial Up

Paso 1 Para esta experiencia es necesario un modem soportado por Linux. Estos son los modem estándar o los modem internos, los modem tipo winmodem en general ocasionan problemas.

Tiene que detectar cual es la puerta serial en donde está instalado el modem.

- Si el modem es interno, se puede obtener esta información del manual del modem.
- Si además de interno tiene switches de configuración de puerta serial e IRQ, basta con leer esta configuración (apóyese en el manual).
- Si es externo, la puerta serial asignada depende de la configuración de puertas seriales que se indico en la BIOS de la tarjeta madre.

Una vez localizada la puerta serial, se debe indicar que puerta ttySx para el modem, en la Tabla 12 se indica la relación

Tabla 12. Asociación de puerta serial COM con ttySx

Puerta serial	Dispositivo Linux
com1	/dev/ttyS0
com2	/dev/ttyS1
com3	/dev/ttyS2
com4	/dev/ttyS3

Por último, y para simplificar las cosas realice el siguiente link. En el ejemplo el modem esta en la ttyS0

```
[root@almendra /root]# ln -s /dev/ttyS0 /dev/modem
```

Si el modem no está en alguno de los cuatro puertos anteriores necesitará usar el comando `setserial` (`man setserial`) por ejemplo, para indicar que la IRQ del modem en ttyS2 es el IRQ 11, se usa:

```
/bin/setserial -b /dev/ttyS2 IRQ 11
```

Monte el cdrom de Red Hat 6.2, y cámbiese al directorio de los paquetes

```
[root@almendra /root]# mount /dev/cdrom
[root@almendra /root]# cd /mnt/cdrom/RedHat/RPMS
```

Instale el paquete `ppp-2.3.11-4.i386.rpm`

```
[root@almendra RPMS]# rpm -i ppp-2.3.11-4.i386.rpm
```

Configuración del enlace:

Paso 2 Lance el configurador de redes `netconf`. `netconf` tiene interfaces para X windows y otra para consola.

```
[root@almendra RPMS]# netconf
```

Ver Figura 47.

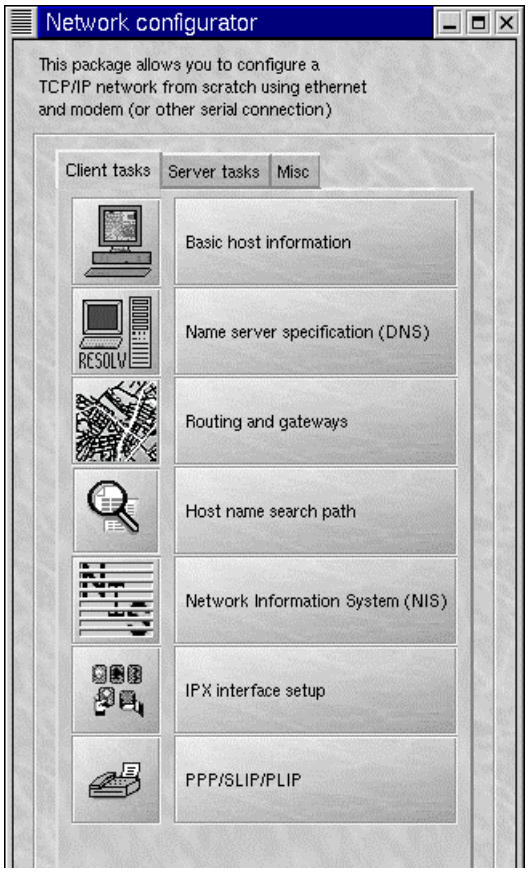


Figura 47. Configurador de Redes netconf

Paso 3 Pinche o escoja en PPP/SLIP/PLIP (Ver Figura 48).

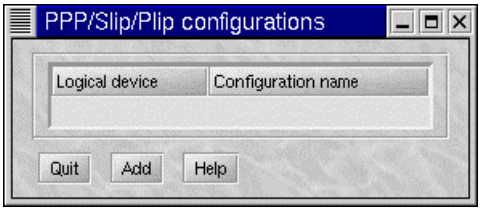


Figura 48. Configuración de enlace PPP

Paso 4 Pinche o escoja en Add (Ver Figura 49).

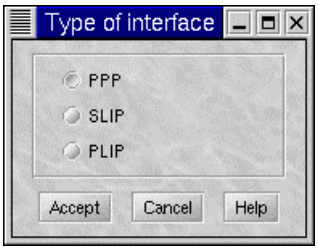


Figura 49. Tipo de interface

Paso 5 Pinche o escoja en PPP (Ver Figura 50).

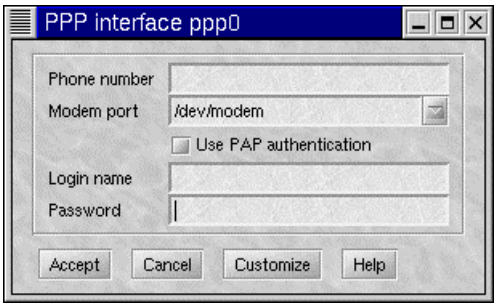


Figura 50. Configuración de la interfaz ppp0

Paso 6 Complete los datos y pinche o escoja en aceptar (Ver Figura 51).

Figura 51. Datos para la configuración de la interfaz ppp0

Para permitir que cualquier usuario pueda utilizar la interfaz ppp0 haga lo siguiente:

Pinche o escoga en la interfaz ppp0 y pinche o escoja el botón `Allow any user (de)activate the interface`.

Punto de control 1: Que utilidad tiene que los usuarios puedan levantar el enlace ppp.

Paso 7 Luego pinche o escoja en `quit`, y active los cambios (Ver Figura 52).

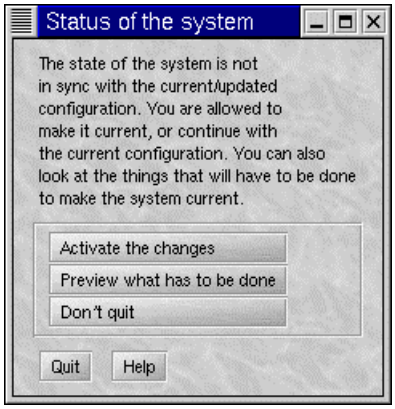


Figura 52. Activación de cambios de netconf

E.10. Sección 2: Pruebas de acceso conmutado como cliente

Paso 1 Por precaución copie el archivo `/etc/resolv.conf` en `/etc/resolv.conf.local`

```
[root@almendra RPMS]# cp /etc/resolv.conf /etc/resolv.conf.local
```

Paso 2 Levante la conexión con el comando `ifup ppp0`

```
[root@almendra RPMS]# ifup ppp0
```

Paso 3 Para observar la ejecución de la conexión utilice `tail -f /var/log/messages`, en otra ventana.

```
[root@almendra root]# tail -f /var/log/messages
```

```
Jul   2 19:37:29 almendra ifup-ppp: pppd started for ppp0 on /dev/modem at
115200
Jul  2 19:37:29 almendra chat[1604]: expect (OK)
Jul  2 19:37:29 almendra chat[1604]: ATZ^M^M
Jul  2 19:37:29 almendra chat[1604]: OK
Jul  2 19:37:29 almendra chat[1604]:  -- got it
Jul  2 19:37:29 almendra chat[1604]: send (ATDT155018008332200^M)
Jul  2 19:37:29 almendra chat[1604]: expect (CONNECT)
Jul  2 19:37:29 almendra chat[1604]: ^M
Jul  2 19:37:56 almendra chat[1604]: ATDT155018008332200^M^M
Jul  2 19:37:56 almendra chat[1604]: CONNECT
Jul  2 19:37:56 almendra chat[1604]:  -- got it
Jul  2 19:37:56 almendra chat[1604]: send (^M)
Jul  2 19:37:56 almendra chat[1604]: timeout set to 5 seconds
Jul  2 19:37:56 almendra chat[1604]: expect (~)
Jul  2 19:37:56 almendra chat[1604]:  52000/ARQ/x2/LAPM/V42BIS^M
Jul  2 19:37:57 almendra chat[1604]: ^M
Jul   2 19:37:57 almendra chat[1604]: Welcome to 3Com Total Control HiPer ARC
(TM)^M
Jul  2 19:37:57 almendra chat[1604]: Networks That Go The Distance (TM)^M
Jul  2 19:37:57 almendra chat[1604]: ^M
Jul  2 19:38:01 almendra chat[1604]: alarm
Jul  2 19:38:01 almendra chat[1604]: send (^M)
Jul  2 19:38:01 almendra chat[1604]: send (^M)
Jul  2 19:38:01 almendra pppd[1595]: Serial connection established.
Jul  2 19:38:01 almendra pppd[1595]: Using interface ppp0
Jul  2 19:38:01 almendra pppd[1595]: Connect: ppp0 <--> /dev/modem
Jul  2 19:38:03 almendra pppd[1595]: local  IP address 10.40.20.98
Jul  2 19:38:03 almendra pppd[1595]: remote IP address 192.168.0.8
Jul  2 19:38:03 almendra pppd[1595]: primary   DNS address 200.9.97.3
Jul  2 19:38:03 almendra pppd[1595]: secondary DNS address 200.9.100.1
```

Paso 4 Note que al levantar la conexión, dependiendo de como se configure, se modifica el archivo `/etc/resolv.conf`, para utilizar el DNS local, debe recuperar este archivo (`/etc/resolv.conf`), esto se puede automatizar con el siguiente script. El script `ifupppp0` automatiza el proceso de levantar el enlace y recuperar el archivo `/etc/resolv.conf`

Punto de Control 2: Interprete las líneas marcadas en negritas:

```
[root@almendra root]# vi /bin/ifupppp0

------------------------------------------------------------
#! /bin/sh

/sbin/ifup ppp0
/bin/cp /etc/resolv.conf /etc/resolv.conf.bak
/bin/cp /etc/resolv.conf.local /etc/resolv.conf
------------------------------------------------------------
```

Paso 5 Con esto para levantar la conexión utilice el programa `/bin/ifupppp0`

```
[root@almendra RPMS]# /bin/ifupppp0
```

Para cortar el enlace detenga el proceso `ifup ppp0` con un Ctrl-C, o invoque `ifdown ppp0`

E.11. Sección 3: Configuración de Dial In

Paso 1 Relea el Paso 1 de la sección Dial Up.

En una conexión conmutada, técnicamente no hay diferencia entre el cliente y el servidor, puesto que es una conexión peer to peer.

Paso 2 Soporte de Kernel

Si al iniciar la máquina aparece el mensaje:

```
------------------------------------------------------------------
PPP Dynamic channel allocation code copyright 1995 Caldera, Inc.
PPP line discipline registered.
------------------------------------------------------------------
```

O uno similar, entonces el kernel soporta PPP, si no, hay que recompilarlo (refiérase a la experiencia 2 para esto). Recuerde activar PPP, SLIP, CSLIP, IP forwarding, etc. Revise las opciones Network devices y Network options.

Otro método más simple es instalar los módulos para PPP. Si el sistema tiene instalado el comando `insmod`, se recomienda este método. Recuerde agregar las líneas en el archivo `/etc/rc.d/rc.local`

Paso 3 Para instalar el módulo `ppp.o`, se debe instalar primero el módulo `slhc.o`. Hay definiciones necesarias para `ppp` que están contenidas en el módulo `slhc`.

```
[root@almendra /root]# cd /lib/modules/2.2.14-5.0smp/net/
[root@almendra net]# insmod slhc.o
[root@almendra net]# insmod ppp.o
```

Paso 4 Con `lsmod` se verifican los módulos que están instalados:

```
[root@almendra net]# lsmod
```

```
Module                  Size  Used by
ppp                    21068   0  (unused)
slhc                    4560   0  [ppp]
lockd                  32072   1  (autoclean)
sunrpc                 54692   1  (autoclean) [lockd]
3c509                   6256   1  (autoclean)
nls_iso8859-1           2244   3  (autoclean)
nls_cp437               3752   2  (autoclean)
vfat                    9532   2  (autoclean)
fat                    31584   2  (autoclean) [vfat]
```

Paso 5 Edite el archivo `/etc/rc.d/rc.local`. No modifique el resto del archivo.

```
[root@almendra net]# vi /etc/rc.d/rc.local

----------------------------------------------------------------
#!/bin/sh
#
# This script will be executed *after* all the other init scripts.
# You can put your own initialization stuff in here if you don't
# want to do the full Sys V style init stuff.

# lanzando el DNS
/etc/rc.d/init.d/named start
# lanzando el proxy
/etc/rc.d/init.d/squid start
# instalando los módulos para ppp
/sbin/insmod /lib/modules/2.2.14-5.0smp/net/slhc.o
/sbin/insmod /lib/modules/2.2.14-5.0smp/net/ppp.o
----------------------------------------------------------------
```

Paso 6 Para monitorear el modem, necesita el paquete `mgetty`. Instale el paquete `mgetty-1.1.21-4.i386.rpm`. Esto permite crear el tty que controle el modem.

```
[root@almendra /root]# cd /mnt/cdrom/RedHat/RPMS
[root@almendra RPMS]# rpm -i mgetty-1.1.21-4.i386.rpm
```

Edite el archivo `/etc/inittab` y agregue las siguientes líneas. Nota, el modem del ejemplo está conectado al ttyS0, verifique en donde esta conectado el modem en su equipo.

```
[root@almendra RPMS]# vi /etc/inittab

----------------------------------------------------------------
# Para accesar por telefono via mgetty
# La linea comienza con S0 y termina con /dev/ttyS0
S0:2345:respawn:/sbin/mgetty ttyS0 -D /dev/ttyS0
----------------------------------------------------------------
```

Punto de control 3: Intuitivamente responda, ¿para qué son los programas que tienen relación con `getty`?

_____

_____

_____

_____

La opción `-D` le indica a `mgetty` que espere llamadas de datos, no de fax.

Paso 7 Active los cambios, con `kill -1 1`, esto fuerza a `initd` a releer el archivo `/etc/inittab`

```
[root@almendra RPMS]# kill -1 1
```

Con `ps -ax | grep getty` verifique que el proceso `mgetty` está corriendo:

```
[root@almendra RPMS]# ps -ax | grep getty
  693 tty2     SW     0:00 [mingetty]
  694 tty3     SW     0:00 [mingetty]
  695 tty4     SW     0:00 [mingetty]
  696 tty5     SW     0:00 [mingetty]
  697 tty6     SW     0:00 [mingetty]
 2267 ?        S      0:00 /sbin/mgetty ttyS0 -D /dev/ttyS0
 2277 pts/0    S      0:00 grep getty
```

Con esto `mgetty` negocia una conexión SLIP con el cliente. La autentificación se realizar a través del archivo `/etc/passwd`, por lo cual cuando pruebe la conexión debe ocupar una cuenta que figure en este archivo.

E.12. Sección 4: Pruebas de acceso conmutado como servidor

Pruebe la conexión desde un cliente. En windows debe hacer lo siguiente:

Paso 1 Click en My Computer.
Paso 2 Click en Dial-UP Networking.
Paso 3 Click en Make new Connection.
Paso 4 Indique el telefono y los otros parámetros que necesite.
Paso 5 Right-click en el icono para la conexión.
Paso 6 Click en Properties.
Paso 7 Click en Configure.
Paso 8 Click en Options.
Paso 9 Click en "Bring up terminal window after dialing".

En español:

Paso 1 Click en Mi computador.
Paso 2 Click en Hacer nueva conexión.
Paso 3 Indique el telefono y los otros parámetros que necesite.
Paso 4 Right-click en el icono para la conexión.
Paso 5 Click en Propiedades.
Paso 6 Click en General.
Paso 7 Click en Configuración.
Paso 8 Click en Opciones.
Paso 9 Click en "Mostrar la ventana del terminal después del marcado".

Con `tail -f /var/log/messages` puede ver como se lleva a cabo la llamada.

E.13. Sección 5: Configuración de interfaces para ruteo directo

El ruteo directo es la técnica más simple de ruteo, puesto que sólo hay que configurar las interfaces del router, y habilitar el reenvío de paquetes IP (IP forward).

Paso 1 Con netconf asigne las direcciones según la Tabla 13

Tabla 13. Direcciones para el router Linux

Interfaz Ethernet	Dirección IP/Máscara
eth0	192.168.3.1/24
eth1	192.168.4.1/24

```
[root@almendra /root]# netconf
```

Recuerde la Figura 47.

Paso 2 Pinche o escoja en Basic Host Configuration (Ver Figura 53). Llene la información asociada a Host name (si es que no lo ha hecho antes).

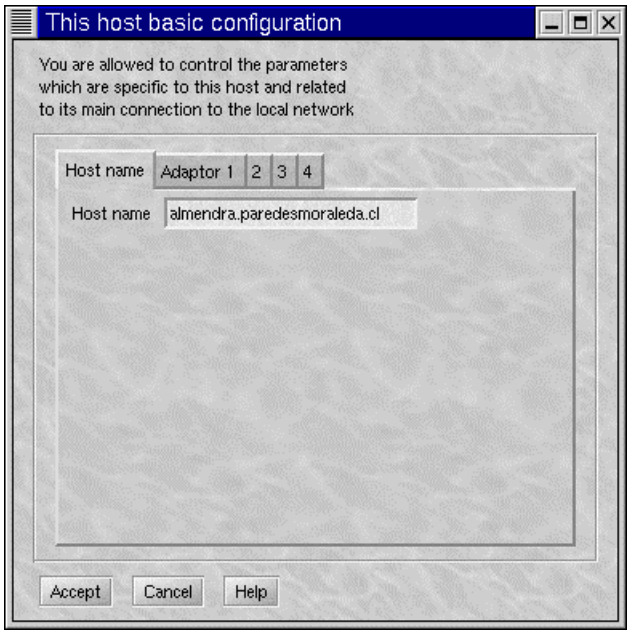


Figura 53. Configuración básica del host

Paso 3 Pinche o escoja en Adaptor 1 (Ver Figura 54). Llene los datos que correspondan para la interfaz eth0.

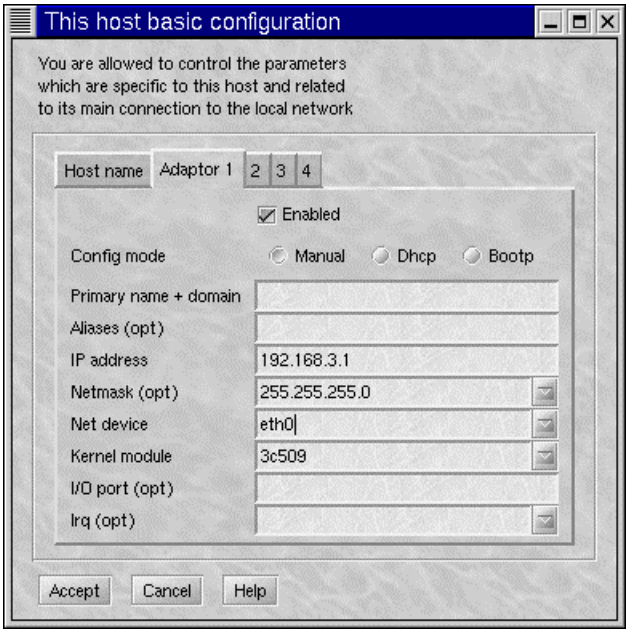


Figura 54. Configuración de la interfaz ethernet 0

Paso 4 Pinche o escoja en Adaptor 2. Llene los datos que correspondan para la interfaz eth1.

Paso 5 Al PC1 indique la dirección 192.168.3.10/24.

Paso 6 Al PC2 indique la dirección 192.168.4.10/24.

Paso 7 Reinicie todas las máquinas.

E.14. Sección 6: Pruebas iniciales de ruteo directo

Paso 1 Pruebe el comando `ping` desde el router a los clientes. Recuerde que el comando se corta con un Ctrl-C.

```
[root@almendra /root]# ping 192.168.3.10
PING 192.168.3.10 (192.168.3.10) from 192.168.3.1 : 56(84) bytes of data.
64 bytes from 192.168.3.10: icmp_seq=0 ttl=128 time=0.4 ms
64 bytes from 192.168.3.10: icmp_seq=1 ttl=128 time=0.4 ms
64 bytes from 192.168.3.10: icmp_seq=2 ttl=128 time=0.3 ms
64 bytes from 192.168.3.10: icmp_seq=3 ttl=128 time=0.4 ms

--- 192.168.3.10 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.3/0.3/0.4 ms
[root@almendra /root]# ping 192.168.4.10
PING 192.168.4.10 (192.168.4.10) from 192.168.4.1 : 56(84) bytes of data.
64 bytes from 192.168.4.10: icmp_seq=0 ttl=128 time=1.8 ms
64 bytes from 192.168.4.10: icmp_seq=1 ttl=128 time=0.8 ms
64 bytes from 192.168.4.10: icmp_seq=2 ttl=128 time=0.8 ms
64 bytes from 192.168.4.10: icmp_seq=3 ttl=128 time=0.8 ms

--- 192.168.4.10 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.8/1.0/1.8 ms
```

Paso 2 Pruebe `ping` desde un cliente al router.

```
C:\WINDOWS\Escritorio>ping 192.168.3.1

Haciendo ping a 192.168.3.1 con 32 bytes de datos:

Respuesta desde 192.168.3.1: bytes=32 tiempo=1ms TDV=255
Respuesta desde 192.168.3.1: bytes=32 tiempo<10ms TDV=255
Respuesta desde 192.168.3.1: bytes=32 tiempo<10ms TDV=255
Respuesta desde 192.168.3.1: bytes=32 tiempo<10ms TDV=255

Estadísticas de ping para 192.168.3.1:
    Paquetes: enviados = 4, Recibidos = 4, perdidos = 0 (0% loss),
Tiempos aproximados de recorrido redondo en milisegundos:
    mínimo = 0ms, máximo =  1ms, promedio =  0ms
```

Paso 3 pruebe ping desde un cliente al otro.

```
C:\WINDOWS\Escritorio>ping 192.168.4.10

Haciendo ping a 192.168.4.10 con 32 bytes de datos:

Tiempo de espera agotado.
Tiempo de espera agotado.
Tiempo de espera agotado.
Tiempo de espera agotado.

Estadísticas de ping para 192.168.4.10:
    Paquetes: enviados = 4, Recibidos = 0, perdidos = 4 (100% loss),
Tiempos aproximados de recorrido redondo en milisegundos:
    mínimo = 0ms, máximo =  0ms, promedio =  0ms
```

Paso 4 Verifique la tabla de enrutamiento del router Linux.

```
[root@almendra /root]# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.3.1     0.0.0.0         255.255.255.255 UH    0      0        0 eth0
192.168.4.1     0.0.0.0         255.255.255.255 UH    0      0        0 eth1
192.168.4.0     192.168.4.1     255.255.255.0   UG    0      0        0 eth1
192.168.4.0     0.0.0.0         255.255.255.0   U     0      0        0 eth1
192.168.3.0     192.168.3.1     255.255.255.0   UG    0      0        0 eth0
192.168.3.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
127.0.0.0       0.0.0.0         255.0.0.0       U     0      0        0 lo
```

Punto de Control 4: ¿Por qué no funcionó? Aventure una respuesta:

E.15. Sección 7: Habilitación de ruteo directo

Paso 1 El Kernel debe soportar Ruteo, si en la experiencia 2 no se preocupó de activar esto ahora es tiempo de hacerlo (refiérase a la experiencia 2 para las instrucciones de compilación del kernel).

Se debe activar en Networking options:

```
IP: advanced router
IP: verbose route monitoring (NEW)
IP: large routing tables (NEW)
```

Aprovechando la oportunidad Activar en Network device support:

```
Ethernet (10 or 100Mbit)  --->
    Aproveche de insertar los módulos de sus tarjetas de red al kernel (si los
conoce)
PPP (point-to-point) support
SLIP (serial line) support
```

Paso 2 Luego de compilar el kernel reinicie el router Linux.

Paso 3 Pruebe nuevamente el `ping` de un cliente a otro, que sucede.

Paso 4 Lo que falta es indicar explícitamente que el computador central efectúe el ruteo de los paquetes (IP forwarding). Para eso, hay que escribir un `1` en el archivo `/proc/sys/net/ipv4/ip_forward`

```
[root@almendra /root]# echo "1" > /proc/sys/net/ipv4/ip_forward
```

Punto de Control 5: Según su parecer, ¿tiene sentido hacer esta modificación?

_____
_____
_____
_____

E.16. Sección 8: Pruebas de ruteo directo

Paso 1 Pruebe ahora `ping` desde un cliente a otro:

```
C:\WINDOWS\Escritorio>ping 192.168.4.10

Haciendo ping a 192.168.4.10 con 32 bytes de datos:

Respuesta desde 192.168.4.10: bytes=32 tiempo=2ms TDV=127
Respuesta desde 192.168.4.10: bytes=32 tiempo=1ms TDV=127
Respuesta desde 192.168.4.10: bytes=32 tiempo=1ms TDV=127
Respuesta desde 192.168.4.10: bytes=32 tiempo=1ms TDV=127

Estadísticas de ping para 192.168.4.10:
    Paquetes: enviados = 4, Recibidos = 4, perdidos = 0 (0% loss),
Tiempos aproximados de recorrido redondo en milisegundos:
    mínimo = 1ms, máximo =  2ms, promedio =  1ms
```

Paso 2 Pruebe un `tracert` desde un cliente a otro:

```
C:\WINDOWS\Escritorio>tracert 192.168.4.10
```

```
Traza a la dirección NOTEBOOK2 [192.168.4.10]
sobre un máximo de 30 saltos:

  1   <10 ms   <10 ms   <10 ms  192.168.3.1
  2     1 ms     1 ms     1 ms  NOTEBOOK2 [192.168.4.10]

Traza completa.
```

Paso 3 Ahora que está operando el ruteo, modifique la asignación explícita de `ip_forward` en el archivo `/etc/rc.d/rc.local`

```
[root@almendra /root]# vi /etc/rc.d/rc.local
```

```
------------------------------------------------------------
#!/bin/sh
#
# This script will be executed *after* all the other init scripts.
# You can put your own initialization stuff in here if you don't
# want to do the full Sys V style init stuff.

/bin/echo "1" > /proc/sys/net/ipv4/ip_forward
------------------------------------------------------------
```

Paso 4 Reinicie la máquina, y vuelva a verificar el ruteo directo.

E.17. Cuestionario Final

1. Un modem en Linux puede usarse tanto para Dial Up y Dial In simultáneamente
2. Si su respuesta es negativa, como solucionaría este problema. Diseñe un esquema que permita al menos implementar Dial IN y Dial Up en forma alternada.
3. Explique cómo opera el ruteo directo.

Anexo F. Experiencia 5: Habilitación de Servicios Internet II

F.1. Resumen

En esta experiencia se pretende terminar la instalación de los servicios de un ISP mínimo, y tocar un poco el tema de la seguridad.

Respecto a los servicios, está en deuda el correo electrónico, por lo que se mostrará la instalación de sendmail y POP3. Para la autentificación de los usuarios en POP3 se habilitara PAM (Pluggable Authentication Modules), que es una opción que provee Red Hat.

Para hacer una introducción al tema de seguridad en redes se muestra el servicio proxy y una implementación de firewall para Linux.

F.2. Esquemas generales

En esta experiencia interesa continuar con los servicios de Internet. Para mostrar el esquema de cliente servidor, para esta experiencia se separarán los computadores en pares, donde uno de ellos será el ISP y el otro solicitará servicios. La nube Internet se refiere a los otros pares de computadores, esto para hacer más interesante la experiencia. El esquema de conexión se ve en la Figura 55. El esquema físico de la experiencia se ve en la Figura 42.

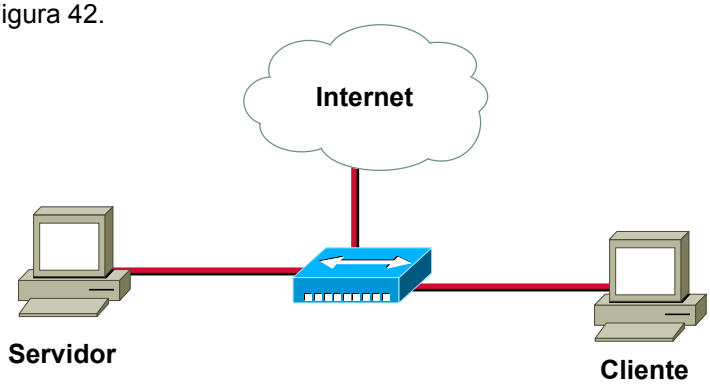


Figura 55. Esquema lógico experiencia 5

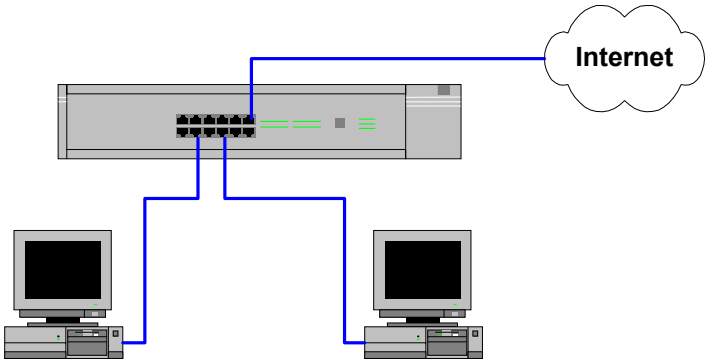


Figura 56. Esquema físico experiencia 5

F.3. Materiales

Para esta experiencia se necesita lo siguiente:

- ✓ 1 Computador habilitado como ISP mínimo.
- ✓ 1 Computador habilitado como cliente dedicado.
- ✓ 3 Cables UTP con conectores machos.
- ✓ 1 Cable UTP cruzado con conectores machos (respaldo si falla la puerta cross-over del hub).
- ✓ 1 Hub que soporte cross-over en alguna puerta.
- ✓ 1 CD-ROM con la distribución de Linux Red Hat 6.2 o superior.

F.4. Objetivos

1. Instalación y configuración del firewall.
2. Instalación y configuración del servicio SMTP.
3. Instalación y configuración del servicio POP3.
4. Instalación y configuración del proxy.

F.5. Requisitos, conceptos y habilidades necesarias

- ✓ Conocimientos básicos de sistemas operativos.
- ✓ Noción de red de computadores.
- ✓ Paradigma cliente/servidor.
- ✓ Noción de diseño modular.
- ✓ Modelos de referencia OSI y TCP/IP.
- ✓ Conocimientos básicos de direccionamiento IP.
- ✓ Conocimientos básicos en sistemas de archivos.
- ✓ Conocimientos básicos en redes TCP/IP.
- ✓ Conocimientos básicos en resolución de nombres directa y inversa.
- ✓ Las recomendaciones del Anexo G. Recomendaciones Generales.

F.6. Bibliografía y referencias

1. Apuntes del curso el54b: “Sistemas de Procesamiento de la Información”.
2. Apuntes del curso el64e: “Redes de Computadores”.
3. Apuntes del curso el647: “interfaces digitales y Periféricos”.
4. Apuntes del curso el649: “Programación y Operación de Computadores”.
5. Apuntes del curso cc51c: “Comunicación de Datos”.
6. Andrew S. Tanenbaum, "Redes de Computadoras", Tercera Edición, Prentice Hall, 1997.
7. LDP, Anton Chuvakin, “”Pocket” ISP based on RedHat Linux”, http://metalab.unc.edu/pub/Linux/docs/HOWTO/other-formats/pdf/ISP-Setup-RedHat.pdf, 07 de Junio de 2000.
8. LDP, Mark Grennan, “Firewall and Proxy Server HOWTO”, http://metalab.unc.edu/pub/Linux/docs/HOWTO/other-formats/pdf/Firewall-HOWTO.pdf, 07 de Junio de 2000.
9. LDP, Paul Russell, “Linux IPCHAINS-HOWTO”, http://metalab.unc.edu/pub/Linux/docs/HOWTO/other-formats/pdf/IPCHAINS-HOWTO.pdf, 07 de Junio de 2000.

F.7. Plan de acción

Los pasos a seguir en esta experiencia son:

1. Instalación y configuración del firewall.
2. Instalación y configuración del servicio SMTP.
3. Instalación y configuración del servicio POP3.
4. Instalación y configuración del proxy.

F.8. Sección 0: Conexiones

Paso 1 Se debe verificar todo el material.

Paso 2 Realice las conexiones tal como se muestran en el diagrama físico.

F.9. Sección 1: Instalación y configuración de Firewall

Se utilizará tcp_wrappers para esta sección, que es una aplicación de seguridad de fácil manejo.

Con tcp_wrappers se puede implementar un firewall a nivel de la capa de aplicación. Esto se puede hacer con la herramienta de control de acceso tcpd (/usr/sbin/tcpd), que opera como un envoltorio para las aplicaciones, o una aplicación intermedia. Para implementar un firewall a nivel de kernel se puede emplear ipchains.

De este modo, al utilizar uno de los servicios protegidos por tcpd, los accesos son controlados por las reglas definidas en el tcp_wrappers. Nota: esto no opera con los servicios basados en UDP.

Para proteger o monitorear los servicios con tcpd hay que agregarlos en el archivo /etc/inetd.conf. Por ejemplo para proteger el demonio telnet se configura lo siguiente:

```
telnet      stream  tcp       nowait  root    /usr/sbin/tcpd      in.telnetd
```

El control del acceso se implementa mediante dos archivos llamados /etc/hosts.allow y /etc/hosts.deny. Estos archivos contienen entradas permitiendo y denegando acceso, para ciertos servicios y nodos. Cuando tcpd recibe una petición de un servicio como telnet, busca las reglas en hosts.allow y hosts.deny, en ese orden y de acuerdo lo especificado permite o deniega el acceso. Las reglas de acceso en términos globales son las siguientes:

- Si existe una entrada en hosts.allow que calce con la solicitud siempre la acepta, incluso si está denegado en hosts.deny
- Si la solicitud calza con alguna entrada en hosts.deny, la rechaza.
- Si no existe un calce en alguno de los archivos acepta la conexión.

Las entradas en los archivos de acceso tienen la siguiente forma:

```
lista_servicios: lista_nodos [: linea_de_comandos]
```

lista_servicios es una lista de nombres de servicio de /etc/services, o la palabra clave all para indicar todos los servicios. Con except se pueden excluir servicios.

lista_nodos es una lista de nombres de nodos o direcciones IP, o palabras claves all, local o unknown. all calza con todos los nodos, local con los nombres de nodos que no contengan un punto (en general son los especificados en el archivo /etc/hosts) y unknown con los nodos cuya búsqueda de dirección falló. Un nombre que comienza con un punto incluye a todos los nodos del dominio, y una red IP que termina en punto incluye todas las direcciones IP de la red. Mayor información en el manual hosts_access (5) (man 5 hosts_access).

linea_de_comandos es opcional e indica acciones a tomar al permitir o denegar. Es útil para registrar los accesos y los rechazos.

Si no está instalado tcp_wrappers, búsquelo en el cdrom de Linux e instálelo.

A medida que modifica los archivos, pruebe los servicios y observe como cambian los archivos.

Paso 1 Construcción del directorio y archivos de log para tcpd. Siga los comandos mostrados a continuación:

```
[root@almendra /root]# cd /var/log/
[root@almendra log]# mkdir tcpd
[root@almendra log]# cd tcpd/
[root@almendra tcpd]# touch tcpd_rechazos
```

```
[root@almendra tcpd]# touch tcpd_local
[root@almendra tcpd]# touch tcpd_telnet
```

Paso 2 Denegación de todos los servicios.

Edite en `/etc/hosts.deny` y agregue:

```
-----------------------------------------------------------------
all : all : spawn (echo "[`date`]\:%d\:%c\:%u" >> /var/log/tcpd/tcpd_rechazos)
-----------------------------------------------------------------
```

Punto de Control 1: Pruebe un telnet a la máquina, ¿qué sucede?, ahora pruebe un `ping` a la máquina, ¿qué sucede?, hay alguna diferencia, ¿por qué?.

Paso 3 Permitir todos los accesos desde la red local:

Edite en `/etc/hosts.allow` y agregue. Note que registra las acciones en el archivo `/var/log/tcpd/tcpd_local`

```
-----------------------------------------------------------------
all: 192.168.3. : spawn (echo "[`date`]\:%d\:%c\:%u" >>
/var/log/tcpd/tcpd_local)
-----------------------------------------------------------------
```

Paso 4 Permitir telnet a la máquina desde los computadores de la escuela.

```
-----------------------------------------------------------------
in.telnetd: 146.83.4., 146.83.6., .uchile.cl, 10.0. : spawn (echo
"[`date`]\:%d\:%c\:%u" >> /var/log/tcpd/tcpd_telnet)
-----------------------------------------------------------------
```

Paso 5 Permitir ftp, httpd y otros adicionales a la máquina desde todo el mundo, sin registro de acciones:

```
-----------------------------------------------------------------
in.ftpd, httpd, in.identd in.ntalkd, in.talkd  in.ntalkd, in.talkd : all
-----------------------------------------------------------------
```

Punto de Control 2: ¿Verificó que los servicios están operando?, si no lo hizo, hágalo ahora.

F.10. Sección 2: Instalación y configuración de SMTP

Paso 1 Monte el cdrom de Linux, y ubíquese en el directorio de los paquetes.

```
[root@almendra /root]# mount /dev/cdrom
[root@almendra /root]# cd /mnt/cdrom/RedHat/RPMS/
```

Paso 2 Instale los paquetes de `sendmail` (el agente de correos usual en Linux).

```
[root@almendra RPMS]# rpm -i sendmail-8.9.3-20.i386.rpm
[root@almendra RPMS]# rpm -i sendmail-cf-8.9.3-20.i386.rpm
[root@almendra RPMS]# rpm -i sendmail-doc-8.9.3-20.i386.rpm
```

Paso 3 Instale algún cliente de correos.

```
[root@almendra RPMS]# rpm -i pine-4.21-8.i386.rpm
```

Paso 4 Edite el archivo `/etc/sendmail.cw` y agregue los sitios que correspondan, son los dominios configurados en el servidor de nombres en la experiencia 3.

```
[root@almendra RPMS]# cd /etc/
[root@almendra /etc]# vi sendmail.cw

-----------------------------------------------------------------
# sendmail.cw - include all aliases for your machine here.

paredesmoraleda.cl
test.cl
-----------------------------------------------------------------
```

Para mejorar la seguridad del sitio, es mejor tener `sendmail` corriendo desde `inetd.conf` (y así aprovechar al `tcp_wrapper`) y no como un demonio autónomo. Para esto se necesita agregarlo dentro de `/etc/inetd.conf`, y eliminarlo del directorio de demonios `/etc/rc.d/init.d`, también hay que agregar la cola de procesamiento de `sendmail` dentro del `cron`. Para esto:

Paso 5 Agregar la siguiente línea dentro de `/etc/inetd.conf` en la sección de correos (sólo para mantener el orden). Note que en este archivo se habilita el protocolo, el nombre del binario que lo ejecuta es circunstancial.

NOTA: sólo se muestra como debe quedar la sección de correos, el archivo `/etc/inetd.conf` tiene otras configuraciones, NO borre ni cambie las otras opciones:

```
[root@almendra /etc]# vi inetd.conf

-----------------------------------------------------------------
#
# Pop and imap mail services et al
#
#pop-2   stream  tcp     nowait  root    /usr/sbin/tcpd ipop2d
#pop-3   stream  tcp     nowait  root    /usr/sbin/tcpd ipop3d
#imap    stream  tcp     nowait  root    /usr/sbin/tcpd imapd
smtp    stream  tcp     nowait  root    /usr/sbin/tcpd /usr/sbin/sendmail -bs
-----------------------------------------------------------------
```

Paso 6 Edite el archivo `/etc/rc.d/init.d/sendmail`. Al comienzo, luego de la línea de llamada al interprete de comando agregue la línea `exit 0`, de modo que no haga ninguna acción al iniciar `sendmail`, no borre ni cambie nada más del archivo.

```
[root@almendra /etc]# cd /etc/rc.d/init.d/
[root@almendra init.d]# vi sendmail

-----------------------------------------------------------------
#!/bin/sh

exit 0

#
-----------------------------------------------------------------
```

Paso 7 Edite el `crontab` del root y agregue la siguiente línea.

```
[root@almendra init.d]# crontab -e

----------------------------------------------------------------------
*/20 * * * * /usr/sbin/sendmail -q
----------------------------------------------------------------------
```

Con esto se procesara la cola de correos cada 20 minutos (si es que existe algún correo que enviar).

Paso 8 Baje y suba los servicios de red:

```
[root@almendra init.d]# ./inet restart
Stopping INET services:                                    [  OK  ]
Starting INET services:                                    [  OK  ]
```

Punto de Control 3: Envíe correos entre las cuentas que están operando en la máquina. Verifique que los correos son enviados, para ello puede usar el cliente de correos `pine`, u otro que maneje. Notará que si escribe mal la dirección de correos estos no llegarán. ¿De qué depende esto?, ¿Cuáles son los dominios válidos para correos?, ¿Dónde se especificó esto?

_____
_____
_____
_____

F.11. Sección 3: Configuración de POP3

Paso 1 Baje el servidor desde la ubicación indicada a continuación, si no tiene operando la aplicación `wget` tiene dos opciones, instálela o utilice ftp como usuario anónimo.

```
[root@almendra /root]# wget ftp://ftp.qualcomm.com/eudora/servers/unix/popper/qpopper3.0.2.tar.gz
```

Paso 2 Descomprima el archivo:

```
[root@almendra /root]# gunzip qpopper3.0.2.tar.gz
[root@almendra /root]# tar -xvf qpopper3.0.2.tar
```

Paso 3 Cámbiese al directorio de las fuentes de `qpopper`

```
[root@almendra /root]# cd qpopper3.0.2
```

Paso 4 Configure la compilación

```
[root@almendra qpopper3.0.2]# ./configure --enable-specialauth --with-pam --enable-log-login --enable-shy
```

Las opciones utilizadas se ven en la Tabla 14:

Tabla 14. Opciones para la compilación de qpopper

Opción	Explicación
--enable-specialauth	permite shadow passwords, y password MD5.
--with-pam	Permite el uso de la tecnología Red Hat PAM (Pluggable Authentication Modules).
--enable-log-login	Registra los login (ingresos) exitosos, no los defectuosos.
--enable-shy	Encubre el número de la versión.

Paso 5 Compile:

```
[root@almendra qpopper3.0.2]# make
```

Paso 6 Copie el archivo `popper/popper` a `/usr/local/bin` y asigne los permisos indicados:

```
[root@almendra qpopper3.0.2]# cp popper/popper /usr/local/bin
[root@almendra qpopper3.0.2]# chmod 700 /usr/local/bin/popper
[root@almendra qpopper3.0.2]# ls -la /usr/local/bin/popper
```

Paso 7 Agregue (o modifique) la línea indicada al archivo `/etc/inetd.conf`

```
[root@almendra qpopper3.0.2]# cd /etc/
[root@almendra /etc]# vi inetd.conf

-----------------------------------------------------------------
pop3    stream  tcp     nowait  root   /usr/sbin/tcpd /usr/local/bin/popper -s
-----------------------------------------------------------------
```

Para que el `qpopper` solicite autentificación PAM, debe crear un archivo para el servicio POP3 en el directorio `/etc/pam.d/`. El archivo se llamara pop3, el mismo nombre que en el archivo `/etc/services`:

```
[root@almendra /etc]# cd pam.d/
[root@almendra pam.d]# vi pop3

-----------------------------------------------------------------
auth       required    /lib/security/pam_pwdb.so shadow
account    required    /lib/security/pam_pwdb.so
password   required    /lib/security/pam_cracklib.so
password   required    /lib/security/pam_pwdb.so nullok use_authtok md5 shadow
session    required    /lib/security/pam_pwdb.so
-----------------------------------------------------------------
```

Paso 8 Verifique que en el archivo /etc/services exista el servicio pop3, debe aparecer al menos la línea que indica que pop3 opera sobre TCP (si no es así, agréguela). En general POP3 opera sobre TCP, pero no molesta la otra línea, y además es usual configurar para TCP y UDP el mismo puerto para un servicio dado.

```
[root@almendra pam.d]# cd /etc/
[root@almendra /etc]# vi services

-----------------------------------------------------------------
pop3            110/tcp         pop-3           # POP version 3
pop3            110/udp         pop-3
-----------------------------------------------------------------
```

Paso 9 Baje y suba los servicios de red.

```
[root@almendra /etc]# cd /etc/rc.d/init.d/
[root@almendra init.d]# ./inet restart
Stopping INET services:                                    [  OK  ]
Starting INET services:                                    [  OK  ]
```

Punto de Control 4: En el computador cliente configure la una cuenta de correos. Debe ser alguna de las cuentas que están operativas en la máquina que sirve correos. NO utilice la cuenta root para esto. Donde le consulte por el servidor SMTP y POP3 indique el nombre de la máquina que sirve correos. En el caso de la experiencia es `mail.paredesmoraleda.cl`. Este nombre debe estar registrado en el DNS.

Paso 10 Ahora hay que abrir `sendmail` y `popper` en `/etc/hosts.allow`

```
[root@almendra /root]# cd /var/log/tcpd/
[root@almendra tcpd]# touch tcpd_sendmail
[root@almendra tcpd]# touch tcpd_popper
```

Edite en `/etc/hosts.allow` y agregue:

```
-----------------------------------------------------------------
sendmail:     all     :     spawn     (echo     "[`date`]\:%d\:%c\:%u"     >>
/var/log/tcpd/tcpd_sendmail)
popper: all : spawn (echo "[`date`]\:%d\:%c\:%u" >> /var/log/tcpd/tcpd_popper)
-----------------------------------------------------------------
```

F.12. Sección 4: Instalación y configuración de un Proxy como acelerador httpd

Como tendremos en la misma máquina el proxy y el servidor httpd, haremos algunas modificaciones, tanto en el DNS, y la configuración de apache.

Paso 1 Realice las siguientes modificaciones en el DNS de la máquina. Modifique el archivo de zona directo:

```
-----------------------------------------------------------------
proxy           IN      CNAME   ns
-----------------------------------------------------------------
```

y luego reinicie el DNS (`/etc/rc.d/init.d/named restart`)

Paso 2 Cambios en Apache

Cambie la dirección donde escucha solicitudes Apache:

```
[root@almendra /root]# vi /etc/httpd/conf/httpd.conf
```

Busque la línea `Port 80` y cámbiela por:

```
-----------------------------------------------------------------
Port 81
-----------------------------------------------------------------
```

Con esto, Apache escucha las solicitudes por el puerto 81 y no en el 80 (que es el puerto por defecto).

Reinicie el servidor apache. Por seguridad haga dos stop. Lo que sucede es que a veces quedan procesos fantasmas corriendo y se eliminan con el segundo stop.

```
[root@almendra /root]# /etc/rc.d/init.d/httpd stop
[root@almendra /root]# /etc/rc.d/init.d/httpd stop
[root@almendra /root]# /etc/rc.d/init.d/httpd start
```

Punto de Control 5: Verifique que se ve www:81, y que no se ve www:80 con el browser

Paso 3 Instalación del paquete squid.

```
[root@almendra /root]# cd /mnt/cdrom/RedHat/RPMS/
[root@almendra RPMS]# rpm -i squid-2.3.STABLE1-5.i386.rpm
```

Paso 4 Respalde el archivo de configuración de squid.

```
[root@almendra RPMS]# cd /etc/squid
[root@almendra squid]# cp squid.conf squid.conf.old
```

Paso 5 Edite el archivo de configuración de squid con lo siguiente. Busque las líneas en el archivo y cámbielas, si está igual conserve la línea tal como está.

```
[root@almendra squid]# vi squid.conf
```

```
-----------------------------------------------------------------
http_port 80
acl QUERY urlpath_regex cgi-bin \?
no_cache deny QUERY
cache_dir ufs /var/spool/squid 100 16 256
emulate_httpd_log on
redirect_rewrites_host_header off
refresh_pattern         ^ftp:           1440    20%     10080
refresh_pattern         ^gopher:        1440    0%      1440
refresh_pattern         .               0       20%     4320
acl all src 0.0.0.0/0.0.0.0
#acl manager proto cache_object
#acl localhost src 127.0.0.1/255.255.255.255
#acl SSL_ports port 443 563
#acl Safe_ports port 80 21 443 563 70 210 1025-65535
#acl Safe_ports port 280                # http-mgmt
#acl Safe_ports port 488                # gss-http
#acl Safe_ports port 591                # filemaker
#acl Safe_ports port 777                # multiling http
#acl CONNECT method CONNECT
#http_access allow manager localhost
#http_access deny manager
#http_access deny !Safe_ports
#http_access deny CONNECT !SSL_ports
http_access allow all
#http_access allow localhost
#http_access deny all
#icp_access allow all
#miss_access allow all
cache_effective_user squid
cache_effective_group squid
httpd_accel_host 192.168.3.1
httpd_accel_port 81
log_icp_queries off
buffered_logs on
-----------------------------------------------------------------
```

Para esto busque las líneas con el comando de búsqueda de vi (en modo de comandos con `/patron_de_busqueda` un "/" seguido del patrón de búsqueda) y modifíquelas con lo mostrado en la guía (recuerde dejarlas activas), las otras líneas deben estar comentadas (con el caracter #).

Con esto el proxy queda abierto a consultas por parte de los usuarios.

La explicación de algunas de las opciones se ve en la Tabla 15.

Tabla 15. Configuración de squid

Parámetro	Explicación
`http_port 80`	Está usando el puerto 80 !!
`acl QUERY urlpath_regex cgi-bin \?`	Regenera los cgi-bin
`cache_dir ufs /var/spool/squid 100 16 256`	Tamaño del directorio de Cache
`emulate_httpd_log on`	Emulando el servidor httpd
`acl all src 0.0.0.0/0.0.0.0`	Define la lista de acceso que permite a todos
`http_access allow all`	Permite el acceso a todos
`cache_effective_user squid`	Setea el user del proceso a squid
`cache_effective_group squid`	Setea el group del proceso a squid
`httpd_accel_host 192.168.3.1`	Dirección IP del servidor httpd local que acelera
`httpd_accel_port 81`	Puerto del servidor httpd local que acelera

Paso 6 Lance el servidor squid:

```
[root@almendra squid]# /etc/rc.d/init.d/squid start
```

Para lanzarlo en forma permanente, edite el archivo `/etc/rc.d/rc.local`

```
[root@almendra /root]# vi /etc/rc.d/rc.local

----------------------------------------------------------------
#!/bin/sh
#
# This script will be executed *after* all the other init scripts.
# You can put your own initialization stuff in here if you don't
# want to do the full Sys V style init stuff.

# lanzando el DNS
/etc/rc.d/init.d/named start
# lanzando squid
/etc/rc.d/init.d/squid start

----------------------------------------------------------------
```

Con esto, cuando un cliente http se conecte al servidor www, lo que en realidad ve es el servidor proxy (el cliente por defecto se conecta al puerto 80), de modo que si el proxy no tiene la página, la recupera del httpd. Con esto el cliente automáticamente ve al proxy, sin la necesidad de configurarlo manualmente.

Punto de control 7: Para ver como el proxy acumula información, inspeccione el directorio `/var/spool/squid`, y dentro de él vea como aumentan los archivos guardados en los directorios de cache. Como está recién instalado el proxy, observe el directorio `00/00`

F.13. Sección 5: Configuración de un Proxy como web-caching

Acá lo que hay que hacer es cambiar la configuración de los clientes. Importante: para ver los sitios web fuera del sitio local se usa el proxy, y para la red interna no se usa el proxy. Esto se puede configurar en un cliente http tal como es Netscape. En el menú Edición, pinche en las preferencias. Con eso verá la Figura 57.

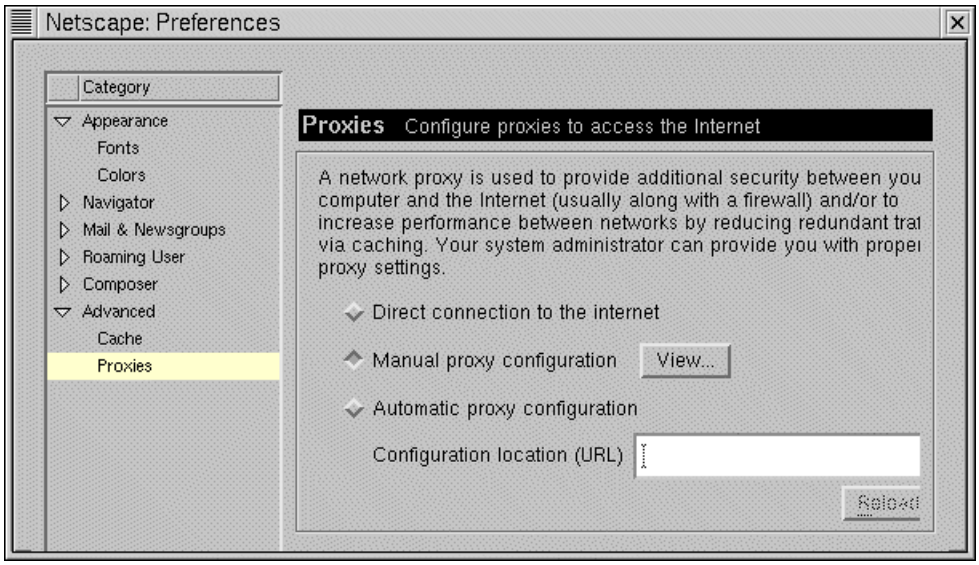


Figura 57. Menú de Preferencias de Netscape

Seleccione los avanzados, y luego proxies, pinche en configuración manual del proxy y luego en view, con esto verá la Figura 58. Llene los valores según se muestra en la figura.

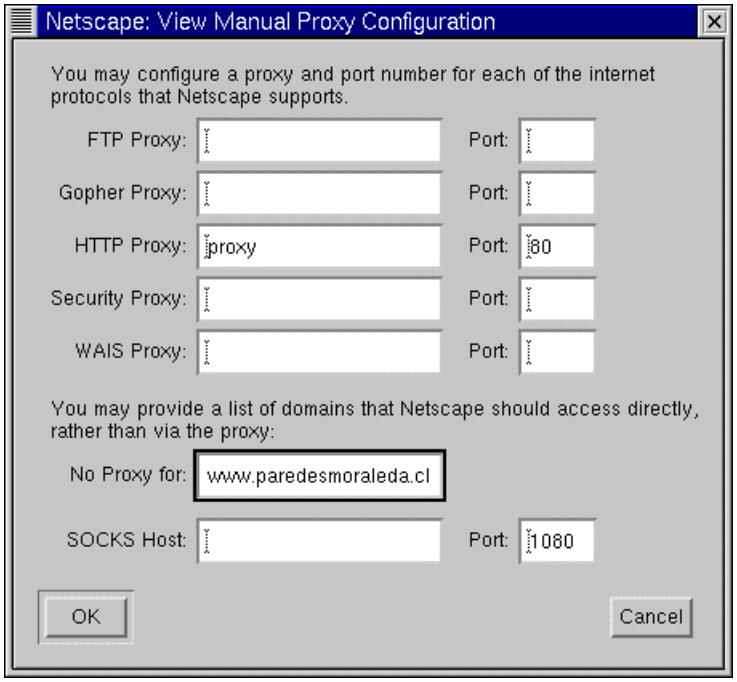


Figura 58. Configuración del proxy en netscape

Con esto, cuando el cliente quiera ver los sitios locales, en realidad se conecta con el proxy pero de modo automático, en cambio cuando quiera salir fuera de la red, se conectará explícitamente a través del proxy.

Punto de control 8: Con algún cliente dentro de la red, busque algún sitio HTML estático (existen varios sitos de este tipo en la red), en otro cliente de la misma red, repita la prueba, y compare los tiempos.

F.14. Sección 6: Bonus: Instalación de Webmin

Para simplificar la configuración de los servicios se tienen varias herramientas gráficas, y algunas de administración vía web.

Uno de ellos es webmin, en esta sección se mostrará su instalación, y se mostrará los servicios que maneja, queda para el alumno probar sus capacidades.

Paso 1 Obtenga el paquete de www.webmin.com, última versión a la fecha del desarrollo de esta guía es webmin-0.80.

Paso 2 Instálelo

```
[root@almendra /root]# rpm -i webmin-0.80.rpm
```

Note que el servicio corre en el puerto 10000

Paso 3 Entre al webmin. En un browser indique la dirección http://www.paredesmoraleda.cl:10000, le solicita login y password, si no ha cambiado el password de root, la password del root es labISP2000. En la Figura 59 se muestra la portada de webmin.

Figura 59. Portada de Webmin

Paso 4 Pinche en la lengueta Servers.

Observe los distintos servidores y las configuraciones. En la Figura 60 se ve la configuración del proxy. Arriba a la izquierda está la ayuda en línea, y arriba a la derecha el controlador de parada y lanzamiento de demonios.

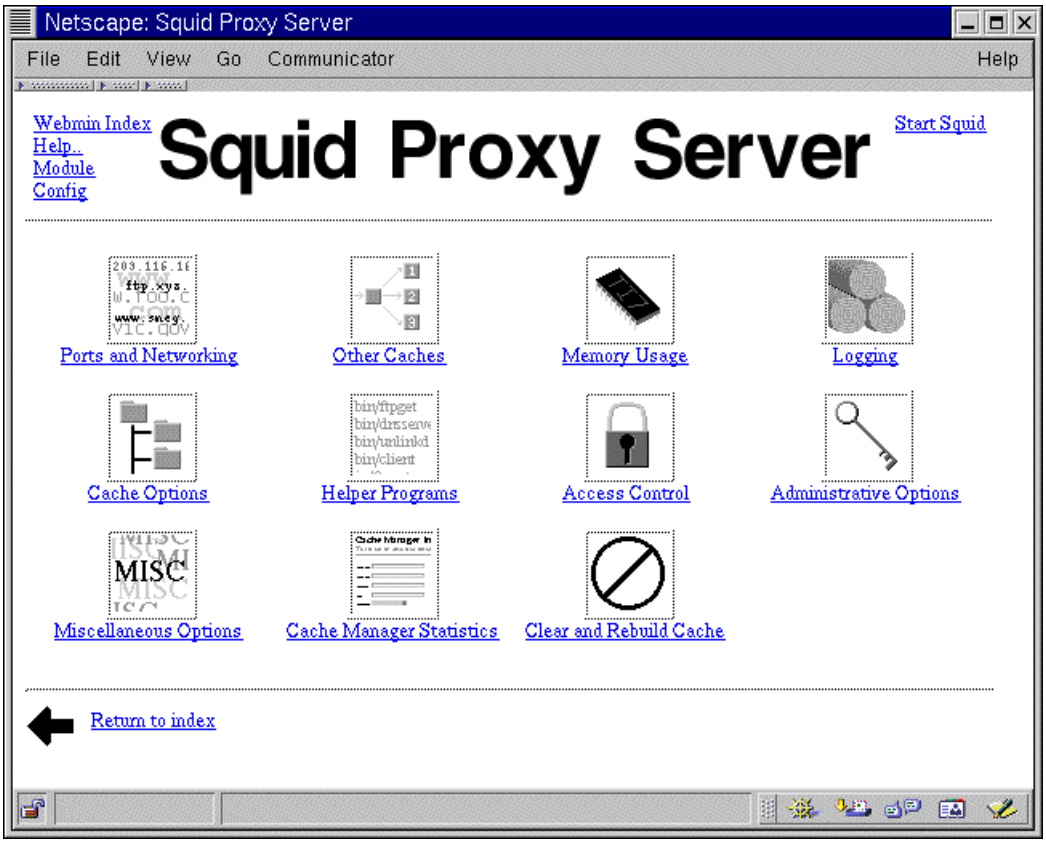


Figura 60. Servidores configurables con Webmin 0.80

F.15. Cuestionario final

1. Cuál es la función de tcpd.
2. Tiene sentido habilitar políticas de seguridad en una red tipo isla.
3. Cuál es el riesgo de manejar servicios autónomos.
4. Cuál es la función de sendmail y popper.
5. Cuál es la función de un proxy.
6. Por que razón se puede habilitar el proxy como un acelerador httpd.
7. En que difiere el cache que manejan los clientes http por separado, y el cache del proxy
8. Tiene sentido habilitar el proxy en una red de:
   8.1. Un computador monousuario.
   8.2. Un computador multisusuario.
   8.3. Varios computadores.

Anexo G. Recomendaciones Generales

1. Debido a que se está operando con equipos que utilizan corriente alterna se insiste en tomar precauciones en el manejo de los equipos.

2. Por simpleza en los procedimientos las experiencias se realizan en modalidad root (superusuario).

3. Si tiene problemas con la memoria del sistema en los procesos de compilación, compile en modo consola, es decir, no compile sobre X windows.

4. Las versiones de los paquetes cambian en el tiempo, luego cuando corresponda instalar algún paquete, tome nota del número de la versión que disponga.

5. En los procesos de configuración de software, es muy probable que cometa algún error durante las modificaciones, por lo cual es sumamente importante que guarde las versiones iniciales de los archivos de configuración antes de hacer un cambio.

6. Los procesos de configuración son altamente iterativos, luego tenga paciencia, y verifique que cada paso se realiza correctamente.

7. Existe una gran variedad de documentación sobre Linux en la Internet, se recomienda que la revise o al menos disponga de una copia electrónica de ellas antes de realizar las experiencias.

8. Cuando realice las conexiones físicas de lo equipos recuerde que está trabajando con equipos eléctricos, y un accidente podría ser grave. Cualquier consideración respecto a la seguridad es válida. La principal es que sea cauto al realizar las conexiones, no fuerze los conectores, y verifique el estado de los interruptores de energía a la hora de encender los equipos.

9. No olvide actualizar el sistema una vez que realice algún cambio. Existen servicios que se acualizan automáticamente, otros en cambio hay que actualizarlos explícitamente bajando y subiendo el servicio. Esto se puede hacer de muchas maneras, pero la usual es `/etc/rc.d/inet.d/demonio restart`

10. Estas experiencias no son de seguridad (o inseguridad) de redes, por lo cual no se tienen grandes consideraciones sobre este tema. Si desea obtener información sobre seguridad en redes dispone de documentación en Internet y también de la memoria de Alberto Castro, disponible en la biblioteca del departamento de Ingeniería Eléctrica.

11. Respecto a la instalación de modems para Linux se recomiendan los modems no PnP. En general los modem externos dan buenos resultados. En algunas experiencias se utilizó el modem/fax interno Zoltrix 14.400, y en otras el modem/fax externo USRobotics Sportster Voice x2.

12. Respecto a la instalación de las tarjetas de red en Linux se recomiendan las 3com, puesto que luego de instalar el módulo apropiado, no se tienen mayores problemas.

13. Para obtener una referencia rápida sobres los temas analizados, términos y acrónimos empleados en el laboratorio se recomienda revisar www.whatis.com.

Anexo H. Configuración de los Computadores de Pruebas

A continuación se detallan las componentes relevantes para el laboratorio de los computadores utilizados, todos ellos cuentan con gabinete mini torre, monitor, teclado, mouse y tarjetas madres acordes con el procesador.

Tabla 16. Configuración del servidor de pruebas 1

Procesador	AMD K6-2/500
Memoria	128 MB
Sistema operativo	Linux Red Hat 6.2 Windows 98
Particiones de disco	4 GB FAT 32 1 GB FAT32 2 GB Linux native (ext2fs) 64 MB Linux swap
Modem	Modem/fax Interno Zoltrix 14.400 US Robotics sportster voice x2 externo
Interfaces de red	3com 509 TP Winbond W89C940
CDROM	Genérico ATAPI IDE 36x

Tabla 17. Configuración del servidor de pruebas 2

Procesador	Intel Celeron 400
Memoria	64 MB
Sistema operativo	Linux Red Hat 6.2
Particiones de disco	8 GB Linux native (ext2fs) 128 MB Linux swap
Modem	US Robotics sportster voice x2 externo
Interfaces de red	Dlink
CDROM	Genérico ATAPI IDE 36x

Tabla 18. Configuración del cliente de pruebas 1

Procesador	Intel Pentium 133
Memoria	64 MB
Sistema operativo	Windows 98
Particiones de disco	2 GB FAT 32
Modem	Modem/fax winmodem interno Motorola 56k
Interfaces de red	Winbond W89C940
CDROM	Genérico ATAPI IDE 12x

Tabla 19. Configuración del cliente de pruebas 2

Procesador	Intel Celeron 400
Memoria	64 MB
Sistema operativo	Windows 98
Particiones de disco	8 GB FAT 32
Interfaces de red	Dlink

Anexo I. ¿Qué es un ISP?

I.1. Generalidades

Un Proveedor de Servicios Internet es una compañía que permite el acceso de otras compañías o individuos a la Internet, ofreciendo servicios Internet y conectividad. Dentro de los servicios que entrega figuran el correo electrónico (e-mail), construcción de sitios Web y su mantención (Web Hosting), servicios de resolución de nombres (DNS), servicios de noticias USENET, servicios de transferencia de archivos (FTP) entre otros.

Un ISP tiene el equipamiento y las líneas de acceso de telecomunicaciones necesarias para constituir un punto de presencia en Internet y así poder prestar servicios en un área geográfica dada. Los grandes ISP poseen enlaces de comunicaciones propios lo que los hace menos dependientes de otros proveedores de telecomunicaciones permitiéndoles de está manera brindar mejores servicios a sus clientes.

Una clase especial de ISP son los proveedores de servicios Internet virtuales (VISP). Un VISP sólo provee los servicios Internet, los que son implementados en la granja de servidores ubicada en la red interna, y no provee servicios de conectividad, sino que los arrienda a otras empresas.

Siguiendo este esquema, se pueden considerar las siguientes visiones:

I.1.1. ¿Cuál es la visión del cliente?

Para los clientes, un ISP tiene básicamente dos funcionalidades:

- Ofrece conectividad a la Internet: El ISP les abre la puerta a la nube Internet, de manera de poder utilizar todos los servicios que ofrece la red.
- Servicios de Internet: Una vez que la conexión se ha establecido, el ISP debe garantizar al cliente la disponibilidad de sus servicios. Se hace un especial hincapié a dos servicios que son masivamente empleados por los usuarios, estos son correo electrónico y WWW. Un tercer servicio de uso masivo es el de transferencia de archivos.

Esto se puede apreciar en la Figura 1:

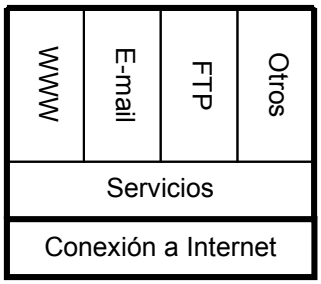


Figura 1: Visión del Cliente de un ISP

Los clientes de un ISP se pueden conectar desde su hogar, oficina, o lugares de acceso público. Para esto deben de disponer del software necesario. Windows 98, Mac OS y Linux, entre otros, incluyen un conjunto de aplicaciones necesarias para establecer su conexión. Esto incluye la pila de protocolos TCP/IP. También se dispone de sitios web en donde pueden bajar aplicaciones libres de costo.

Estos softwares, en combinación a los navegadores web Microsoft Internet Explorer y Netscape Communicator permiten a los usuarios el acceso a Internet, y a sus servicios. Ambos navegadores

implementan HTML (web), NNTP (noticias), FTP (transferencia de archivos) y SMTP/POP3 (correo). En este punto los usuarios están conectados, y pueden obtener más programas.

Para facilitar el proceso de la primera conexión, algunos ISPs distribuyen un CD-ROM con software de licencia pública. Estos CD pueden ser usados como una excelente herramienta de marketing, entregando las aplicaciones preconfiguradas según los intereses del ISP.

I.1.2. ¿Cuál es la visión del proveedor?

La visión del proveedor es mucho más compleja, pues es él quien se encarga de entregar la conectividad a sus clientes. Obviamente, un ISP pequeño puede ser cliente de otro ISP mayor, delegando parte del problema de la conexión a Internet en el ISP mayor.

En términos conceptuales, no existe una gran disparidad entre un ISP y cualquier computador que esté en Internet. La única funcionalidad que marca la diferencia, es que el ISP es capaz de permitir la conexión de otros computadores a través de él, misión que podría asumir cualquier ordenador que ya posea su conexión a Internet. Esta “capacidad especial” se debe a que el “computador ISP”, posee los permisos necesarios para interactuar con otros elementos de la red, tales como modems, routers o switches, que son los dispositivos que permiten el acceso a los clientes.

Por otro lado, el ISP ofrece servicios Internet, que son implementados en la granja de servidores, los que forman la red interna del ISP.

Para facilitar el análisis, el problema se subdivide en varios aspectos:

- Diseño de la red interna del ISP.
- Canal de conexión hacia la Internet.
- Canales de acceso hacia sus clientes.
- Planificación de los servicios prestados.
- Mecanismos de seguridad.

En lo medular todo ISP debe velar por dos objetivos, estos son:

1º Debe conservar alta disponibilidad de conectividad con la Internet y sus clientes.
2º Debe mantener alta disponibilidad en la prestación de los servicios básicos de un ISP.

Todas las otras prestaciones que el cliente desee, pueden obtenerse una vez dentro de Internet, utilizando los recursos que ya existan, por ejemplo para correo Hot Mail, para buscadores en Altavista, sitios de Web Hosting gratuitos, etc.

Siguiendo este desarrollo un ISP básico sólo necesita contar con tres elementos:

- Canal de acceso Cliente – ISP.
- Canal de acceso ISP – Internet.
- Servicios básicos (resolución de nombres).

En este caso, se tiene un ISP que sólo sirve de intermediario entre el cliente y la Internet.

Adicionalmente es sumamente importante implementar mecanismos de seguridad en el sitio, de modo de protegerlo frente a la gran variedad de ataques que disponen los hackers.

Para el caso en que se quieran mayores prestaciones o entregar una mejor calidad de servicio, entra el juego el diseño de la red interna del ISP, y la planificación de los servicios que se ofrecerán a los usuarios. Para un análisis riguroso de está situación, se deben considerar parámetros tales como:

- El número de clientes conmutados y dedicados.
- Cuál es el ancho de banda asignado a los clientes.

- Cuáles servicios se prestaran en forma local desde la red interna, y cuáles desde Internet.
- Cuál es la estimación absoluta y porcentual de tráfico local y externo.
- Qué nivel de tolerancia a fallas se desea para el Sitio.
- Qué tiempo promedio, y mínimo entre fallos se espera.
- Qué especificación se quiere para el tiempo de recuperación de fallos.
- Qué alternativas de redundancia se utilizarán, etc.

Otro dato importante de considerar, es que parte del tráfico externo va dirigido a otros ISP locales, en el caso chileno, otros ISP nacionales, con lo que se divide el tráfico en nacional e internacional. De este modo se podría disminuir notablemente el tráfico hacia la Internet global (que corresponde al tráfico internacional), si existen conexiones interiores con los otros ISP de la región.

Para el diseño de la red interna del ISP, conviene utilizar un modelo jerárquico de capas, de manera de poder dividir funcionalmente el problema. Este modelo permite definir claramente la misión de los elementos de la red, lo que permite administrar la red como una colección de unidades operativas independientes, replicables, y escalables. Por otra parte, un modelo jerárquico permite al administrador detectar, aislar y corregir las fallar con mayor facilidad. En la sección siguiente se mostrará una propuesta de modelo jerárquico para redes.

Para la planificación de servicios, se debe considerar desde la población objetivo, es decir, los requerimientos planteados por los clientes; hasta el nivel de servicios que ofrece la competencia. Es importante destacar que en el corazón de los servicios se encuentra el de resolución de nombres (DNS), pues permite la traducción de nombres a direcciones IP y la traducción reversa, funcionalidad vital en el ambiente Internet.

I.2. Modelo jerárquico de redes

La Figura 2 muestra el modelo jerárquico de redes [Cisco idg4 Basics]. Está compuesto por las siguientes tres capas:

- Capa de Núcleo: Provee un transporte óptimo entre los sitios.
- Capa de Distribución: Provee y administra las políticas de conexión.
- Capa de Acceso Local: Provee el acceso a usuarios y grupos de trabajo a la red.

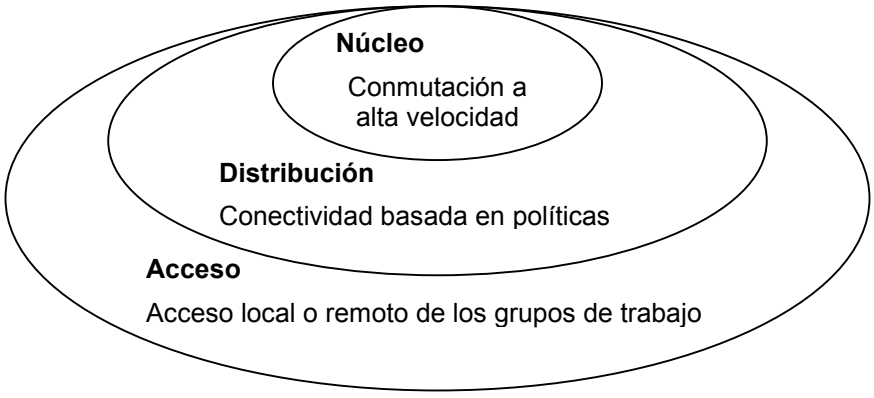


Figura 2: Modelo de Diseño Jerárquico de Redes

I.2.1. Función de la capa de Núcleo

La capa de núcleo constituye el esqueleto de la red, y se debe diseñar de manera que sea capaz de conmutar los paquetes a la mayor velocidad posible. Esta capa de la red no realiza ninguna manipulación

sobre los paquetes (tales como listas de acceso o filtraje) pues esto disminuiría la velocidad en la conmutación de los paquetes.

I.2.2. Función de la capa de Distribución

Esta capa establece la delimitación entre la capa de acceso y la de núcleo, y ayuda a definir y diferenciar el núcleo. El propósito de esta capa es proveer una definición de los límites y es aquí donde toma lugar la manipulación de los paquetes. En ambientes de campus, esta capa puede incluir varias funciones, tales como:

- Agregación de direcciones o áreas.
- Acceso a departamentos o grupos de trabajo.
- Definición de dominios de broadcast y multicast (dominios de difusión colectiva y selectiva, respectivamente).
- Enrutamiento de LAN virtuales (VLAN).
- Adaptación de medios de transporte.
- Seguridad del sitio frente a ataques.

En ambientes que no son del tipo campus, la capa de distribución puede constituirse como el punto de redistribución de los dominios de ruteo, o la zona de demarcación entre los protocolos de ruteo estático y dinámico. También puede ser el punto en el cual los sitios remotos pueden acceder a la red corporativa.

La función de la capa de distribución se puede resumir como la capa que provee las bases de las políticas de conectividad.

I.2.3. Función de la capa de Acceso

La capa de acceso es el punto en el cual se permite el acceso dentro de la red a los usuarios finales locales. Esta capa puede emplear listas de acceso o filtros para optimizar la atención a algún conjunto particular de usuarios. En ambientes de campus, las funciones de esta capa incluyen las siguientes:

- Compartición del ancho de banda.
- Conmutación del ancho de banda.
- Filtraje según la capa MAC.
- Microsegmentación del tráfico.

En los ambientes que no son del tipo campus, la capa de acceso puede entregar acceso a sitios remotos a la red corporativa, vía alguna tecnología de área ancha, tales como Frame Relay, ISDN, o líneas arrendadas.

I.2.4. Algunas consideraciones al modelo

A menudo se piensa erróneamente que las tres capas (núcleo, distribución y acceso) deben existir en entidades físicas claras y distinguibles, pero esto no tiene por qué ser así. Las capas son definidas para apoyar a un diseño exitoso de la red y para representar las funcionalidades que deben existir en una red. La instanciación de cada capa puede ser en distintos routers o switches, puede ser representado por algún medio físico, pueden ser combinados en un único dispositivo, o pueden ser omitidas completamente. Note, sin embargo, que para que la funcionalidad de la red sea óptima, la jerarquía debe ser mantenida.

I.3. Objetivos de un ISP pequeño

Las actividades económicas en Internet pueden ser divididas en brindar facilidades de conexión, que permite a los usuarios comunicarse e intercambiar información; y los servicios de información propiamente tales, por ejemplo: correo electrónico, www, ftp, DNS, etc. [Intel tutorial isp].

Las funciones de conectividad se pueden lograr a través de la jerarquía de los proveedores de servicio.

El papel de un ISP pequeño es proveer acceso local a Internet con la mejor calidad de servicio posible.

Luego del proveedor de acceso local viene una serie de entidades que permiten la comunicación global a través de Internet. El proveedor local es a su vez, cliente de otros proveedores para servicios de backbone, quienes son los responsables de transportar lo paquetes IP a través de grandes distancias. El proveedor de backbone a su vez, emplea los servicios de las compañías que ofrecen circuitos de datos y arriendan líneas de servicio.

Las funciones de los servicios Internet, pueden separarse en las siguientes categorías:

- Portales: Un portal, es un sitio cuya función es conectar a los visitantes con otros sitios. Debe disponer de funciones útiles y atractivas a los usuarios para atraer visitas, por ejemplo, debería disponer de una máquina de búsqueda, informaciones variadas agrupadas en áreas temáticas, etc. La justificación comercial para un portal radica en los auspiciadores y la publicidad en la red. Ejemplos de portales son Yahoo (www.yahoo.com) y Altavista (www.altavista.com).
- Servicios de Backend (servicios de apoyo a la gestión y operación de la empresa): Los servicios de Backend pueden incluir servidores de cache, tecnologías para la operación del motor de búsqueda, servicios para la operación de tarjetas de crédito. Dentro de esta clase también se consideran los servicios de datos que incluyen web hosting y creación de contenidos. Un negocio puede solicitar estos servicios debido a la falta de experticia de sus empleados, o por razones de tiempo.
- Servicios de co-locación (hosting o housing): Esto corresponde al hecho de que los servidores de los clientes son ubicados en las instalaciones del proveedor. Esto mejora considerablemente las velocidades de acceso al servidor del cliente, puesto que el proveedor cuenta con líneas de comunicaciones de mayor velocidad; por otro lado las economías de escala permiten al proveedor instalar a los servidores en un ambiente controlado y seguro a menor costo.

Lo descrito anteriormente muestra la diversidad de servicios que puede ofrecer un ISP pequeño. Un ISP que comienza el cubrimiento de un área sin un acceso previo a Internet, puede comenzar con servicios de web, de noticias, y de correo electrónico. A medida que los requerimientos crecen, se pueden hacer sofisticaciones a los servicios, con esto aparece el servicio de web hosting para personas y empresas, web scripting y generación dinámica de paginas web, comercio electrónico, etc.

I.4. Lineamientos de diseño para ISPs pequeños

Se pueden separar dos grupos dentro de los ISPs pequeños, los que tienen menos de 1000 subscriptores (categoría 1K), y los que tienen menos de 10000 subscriptores (categoría 10 K). Estos ISP enfocan su negocio proveyendo conexión local y servicios de protocolos Internet (IP).

La pregunta que naturalmente surge es: ¿Cuál es la arquitectura de un sistema capaz de proveer los servicios mencionados anteriormente?. Claramente la respuesta a está pregunta no es única, y es fruto de un trabajo continuo y riguroso, tanto en la selección de alternativas como en su sintonización. A continuación se entregarán algunos lineamientos.

La categoría 1K ISP es recomendada para regiones en que la cobertura previa de Internet es débil (por ejemplo, debido a que el ISP más cercano requiere una llamada de larga distancia). Esta configuración se recomienda para ciudades pequeñas. Configuraciones para 10K ISP se recomiendan cuando la base de clientes supera la marca de los 1000, o cuando el estudio indica que este número será rápidamente alcanzado. Se debe tener especial consideración en el hecho de que los aspectos técnicos son sólo una

parte del negocio. La venta, el marketing y el soporte de acceso son aspectos que pueden tomar tanto esfuerzo, o mayor aún que el proceso de adquirir y administrar el equipamiento.

La Figura 3 muestra un ejemplo de configuración mínima para un ISP.

I.4.1. Consideraciones para el establecimiento de un ISP

La primera consideración es el rango de las aplicaciones ofrecidas a los clientes. Un conjunto mínimo de las aplicaciones IP incluyen: correo electrónico (SMTP y POP3), servicios web (HTML), y noticias (NNTP). Para soportar estas aplicaciones, se deben implementar los siguientes servicios: servicios de resolución de nombres (DNS) y servicio de identificación de usuarios (RADIUS). Un servidor de cache es altamente deseable, para poder racionalizar el uso del ancho de banda.

Una red ISP necesita una resistencia inherente a los ataques foráneos o internos. Esto se debe al hecho de que los servidores quedarán expuestos al mundo exterior, prestando servicios a la comunidad de usuarios. Esto lleva a la necesidad de utilizar servidores de protección, conocidos como “firewall”. Para redes pequeñas bastaría con sólo un firewall, en el caso de redes grandes que estén particionadas en subredes, estas subredes se deben aislar a través de un firewall.

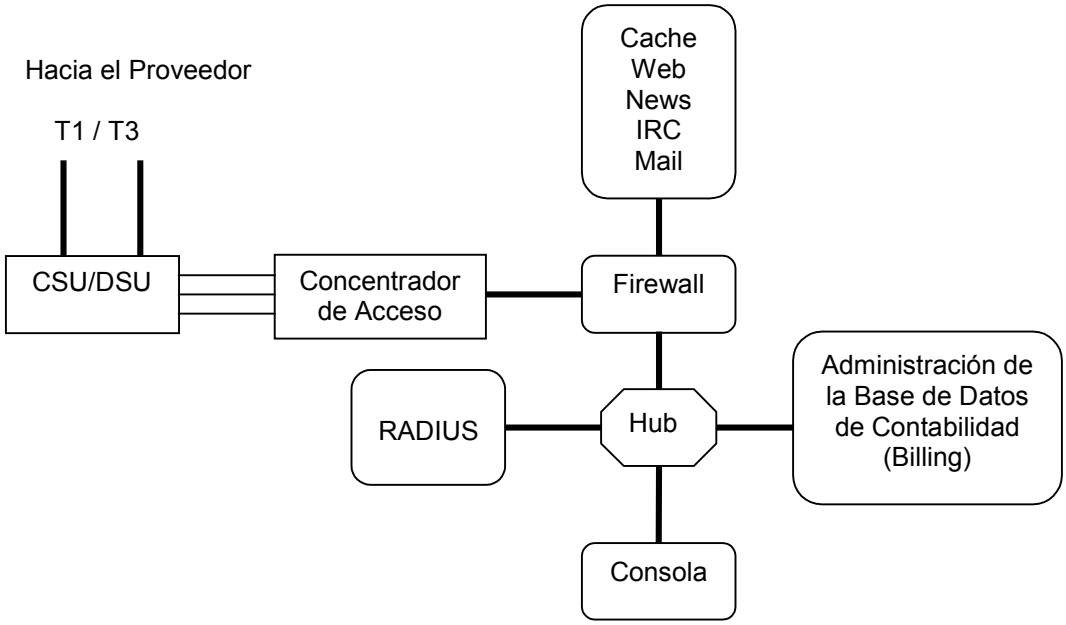


Figura 3: Diagrama en Bloques Mínimo de un ISP

Conectividad

Un ISP pequeño es el primer peldaño en la jerarquía de los proveedores de servicios, conectando su flujo de subida al ISP regional, luego al nacional, y por último al internacional.

La conexión upstream (flujo de subida) al proveedor, también llamada conexión backbone, necesita de ancho de banda suficiente para el punto máximo de la carga. Un criterio de diseño es que se necesita un T1/E1 (1.536/2.048 Mbps) por cada 100 a 200 subscriptores. Otro criterio es, que a plena carga sólo se conecta un 10 % de la población de subscriptores. Con esto se tiene que para una población de 1000 subscriptores, en el peak de se tendrán alrededor de 100 conexiones simultáneas, luego bastaría sólo con una línea E1 para satisfacer las necesidades de tráfico upstream.

La conexión downstream (flujo de bajada) es mucho más exigente, pues no puede considerarse como un canal compartido para los usuarios. Luego para 100 subscriptores, se necesitan 100 líneas troncales, alrededor de 6.4 Mbps, lo que requiere aproximadamente 4 T1, o 3 E1.

El equipamiento tradicional de acceso para clientes conmutados es un banco de modems, aún usado en algunos sitios. Esta configuración además de ser voluminosa y compleja, tiene la desventaja de que no soporta el protocolo V.90, que transmite a 56 Kbps. Para esta labor se prefiere utilizar un terminal concentrador.

Administración de redes

La configuración inicial puede ser de una o dos redes separadas por un firewall. Como se ve en la Figura 3, una implementación para un ISP pequeño, podría consistir en una red de cuatro servidores, los que deben realizar varias tareas cada uno. Para cumplir esta labor, se recomienda el uso del sistema operativo Linux.

A medida que la red crece, se recomienda que algunas aplicaciones, tales como el servidor de correo, se trasladen a un servidor dedicado. Cuando todos los servicios utilicen su servidor propio, se puede mejorar el rendimiento mejorando el hardware de la instalación, esto no sólo significa emplear procesadores más rápidos, también influye la memoria RAM de los sistemas, el disco duro, etc. Hay que recordar que si la aplicación no es multithreading (ejecución paralela) no se obtiene mayor beneficio utilizando multiprocesadores. Otra opción a considerar es utilizar la versión propietaria sintonizada al caso en cuestión, en vez de la versión abierta del producto.

Otra manera de mejorar el rendimiento, es utilizar la descomposición funcional: la función del servidor de correo puede ser descompuesta en la función del agente de transferencia de correos (MTA) y la función de almacenaje de correos, las que podría correr en máquinas separadas. Cuando la transición ocurra, el ISP no podrá volver a ser llamado pequeño.

La mayoría de las distribuciones de Linux (Red Hat, S.u.S.E, Debian) incluyen las aplicaciones básicas para instalar un ISP. Aplicaciones específicas pueden ser adquiridas con proveedores de software. La mayoría de los sistemas operativos modernos implementan los Protocolos Internet (IP) y sus servicios son altamente interoperables, siguiendo esta política de minimizar el costo de las licencias de los softwares, con un impacto positivo en los flujos de caja.

Seguridad

Las grandes instalaciones pueden contener múltiples subredes, definiendo capas de protección. En la fachada del sitio (frontend) se ubican las máquinas que proveen servicios IP, en una capa intermedia están los servidores de aplicación, y en la capa posterior (backend) los servidores que administran las bases de datos. Esta arquitectura define capas sucesivas que incrementan los niveles de seguridad. Un firewall puede ser configurado para implementar políticas que mejoren la seguridad, tales como dirigir el tráfico de correo sólo a los servidores de correo, o los paquetes http a los servidores web.

I.4.2. Equipamiento Computacional

Una elección importante para el ISP es la arquitectura de los computadores. Existen varias arquitecturas compitiendo en este mercado: SPARC, PowerPC, MIPS, Intel. La primera preocupación del ISP es la confiabilidad de su equipamiento. Se puede mejorar la confiabilidad de los equipos instalado sistemas redundantes, lo que también sube los costos.

El equipamiento SPARC ha sido bien considerado para la instalación de ISP, debido a la estabilidad de los sistemas SPARC combinados con el sistema operativo Solaris, y además, porque el fabricante, Sun Microsystems, Inc., ha hecho de Internet el foco de sus esfuerzos de marketing por varios años.

Otra familia con presencia en ISP es Intel. Esto se puede explicar por la gran cantidad de abastecedores de productos Intel, y además por la gran variedad de sistemas operativos que operan sobre esta plataforma.

La configuración mínima para un ISP comercial está formada por tres servidores: el primero para correr los servicios de administración, el segundo para correr los servicios IP y para autentificación y acceso de usuarios, y el tercero de repuesto. El servidor de repuesto puede ocuparse de las tareas no esenciales, y debe estar listo para reemplazar a uno de los dos servidores cuando uno de ellos falle. Para una mayor flexibilidad, se recomienda que los tres servidores posean la misma configuración. También es deseable que los servidores cuenten con un sistema RAID (RAID: arreglo redundante de disco baratos) con discos hot swap (discos de reemplazo en funcionamiento), y que el servidor de reemplazo ubicado en la misma instalación. Si algún disco falla, el servidor de reemplazo es usado para reconstituir el RAID. Si algún servidor falla, se retira de la red, su RAID se instala en el servidor de reemplazo, se repara la falla, y se vuelve a la configuración inicial. Con este esquema se asegura un mínimo de tiempo de falla, con una bajo gasto de capital. La configuración de tres servidores tiene la capacidad suficiente para ISP 1K.

Esta configuración puede ser mejorada adicionándole un firewall, de manera de mejorar el control sobre los paquetes y elevar los niveles de seguridad. Para este caso, cada servidor debe poseer dos interfaces de red, una mirando al frontend de la red, en donde se ofrecen los servicios IP, y la otra mirando al backend, donde se llevan los procesos de administración.

Administración de clientes

Esta labor se puede realizar con un computador de escritorio (procesador Pentium II, 128 MB en memoria, 8 GB en disco duro IDE). Este equipo se puede utilizar como servidor de impresión.

Otros accesorios computacionales

Dispositivos de respaldo en cinta: El respaldo de datos debe ser realizado a intervalos regulares, siguiendo una política establecida. Una máquina de procesador dual puede ser útil para esta tarea, puesto que el sistema operativo puede balancear la carga del proceso de respaldo, con la carga normal de operación, disminuyendo el impacto en el tiempo de respuesta percibido por los usuarios.

Quemadores de CD: Los grabadores de CD ROM son útiles para realizar copias de respaldo de software crítico. Los discos regrabables pueden usarse para guardar copias de datos de operación críticos. Lamentablemente el uso de estos dispositivos de respaldo, esta limitado por su capacidad de 640 MB. Con el surgimiento de los grabadores para DVD se podrá aumentar la capacidad de almacenamiento a 17 GB en un único disco.

Impresoras: A menos que el ISP provea el servicio de impresión a sus clientes, no hay grandes requerimientos para impresión. Para el ISP basta con tener una impresora de tinta, o una impresora láser de capacidad media.

Unidades de respaldo de energía: Dentro de las medidas para el aseguramiento de disponibilidad de servicio y de protección eléctrica a los equipos, se tiene la del empleo de Sistemas de Energía Ininterrumpida (UPS).

I.4.3. Equipamiento de redes

CSU/DTU

El CSU/DTU (unidad de servicio al cliente / unidad de servicio de datos) es el dispositivo terminal para el backbone del ISP, y para las líneas de conexión de los abonados. Tanto las conexiones de subida como las de bajada son realizadas a través de compañías de telecomunicaciones (portadora). Este dispositivo puede ser arrendado o comprado a la portadora.

Servidores de Acceso

El servidor de acceso es un dispositivo que viene a reemplazar los antiguos bancos de modems. Ya no se recomienda el uso de bancos de modems debido a que no soportan la norma de modems V.90 (33.6 Kbps en subida y 56 Kbps en bajada) debido a una conversión análogo digital extra.

Servidores de acceso populares son de la serie Ascend Max y Livingston Portmaster. Ambas compañías son ahora parte de Lucent Corporation. También se cuenta con el switch de acceso Shiva LANRover de Intel.

I.4.4. Software

La elección del software a utilizar queda subordinada a la elección del sistema operativo. Dentro de las alternativas de sistema operativo se tiene como las más usuales Microsoft Windows NT y Unix en todos sus sabores: Sunsoft Solaris, SunOS 4, o las distribuciones de Linux.

Una razón para escoger NT es evitar aprender de Unix. Tener conocimiento de los sistemas Unix es esencial debido a que muchos computadores en la Internet corren algún sabor de Unix, y los protocolos fundamentales para Internet fueron originalmente investigados y desarrollados para plataformas Unix. Más aún, algunas aplicaciones que corren sobre NT tienen parte de códigos que fueron desarrollados para software de la plataforma Unix. Desconocer la arquitectura del sistema Unix, podría llevar a perdidas de tiempo valioso producto de problemas usuales en la operación del ISP.

Existen varios sitios que tienen software disponible para Linux. Se recomienda visitar http://charter.Linuxberg.com, y http://www.tucows.com.

Servidores web

Existe una gran variedad de software diseñado para distribuir páginas web y aplicaciones para mejorar la prestaciones por web, entre ellas se tiene:

- Apache: Apache es el servidor web más ampliamente utilizado en Internet, más de la mitad de los sitios en el mundo lo utilizan. Está disponible para la mayoría de los sistemas operativos. Vea http://www.apache.org.
- Dbedit: Una buena característica del web es la posibilidad de servir como interfaz para las bases de datos. Dbedit permite la interacción entre páginas web y bases de datos. Vea http://metalab.unc.edu/pub/Linux/apps/database/www.
- Hawkeye: Hawkeye provee un conjunto de aplicaciones TCP/IP integradas que incluyen servidores HTML (web), SMTP/POP3 (correo), NNTP (noticias), FTP(transferencia de archivos) y chat. Originalmente fue desarrollado para correr en Linux. Requiere MySQL. Vea http://www.hawkeye.net.

Servidores para transferencia de archivos

Los programas FTP (protocolo de transferencia de archivos) permiten la transferencia de archivos desde / hacia los sitios FTP. Un cliente FTP es un programa capaz de conectarse con un sitio FTP para subir / bajar archivos al / del sitio. El servidor FTP es el programa que corre en el lado del servidor.

Linux viene con una versión de FTP. Otros servidores FTP son:

- NcFTPd: Es una reimplementación de la versión abierta optimizada para sitios ftp de gran volumen. Tiene licencia comercial. Vea http://www.ncftp.com.
- ProFTPd: Es un servidor FTP para Linux y Unix. Ofrece mejores prestaciones, seguridad y facilidad de administración que la versión estándar abierta del servidor FTP. Las facilidades de configuración y administración son muy similares al Apache. Vea http://www.proftpd.com.

Servidor de resolución de nombres

Un servidor de resolución de nombres (DNS), hace la traducción entre nombres de computadores hacia direcciones IP y viceversa. Por ejemplo convierte www.uchile.cl a 146.83.12.32. Utilitarios como `nslookup` en Unix realizan consultas al servidor DNS para hacer la conversión nombre computador / dirección IP.

- BIND: Es la versión estándar de Internet para DNS, viene incluido en la mayoría de las distribuciones de Linux. El paquete incluye el servidor DNS, la librería para resolución de nombres, y herramientas para verificar la buena operación del servidor DNS. Vea http://www.isc.org/bind.html.
- WebDNS: Provee una interfaz CGI para configurar servidores DNS. Su uso primario es hacer más rápido y fácil la adición de nuevas entradas a los archivos de configuración del DNS. Requiere la librería `cigc` disponible en http://www.boutell.com/cigc. Vea http://www.darkfires.net/webdns.

Agentes de transferencia de correo electrónico

El correo electrónico es una tecnología de almacenamiento y envío. Un MTA (agente de transferencia de correo) es el programa que lleva a cabo esta función. El cliente destino puede estar desconectado cuando el correo llega. Un programa que almacena correos corriendo el protocolo POP3 o IMAP es usado por el ISP destino para conservar los mensajes hasta que ellos sean descargados hasta el cliente destino.

- Sendmail: Es la implementación por defecto para los correos en Internet actualmente. Esta instalado por sobre un 75 % de los servidores de correo en Internet. Viene incluido en la mayoría de las distribuciones Linux. Vea http://www.sendmail.org.
- Qmail: Es una alternativa a Sendmail. Este paquete fue diseñado para confiabilidad, seguridad, desempeño y economía en la utilización de recursos. Puede ser usado junto a los programas de almacenamiento `qpopper` o `ipop3d`. Vea http://www.qmail.org.

Software para servidores de correo electrónico

IMAP (protocolo de acceso de mensajes Internet), es un método para una máquina “post office” (oficina de despacho) que acumula el correo de los usuarios y los envía a la máquina local del usuario para que lea sus correos. IMAP provee la misma funcionalidad que POP, y permite a los usuarios leer correos en una máquina remota sin tener que mover su correo local. Vea las siguientes direcciones: http://www.washington.edu/imap o http://www.imap.org.

- Cyrus IMAP server: La universidad Carnegie Mellon tiene una implementación de IMAP. Sólo está la implementación del servidor donde el usuario final no tiene permitido el acceso. Los correos son mantenidos en una base de datos privada. Se diseñó pensando en la eficiencia, desempeño, escalabilidad y seguridad. Vea http://andrew2.andrew.cmu.edu/cyrus/imapd.
- Netscape Messaging Server: Es la implementación Netscape de IMAP. Es una implementación escalable y confiable. Toma ventajas del procesamiento paralelo de las tareas. Cuenta con facilidades de cache. Tiene licencia comercial. Vea http://home.netscape.com/messaging.

Servidores BOOTP/DHCP

BOOTP corresponde al protocolo Bootstrap y DHCP al protocolo de configuración dinámica de computadores. BOOTP permite que un usuario de la red sea automáticamente configurado, es decir, que soporte una asignación dinámica de una dirección IP de un conjunto de direcciones disponibles. BOOTP también permite inicial el sistema operativo sin interactuar con el usuario. BOOTP y DHCP proveen un marco de trabajo que entrega la información suficiente para configurar computadores en una red TCP/IP (Vea el RFC 2131 DHCP en http://www.ietf.org/rfc/rfc2131.txt). Con esto se consigue que los equipos (computadores personales, servidores de impresión, terminales X, etcétera) no tiene que ser previamente configurados para que puedan comunicarse utilizando el conjunto de protocolos TCP/IP.

- BOOTP/DHCP Server: Vea http://www.geckil.com/~harvest/tcpip-docs/bootpd.html.

Firewall

Un firewall no es sólo un programa, es una combinación de routers, computadores y redes con un software apropiado para implementar políticas de seguridad entre una red protegida y la red externa (Internet). Las funciones implementadas por un firewall incluyen el filtraje de paquetes, por ejemplo dirigir los paquetes http sólo hacia el servidor web. In este caso, cada paquete es examinado independientemente de los otros. Una inspección completa del estado, también puede ser implementada para agregar seguridad.

En http://metalab.unc.edu/mdw/HOWTO/Firewall-HOWTO.html se puede encontrar información adicional sobre firewalls para Linux. También se encuentra información en el sitio de Trusted Information Systems en http://www.tis.com.

Un programa que administra algunas funciones de firewall para Linux es `ipfwadm`, está descrito en http://www.xos.nl/linux/ipfwadm.

Servidores de Chat

Para instalar un servidor de Chat, se tienen versiones publicadas para bajar en http://charter.Linuxberg.com.

- IRCd: Es la versión estándar para los servidores de chat, viene incluida en la mayoría de las distribuciones de Linux. Vea ftp://ftp.irc.org/irc/server y http://www.stealth.net/~kalt/irc/faq.html.

Servidores de noticias

Los softwares de noticias permiten acceder a los grupos de noticias Usenet. En Internet, esto es equivalente al diario mural. Actualmente hay alrededor de 30.000 tópicos, en donde los usuarios pueden leer los artículos publicados, y publicar sus comentarios.

- Dnews: Está ampliamente establecido a nivel Internet, tiene buena documentación y soporte y es fácil de instalar. Es soportado bajo Linux. Vea http://netwinsite.com.
- INN: Presente en la mayoría de las distribuciones de Linux, INN es un completo sistema Usenet. Vea: http://www.redhat.com/corp/support/docs/INN-Tips/INN-TIPs-3.html.

Servidores de Proxy y Cache

Los servidores Proxy son utilizados para proveer un único punto de acceso para los usuarios externos que miran dentro de la red, haciendo más fácil para el administrador la tarea de implementar las políticas de seguridad y las funciones de cache. Los servidores Proxy también funcionan como un embudo para los usuarios dentro de la red, con lo que facilitan el cumplimiento de las funciones de seguridad como el logging y el caching.

- Squid: Ofrece un buen desempeño como cache proxy para clientes web, y soporta requerimientos FTP, Gopher y HTTP. Viene incluido en la distribución Red Hat Linux. Vea http://squid.nlanr.net.

Existen versiones comerciales que realizan funciones de proxy y cache, tales como Traffic Server de Inktomi, Border Manager de Novell.

Software para bases de datos

Los servidores de bases de datos pueden ser usados para guardar la información contable (información sobre el número de accesos, volumen del tráfico, etcétera) de los clientes.

- Essentia: Es un motor de bases de datos con características tales como chequeo automático de consistencia, respaldos incrementales, administración de replicas de la base de datos, transacciones de dos fases (útiles para consultas remotas), conectividad con bases de dato Java (JDBC) y

conexiones a bases de datos abiertas (ODBC). Vea http://metalab.unc.edu/pub/Linux/apps/database/essentia.

- PostgreSQL: Es un administrador de base de datos relacional (DBMS), que soporta la mayoría de las sentencias SQL, incluyendo subconsultas, transacciones, definición de tipos de usuario y funciones. Viene distribuido con Red Hat Linux. Vea http://postgresql.nextpath.com.

Paquetes de contabilidad para ISP

Los softwares de administración de contabilidad permiten llevar estadísticas del consumo de los usuarios, de manera de poder tarifar dicho consumo. A continuación se muestran algunas versiones que trabajan sobre Linux:

- User Tracking & Accounting, de la empresa RTD Systems & Networking, Inc. Ver: http://www.rtd.com/software/uta.html.
- Regulus 1.4, de la empresa S.A.F.E. Ver: http://www.regulus.safe.ca.
- Internet Billing, Internet Admin, de la empresa Collword.com Inc. http://www.coolworld.com.

Existen otras aplicaciones para este tipo de requerimientos, pero no todas ellas pueden trabajan sobre Linux, lo que eventualmente podría complicar la operación del ISP. En www.isp-lists.com/isp-invoicing hay un grupo de discusión y recursos adicionales.

I.5. Bibliografía

I.5.1. Referencias electrónicas

[Cisco idg4 Basics] Cisco Systems, "Internetworking Design Basics", http://www.cisco.com/univercd/cc/td/doc/cisintwk/idg4/nd2002.htm, 06 de Enero de 2000.

[Intel tutorial isp] Intel, "Design Guide for Small ISPs", http://www.intel.com/isp/whitepaper/ispSmallBusiness.PDF, 10 de Enero de 2000.

Anexo J. Resolviendo Problemas

J.1. No se reconoce la tarjeta de red 3Com Etherlink III 3c509b bajo Linux

Tiempo estimado: 1.5 horas

Paso 1 Primero que nada, hay que asegurarse que la tarjeta NO este en modo Plug and Play, debe estar operando en modo ISA.

Esto se puede verificar manualmente, utilizando el programa de configuración que provee el fabricante, para eso hay que tener los drivers de la tarjeta. De no tenerlos a mano, se deben buscar en la red. Generalmente los fabricantes tienen drivers disponibles para ser bajados. Para este caso visite el sitio http://www.3com.com, y busque los drivers que corresponden a la tarjeta.

Paso 2 Con el programa de configuración de la tarjeta de red se debe deshabilitar el modo PnP, asignar una IRQ y asignar una dirección de entrada/salida, ejemplo de esto puede ser:

IRQ 3, I/O Address 0x300

Tenga el cuidado de leer la documentación que viene en los archivos, en general estos programas tienen ciertas restricciones, tales como que sólo operan bajo MS-DOS, o similares.

Paso 3 Esta tarjeta tiene drivers especializados para Linux, en la versión Red Hat 6.1 puede encontrar el archivo en /usr/src/linux/drivers/net/3c509.c, y el archivo compilado o módulo compilado en /lib/modules/2.2.14-5.0/net/3c509.o con los cuales habilitará la tarjeta. Si no encuentra el driver en su distribución, búsquelo en la red.

Para una instalación temporal del módulo, utilice el comando:

```
/sbin/insmod /lib/modules/2.2.14-5.0/net/3c509.o
```

y para verificar que el sistema operativo ve la tarjeta utilice el comando:

```
ifconfig
```

Paso 4 Para una instalación permanente del módulo, en el directorio /etc/rc.d/inet.d agregue el siguiente script, note que la versión de la librería depende de su distribución (en el ejemplo corresponde la versión 2.2.14-5.0).

El nombre del script es 3c509.

```
#!/bin/sh
#
# 3c509       Scrip para hacer funcionar la tarjeta de red 3c509

/sbin/insmod /lib/modules/2.2.14-5.0/net/3c509.o
```

Luego agregue un link en el directorio /etc/rc.d/rc3.d referenciando al script anterior, para eso ejecute lo siguiente:

```
cd /etc/rc.d/rc3.d
ln -s /etc/rc.d/inet.d/3c509 S093c509
```

Note el formato del nombre del link, SXXAAAAA, este formato se refiere a lo siguiente:

- S: Se ejecuta al arranque de la máquina
- XX: Es un número entre 00 y 99 que indica la prioridad de ejecución del script, mientras más pequeño antes se ejecuta. Para el ejemplo se seleccionó 09, puesto que correspondía a un nivel de prioridad posterior a kudzu (kudzu se ejecuta con prioridad 05 y una aplicación Linux que detecta y configura hardware nuevo) y previo a la ejecución del script de red (que tiene un nivel de prioridad de 10).
- AAAAA: Corresponde a una secuencia alfanumérica de largo variable que se utiliza para identificar el script que se ejecutará.

Paso 5 Luego de esto, es probable que tenga que configurar los parámetros para redes tcp/ip, esto se resuelve utilizando el programa netconf, e ingrese los datos que le pide el programa. NO olvide consultarle al administrador de red cual es el número IP de su máquina, el router de su red, en servidor de nombres, y la máscara de la red.

Punto de control 1: Una vez que arranque el computador, verifique el funcionamiento con la tarjeta de red a través del comando:

```
ifconfig –a
```

La salida debiera ser similar a esta:

```
eth0      Link encap:Ethernet  HWaddr 00:A0:24:C6:B4:71
          inet addr:200.27.6.30  Bcast:200.27.6.63  Mask:255.255.255.192
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:109160 errors:2 dropped:0 overruns:0 frame:2
          TX packets:3676 errors:0 dropped:0 overruns:0 carrier:2
          collisions:76 txqueuelen:100
          Interrupt:3 Base address:0x300

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:3924  Metric:1
          RX packets:427 errors:0 dropped:0 overruns:0 frame:0
          TX packets:427 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
```

Si el sistema no ve la tarjeta (en este caso eth0), pruebe exhaustivamente crear el link en los otros niveles de ejecución, es decir pruebe con rc0.d, rc1.d, …, rc7.d, hasta que encuentre el correcto.