Capítulo 4

SEGURIDAD Y SERVICIOS UN PROVEEDOR DE SERVICIO DE INTERNET

A continuación se describe como funciona y configuraciones de los servicios que puede ofrecer un ISP, dentro las dos plataformas más utilizadas y las cuales se han tomado como punto de referencia para nuestro estudio.

4.1. 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.

4.1.1. Servicio de Resolución de Nombres DNS

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.

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)

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. Dependiendo de su localización en la jerarquía, un dominio puede ser de primer, segundo o tercer nivel. Estos dominios se muestran en la Tabla 4.1.

Los dominios geográficos o de país. Esto son todos los dominios de tres caracteres que están basados en los códigos de países definidos por ISO 3166.

Dominio	**Descripción**
edu	Aquí están incluidos todas las universidades y centros educativos.
com	Empresas, organizaciones y compañías comerciales
org	Organizaciones no comerciales. Las redes UUCP privadas están en este dominio.
net	Empresas dedicadas a conexiones de Redes.
mil	Usados por los grupos militares
gov	Empresa o Grupos de gobiernos.
int	Empresa u Organizaciones Internacionales.
uucp	Oficialmente todos los nombres de nodos UUCP sin dominio fueron movidos a este nuevo dominio.

Tabla 4.1. Dominios genéricos

Se conoce actualmente como Sistema de Nombres de Dominio, que en esencia es una base de datos distribuida, gracias a lo cual permite la administración y control local de los fragmentos en que se divide. Funciona a través del esquema cliente-servidor y está diseñado de forma eficiente para lograr un buen rendimiento, además de permitir la replicación y el *cachè*.

Un servidor de nombres es la máquina que ejecuta el programa que implementa la parte servidora del esquema. Este se encarga de almacenar la información asociada al segmento de la base de datos que controla, y de mantenerla accesible a los clientes, que se conocen como *resolvers*. Un *resolver* es una subrutina que genera consultas y las envía a través de la red hacia el servidor de nombres correspondiente.

El Sistema de Nombres de Dominio (*Domain Name System*) es un poderoso y complejo mecanismo que permite entre otras posibilidades, la traducción de nombres a direcciones IP (y viceversa), en las redes computacionales. Este sistema tiene una estructura que responde ante las características actuales de las redes de computadoras, dada su expansión y diversificación.

Las direcciones IP identifican unívocamente a las máquinas de una red permitiendo la comunicación entre estas a través de diversos protocolos con el objetivo de acceder o brindar múltiples servicios.

La primera forma que se utilizó para convertir nombres a números IP y viceversa fue a través de un fichero nombrado HOSTS.TXT el cual debería estar distribuido en todas las máquinas que necesitaban el servicio. Este simplemente contenía una tabla que expresaba la correspondencia entre un número IP y uno o varios nombres. Ejemplo: Tabla 4.2.

Dirección IP	D N S
135.105.32.43	Google
128.102.25.59	Altavista
32.31.5.169	Monografías
192.188.35.9	El Universo

Tabla 4.2. Relación de de Direcciones IP con DNS

4.1.1.1 Espacio de Nombres de Dominio

La estructura de la base de datos del DNS posee una forma jerárquica similar al sistema de ficheros de Linux, ver figura 4.1. Esta es una especie de árbol invertido donde cada nodo representa un segmento o dominio. Los nodos a su vez pueden poseer varios subnodos hijos que constituyen subdominios en el DNS -subdirectorios en el *file system* de Linux. Por último, los nodos que no poseen hijos pueden verse como los nombres de los *hosts* que pertenecen al dominio definido por el nodo padre. Cada nodo se identifica utilizando una etiqueta cuyo tamaño no debe exceder los 63 caracteres. El nodo raíz tiene una etiqueta vacía (longitud cero). Las etiquetas se separan utilizando el caracter "." y se ordenan de abajo hacia arriba a diferencia de los caminos absolutos en el sistema de ficheros de Linux. Ejemplos de nombres en el DNS son:

- www.altavista.com
- www.bacan.con
- www.loteria.com.ec
- www.espol.lsi.edu.ec

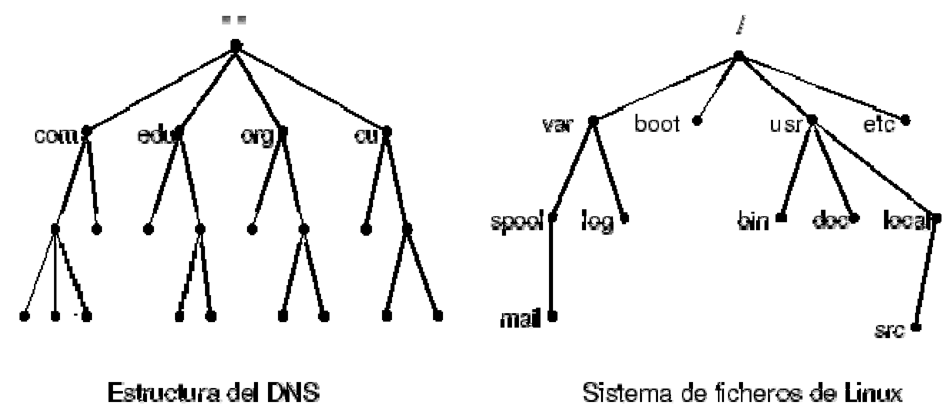

Figura 4.1. Semejanzas entre la estructura del DNS y el sistema de ficheros de Linux

Como conclusión tenemos que un dominio es simplemente un subárbol del espacio de nombres. El nombre de un dominio es el nombre del nodo raíz correspondiente. Un dominio agrupa un conjunto de *hosts* y/o subdominios que se relacionan de acuerdo a cierto criterio, ya sea geográfico u organizacional. En el DNS cada dominio es administrado por una organización o empresa determinada. Esta puede decidir dividir el o los dominios que administra en subdominios, así como asignar la administración de estos a otras entidades. Cada dominio puede contener tanto subdominios como *hosts* independientes, al igual que un directorio posee subdirectorios y ficheros a la vez.

4.1.2. 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.

Los MTAs (*Mail Transport Agent*) o agentes para la transmisión de correo son aquellos programas servidores que permiten transportar el correo electrónico de una máquina a otra a través de la red.

El SMTP como su nombre lo indica es un protocolo muy simple orientado a caracteres y que permite el traslado de los correos tanto desde el cliente al servidor como entre servidores.

Los MUAs (*Mail User Agents*) que son los programas clientes que posibilitan a los usuarios manipular su mensajería. Estos programas son ejecutados directamente por los usuarios. Proveen facilidades para escribir los mensajes, enviarlos, descargar y leer los que llegan, organizarlos en directorios, hacer búsquedas, imprimirlos, mantener un libro de direcciones electrónicas, etc.

El mecanismo de envío de mensajes se ve en la Figura 4.2. 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 los datos ordenados y confiables (TCP).

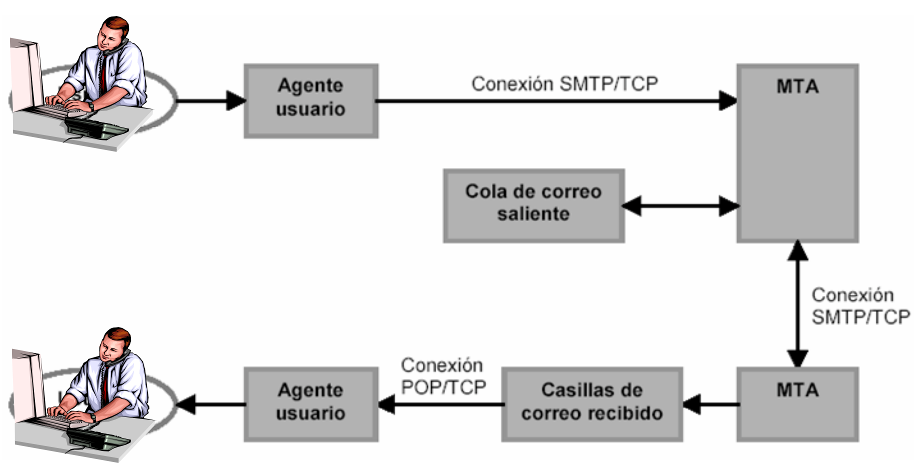

Figura 4.2. Esquema del correo electrónico Internet

En resumen el correo electrónico se clasifica como el servicio más utilizado de todos los que existen actualmente de arquitectura cliente-servidor. Gracias a este se tiene la posibilidad de comunicarse rápidamente con todo el mundo desde una estación de trabajo de forma muy simple y barata.

En la figura 4.3 se representa de forma simplificada como funciona el servicio de correo electrónico y los elementos que intervienen en este proceso.

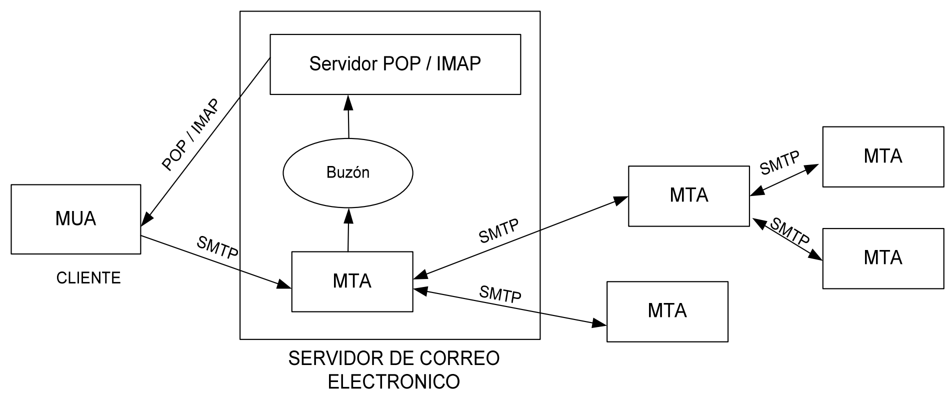

Figura 4.3. Representación esquemática del servicio de correo electrónico

4.1.2.1 Servicio POP3 e IMAP

Existen varias variantes para ambos servicios. A continuación se listan estos ficheros y a que variante corresponden:

ipop3: se corresponde con la variante del protocolo POP número 3 o POP3, que es actualmente la que soportan los clientes de correo modernos como Nestcape Communicator u Outlook.

ipop2: se corresponde con POP2. Raramente es necesario soportar esta variante, pues existen pocos clientes que la necesitan.

Imaz: se corresponde con el protocolo IMAP.

pop3s: se corresponde con el protocolo POP3 con soporte **SSL** (***Secure Socket Layer***).

Imaz: se corresponde con el protocolo IMAP con soporte SSL.

Una vez instalado el servicio solo es necesario habilitar la variante que se desee brindar a los clientes. Por defecto todas están deshabilitadas.

El servidor de POP3 por defecto escucha por el puerto 110, mientras que IMAP lo hace por el 143.

Los mensajes de los usuarios del sistema se almacenan en un directorio específico. En él se encuentra un fichero por cada usuario que posea al menos un mensaje en su buzón y que se nombra utilizando su propio *login*. Aquí realizarán los servidores de POP o de

IMAP las acciones que soliciten los clientes de correo, una vez conectados y autenticados, sobre el buzón correspondiente. También los MTAs colocarán en estos ficheros los mensajes recibidos por los usuarios para su posterior descarga.

4.1.2.2 MTA Sendmail (SMTP)

El Sendmail es el MTA de código abierto (Open Source) más conocido y utilizado actualmente en Internet. Posee numerosas y probadas capacidades que se han enriquecido gracias a su autor principal Eric Allman (creador también de syslog). Con Sendmail y relativamente poco hardware se puede manipular la mensajería de miles de usuarios con seguridad y ausencias de riesgos casi absolutas en entornos Unix o similares. El Sendmail una vez instalado, posee un script de inicio con su mismo nombre.

4.1.3. Servicio World Web Wide (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 browsers también pueden acceder a información mediante otros protocolos, por ejemplo: recuperar archivos con FTP, noticias con NNTP, etc.

4.1.4. 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.

El servicio permite agregar, sacar, borrar, renombrar, mover y copiar archivos en el servidor.

En la configuración del FTP se pueden establecer aspectos como: el máximo de usuarios conectados simultáneamente, restricciones de acceso de acuerdo a clases de usuarios, grupos, clientes, límites en la cantidad de datos transmitidos por sesión, etc.

4.1.5. 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.

4.2. Conectividad

Un ISP dentro de la jerarquía de los proveedores de servicios, puede conectar 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 de acceso para clientes conmutados generalmente es un banco de módems, 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, lo que hemos propuesto en nuestro diseño.

4.3. Administración de redes

La configuración inicial puede ser de una o dos redes separadas por un firewall. A medida que la red crece, recomendamos 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.

Se debe tener en cuenta 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.

Una 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 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.

4.4. 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.

4.5. Equipamiento Computacional

Una elección importante para el ISP es la arquitectura de los computadores. Existen varias arquitecturas compitiendo en este mercado. Se puede mejorar la confiabilidad de los equipos instalado sistemas redundantes, lo que también sube los costos.

A continuación describimos una clasificación estándar, para ser utilizada en un ISP.

La configuración mínima para un ISP comercial estará 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 un ISP.

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.

4.6. Administración de clientes

Esta labor se puede realizar con un computador de escritorio (procesador Pentium III, 128 MB en memoria, 20 GB en disco duro IDE). Este equipo se puede utilizar como servidor de impresión.