UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

ESCUELA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES

TESIS PREVIA A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS

TEMA:

VERIFICACIÓN, AUTENTIFICACIÓN Y TARIFACIÓN DE USUARIOS RAS BAJO PLATAFORMAS LINUX

APLICATIVO:

APLICACIÓN PARA TARIFACIÓN DE USUARIOS RAS EN UN I.S.P BAJO PLATAFORMAS LINUX (TARNET)

AUTORES:

PUSDÁ CHULDE MARCO REMIGIO

TAPIA MELO MILTON RAÚL

DIRECTOR:

ING. JORGE CARAGUAY PROCEL

IBARRA, NOVIEMBRE DE 2003

C E R T I F I C A C I Ó N

Los Señores: Pusdá Chulde Marco Remigio y Tapia Melo Milton Raúl, han trabajado en la investigación "*VERIFICACIÓN y AUTENTIFICACIÓN DE USUARIOS RAS BAJO PLATAFORMAS LINUX*", previa la obtención del Título de Ingenieros en Sistemas Computacionales, realizándola con interés profesional, responsabilidad y esfuerzo tesonero, lo cual certifico en honor a la verdad.

Ing. Jorge Caraguay P.

DIRECTOR DE TESIS

DEDICATORIA

Esta tesis dedico a todos quienes me apoyaron de una u otra manera, especialmente a mis Padres por el apoyo incondicional, para obtener el Título de Ingeniero en Sistemas Computacionales, dedico o todos mis compañeros y amigos con quienes compartimos el período de estudios, formándonos en lo personal y profesional.

MARCO REMIGIO PUSDÁ CHULDE.

D E D I C A T O R I A

A mi madre, quien hizo de mí un hombre honesto y responsable; a mis hermanos: Carmen, Henry y Vanesa, para ellos todo mi esfuerzo hoy y siempre.

MILTON RAÚL TAPIA MELO.

A G R A D E C I M I E N T O

A mis padres por el apoyo moral y económico en todo lo necesario para mi educación y formarme profesionalmente.

A los docentes que impartieron conocimientos, responsabilidades en las aulas universitarias, quienes no enseñaron a emprender metas, objetivos; y prepararnos para que en la vida profesional demostremos los conocimientos adquiridos para el desarrollo de la sociedad.

A nuestro Director de Tesis (Ing. Jorge Caraguay), por el apoyo incondicional, quien no guío en el desarrollo y ejecución del proyecto, gracias a su gran experiencia.

MARCO REMIGIO PUSDÁ CHULDE.

AGRADECIMIENTO

A mi Familia por el apoyo moral y económico que me brindaron de manera incondicional.

Al Ing. Jorge Caraguay, director del proyecto, quien aportó con su experiencia, conocimiento y voluntad, para llevarlo a un feliz termino.

MILTON RAÚL TAPIA MELO.

INTRODUCCIÓN

El presente trabajo de Investigación tiene como finalidad estudiar el campo de Autentificación, Verificación y Tarifación de Usuarios RAS. Los Usuarios RAS utilizan diferentes tecnologías para acceder a los Servicios que presta un ISP, dependiendo de la Arquitectura del mismo. El sistema de acceso de un Usuario está formado por diversidad de elementos. Las tecnologías asociadas se encuentran en franca evolución, tecnologías que permitirán brindar un mejor y eficiente servicio.

Un Usuario que requiera servicios de Internet accede desde un computador normal o redes de ordenadores, que incluyen sistemas y elementos activos de conexión de última tecnología como: vía satélite, dial_in, dial_up, conmutadores de paquetes, switchs, routers, centrales privadas (PBX), sistemas digitales, etc.

Los servicios que prestan los ISPs, dependen de diferentes aspectos respecto a los actuales y futuros servicios de interconectividad, los elementos activos y su comportamiento en la interconexión, los protocolos de conexión a Internet, funciones generales de un RAS, un análisis de las plataformas, herramientas de desarrollo con bases de datos y un estudio del sistema de tarifación RADIUS.

Esta investigación está orientada a personas con diversos niveles de preparación y experiencia, un usuario principiante que necesite una visión general sobre Autentificación, Verificación y Tarifación de Usuarios RAS, deberá revisar el Capítulo I, además para familiarizarse con términos de Redes deberán revisar 9.5 (**GLOSARIO**).

En el **Capitulo I** se analiza la situación de los servicios de interconectividad, desde sus orígenes, la situación actual y su futuro, conceptos de interconexión, sus ventajas, problemas a nivel mundial que servirán de base para futuras redes de interconexión en nuestro país, desafíos y planteamientos a nivel de arquitectura de la tecnología. Así mismo se realiza una breve visión del comportamiento de los proveedores de servicios de Internet, su arquitectura, su papel en los negocios.

En el **Capitulo II** se ofrece la descripción de los elementos activos que intervienen en la interconectividad, mostrando conceptos, terminologías, funciones, las nuevas tecnologías de acceso a un ISP y sobre todo como un usuario obtiene el servicio de INTERNET.

En el **Capitulo III** se detalla los protocolos de conexión frecuentemente usados en el proceso de interconexión, las definiciones más comprensibles de cada uno de los protocolos, una comparación y análisis de TCP/IP (IPV4 e IPV6) y su efecto en la tarifación.

En el **Capitulo IV** se revisan funciones generales de un RAS, definiciones tanto de Software, Interfases, tecnologías de seguridad, herramientas y operabilidad con sus modos de configuración a nivel de rendimiento, estadística, velocidades y paridades.

En el **Capitulo V** se realiza el estudio de plataformas, preferentemente sistemas operativos como LINUX y WINDOWS, sus características tanto en interfaz, acoplamiento con aplicaciones comerciales, costos, rendimiento, seguridad, facilidades, ventajas y desventajas.

En el **Capitulo VI** se hace referencia a tres herramientas de desarrollo compatibles con LINUX, características, tanto a nivel de desarrollo visual como C++, KYLIX, PHP y de desarrollo en base de datos como MySQL.

En el **Capitulo VII** se estudia los sistemas de tarifación, características, ventajas y desventajas, funciones, arquitectura, requisitos de servidor RADIUS, y sus versiones.

En el **Capitulo VIII** se detalla el proceso, análisis, y ejecución para el desarrollo de TarNet.

En el **Capitulo IX** se especifican las conclusiones y recomendaciones producto de la investigación realizada.

Los Autores

CAP. I

INTRODUCCIÓN

REALIDAD ACTUAL DE LOS SERVICIOS DE INTERCONECTIVIDAD.

COMPORTAMIENTO DE LOS PROVEEDORES DE SERVICIOS DE INTERNET

1. INTRODUCCIÓN

La cantidad de usuarios activos de Internet en el Ecuador supera las proyecciones esperadas, ver la **Figura 1.1**[1], por debajo del desarrollo obtenido en otros países, observar la **Figura 1.2**[2]; causa fundamental de estas diferencias es la poca cultura del *uso de Internet e Informática* en nuestro país.

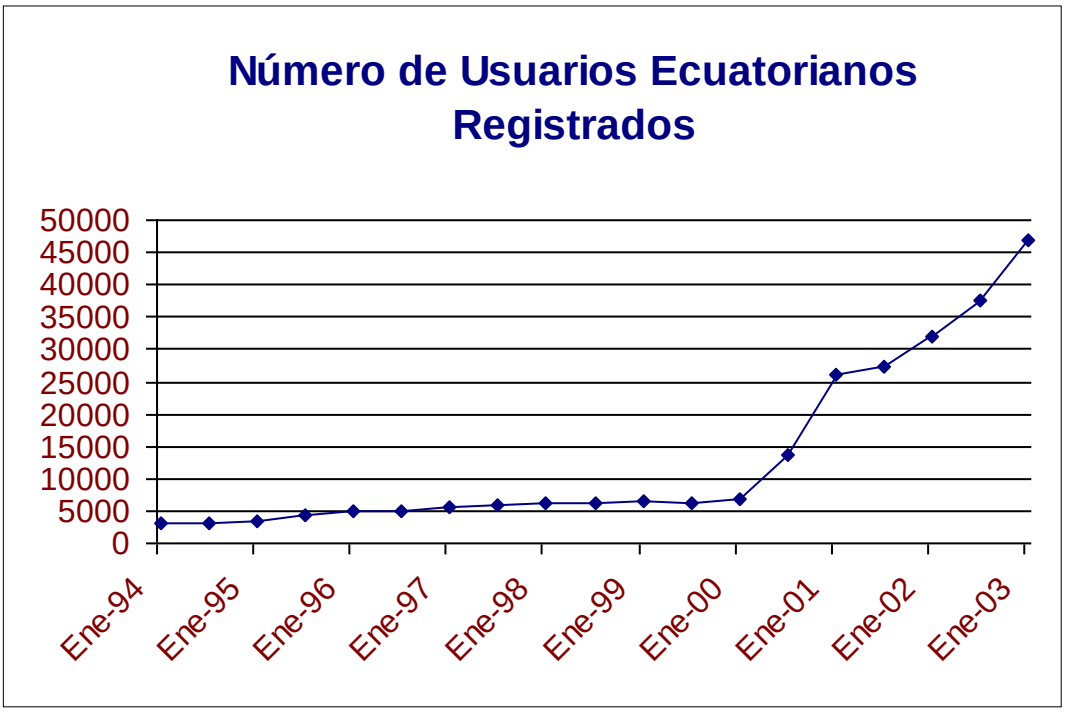
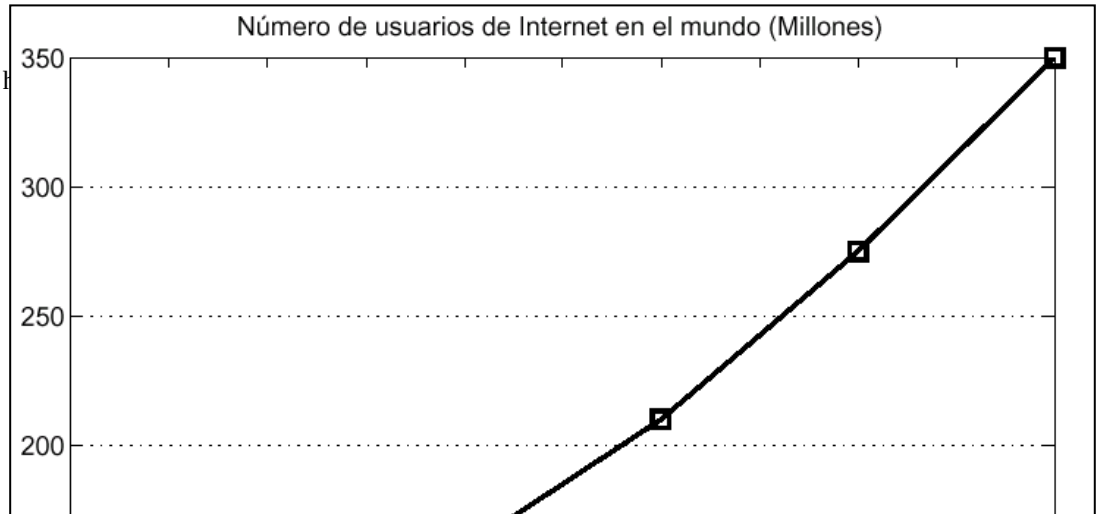


Figura 1.1 Usuarios conectados a Internet en Ecuador



[1] h
[2]

Figura 1.2 Datos del número de usuarios en el mundo de Internet

Con la intención de masificar con calidad el uso de Internet, herramienta mundialmente utilizada por emplear un formato estándar, se han realizado sendos análisis sobre el proceso de desarrollo de la mencionada herramienta en el sector del consumo masivo.

Puesto que nuestro mercado ha alcanzado la madurez suficiente para enfrentar el proceso de masificación de Internet.

1. 1. REALIDAD ACTUAL DE LOS SERVICIOS DE INTERCONECTIVIDAD.

1. 1. 1. ORÍGENES DE LA INTERCONECTIVIDAD

En 1958 en los EE.UU. se crea la agencia gubernamental de investigación, "A.R.P.A"[3] creado en respuesta a los desafíos tecnológicos, que sería base de la red global de computadores, Internet. A.R.P.A, es responsable de la investigación en ordenadores y comunicaciones.

A comienzos de la década del 60 A.R.P.A emprendió la tarea de desarrollar un sistema de comunicaciones en red diseñado específicamente para interconectar computadores en forma descentralizada, cuyo objetivo principal debía ser, continuar operando aún en caso que alguno o varios de los nodos de comunicación fallaran.

A fines de la década de 1960 la investigación se hace realidad la intercomunicación de ordenadores en red, comunicándoles a través de línea telefónica. Durante 1969, se instala el primer nodo de "ARPANET"[4].

[3] Advanced Research Proyect Agency
[4] Primera Red Científica y Académica

En 1972 ARPANET cambiará su denominación y será conocida como "DARPA"[5].

Las redes de comunicaciones y la autopista de la información han evolucionado desde la ARPANET hasta la actual Internet.

1. 1. 2. CONCEPTOS DE INTERCONECTIVIDAD

La Interconexión de Redes (*Internetworking*) es dar un servicio de comunicación de datos que involucre diversas redes con diferentes tecnologías de forma transparente para el usuario.

VENTAJAS DE LA INTERCONECTIVIDAD

Algunas de las ventajas que plantea la interconexión de redes de datos, son:

- Compartición de recursos dispersos.
- Coordinación de tareas de diversos grupos de trabajo.
- Reducción de costos, al utilizar recursos de otras redes.
- Aumento de la cobertura geográfica.

1. 1. 3. PROBLEMAS DE LA INTERCONECTIVIDAD

[5] Defense Advanced Research Projects Agency

Si bien la interconectividad de las redes es la mejor alternativa, tenemos claro los parámetros para analizar a la hora de hacer efectiva dicha posibilidad.

Podemos hacer mención el costo, situación geográfica, el nivel de cultura informático, entre otros.

Dichas experiencias se resumen en la afirmación: ***es totalmente factible interconectar dos o más redes, que mediando la participación de instituciones, se garantice utilización de estándares internacionales, lo más importante, los intereses concretos de los usuarios***.

1. 1. 4. ACTUALIDAD DE LOS SERVICIOS DE INTERCONECTIVIDAD

Superada la desconfianza de los empresarios y organizaciones se da inicio a la automatización de procesos permitiendo que todas las actividades repetitivas, rutinarias, que no agregan valor a la relación comercial sean realizadas de forma que aporten eficiencia a la gestión de negocios en su totalidad.

Hecho el análisis se establece la conclusión; fueron varios los motivos que impidieron el crecimiento de usuarios de Internet en la medida esperada. A partir de proyectos como la creación de centros de distribución automatizados, bases de transferencia, la aparición de operadores logísticos en las actividades comerciales del sector, de

querer trabajar eficientemente, aplicando esquemas de reposición continua de mercaderías, generación automática de ordenes de compras, avisos de despacho anticipados, y sin número de prácticas que llevan implícito el intercambio de información de socios comerciales, estamos usando la *explosión* de Internet herramienta por todos reconocida.

Para garantizar dicho crecimiento se conjugan dos aspectos fundamentales para el éxito de cualquier proyecto: los meramente técnicos y la voluntad de los participantes de *INTERNET*.

Estamos hablando de la necesidad de *INTERCONECTAR LAS REDES* que operar en nuestro sector respetando los estándares y procedimientos definidos.

La interconexión de redes sola no garantiza el éxito de un proyecto, podemos afirmar que es aporte fundamental para ampliar la comunidad multisectorial de usuarios de Internet que necesita interactuar entre distintos sectores de la actividad comercial, educativa e información, es decir la cantidad de proveedores de servicios, que garanticen calidad en las prestaciones, ínterconectividad con redes similares y, un alineamiento incondicional de estándares internacionales, así será más fácil difundir y ampliar la cultura de Internet en la colectividad.

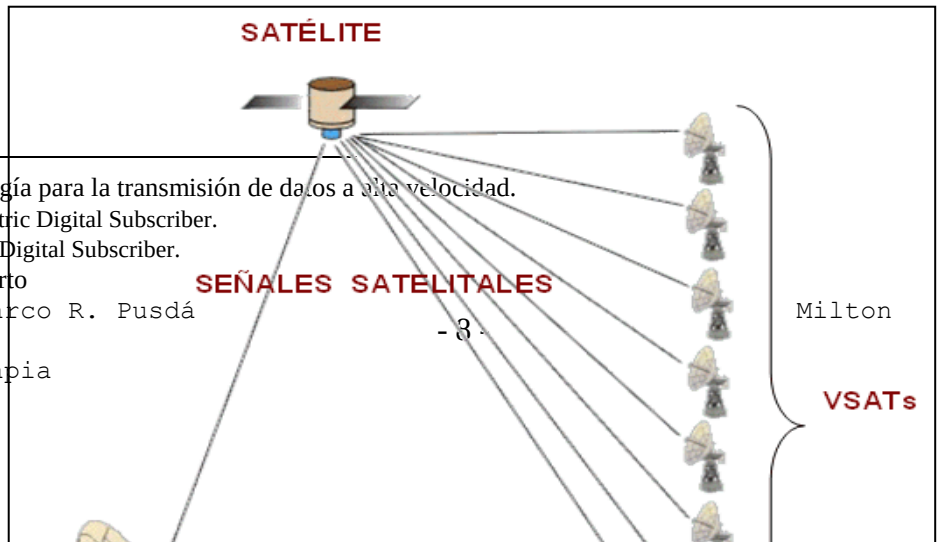
1. 1. 5. FUTURO DE LA INTERCONECTIVIDAD

DESAFÍOS Y PLANTEAMIENTOS.

La permanencia y desarrollo de redes en el futuro será posible si los servicios ofrecidos a los posibles clientes son eficientes, a bajo costo, y con gran velocidad.

La evolución de Internet, y sus formas de acceso a través de tecnologías; "xDSL"[6] que permiten el uso de la línea telefónica estándar. Es llamada xDSL por tener el mismo funcionamiento, pero distintas características en cuanto a prestaciones y distancia máxima del domicilio a la central telefónica. Entre las tecnologías, la mas adecuada para uso domestico son las llamadas "ADSL"[7] (Línea de Abonados Digital Asimétrica), "SDSL"[8] (Línea de Abonados Digital Simétrica),

"RACSA"[9] tecnología que consiste en una red de terminales satelitales de pequeño diámetro, su topología en estrella. Ver **Figura 1.3**



[6] Tecnología para la transmisión de datos a alta velocidad.
[7] Asymmetric Digital Subscriber.
[8] Simetric Digital Subscriber.
[9] Telepuerto

Figura 1.3 Arquitectura RACSA

La interconexión "*VSAT*"[10] permite comunicar sitios geográficamente dispersos, integrándolos en una sola red. VSAT de RACSA es una alternativa atractiva para desarrollar múltiples aplicaciones de transmisión de datos.

Situaciones nuevas e insospechadas que Internet presenta al mundo, ello obliga a realizar planteamientos teóricos y prácticos, no convencionales, y plantea la necesidad de una revisión de los status convencionales y de definir nuevos perfiles profesionales.

Deberán ser afectados por estos planteamientos:

- El conjunto del sistema documental.

[10] Very Small Apertura Terminal.(Antena)

- Limitaciones que el propio sistema impone.

UMBRAL DEL NUEVO SIGLO

Los retos de las telecomunicaciones del siglo XXI, pueden relacionarse con la evolución de los sistemas de información, mediante la adopción de nuevas tecnologías, que trabajen sobre Internet. Tres pueden ser los ámbitos de acción, de cara al nuevo siglo: la arquitectura de sistemas, las tecnologías Web y los sistemas de información documental.

ARQUITECTURA DE LOS SISTEMAS

La sociedad de la información se abre paso, cada vez más, hacia la sociedad de la telecomunicación. Esto supone exigencias y planteamientos nuevos en el ámbito de la transferencia de información y documentación.

Se establece que la estructura básica tiene que mejorar, el ancho de banda no funciona y hay hipocresía económica.

Hoy, y en adelante, la transferencia de datos e información exige planteamientos de arquitecturas transaccionales nuevas, con la flexibilidad necesaria para soportar nuevos servicios y aplicaciones corporativas, como pueden ser Intranet y Extranet. Para ello, es necesario contar previamente con arquitecturas seguras y direcciones

de localización con estructura y normativa de almacenamiento estándar.

Tecnológicamente, se deberán incorporar nuevas tecnologías de bases de datos, soportando mecanismos flexibles de invocación, dentro de entornos heterogéneos, que admitan elevadas transacciones, seguridad y distribución de aplicaciones y datos.

LA EVOLUCIÓN DE LAS TECNOLOGÍAS WEB

En la actualidad, las tecnologías Web tienen aplicaciones tan importantes como decisivas en el funcionamiento empresarial y en el mundo de los negocios, lo cierto es que en sus primeros momentos, se constituyeron en las tecnologías más aptas y adecuadas para la transferencia de datos y, en general, de información. Y así se entendieron desde el ámbito de la investigación científica y de la documentación. ¿Será cierto por ello, que cada vez habrá menos periódicos y más Web?.

Las Web se constituyen en recurso y plataforma imprescindible para la creación de sistemas operativos de carácter universal, brindando servicios corporativos en el mundo empresarial.

LA GESTIÓN DE LA INFORMACIÓN DOCUMENTAL

Las nuevas arquitecturas de sistemas y la evolución de tecnologías Web, imponen aspectos como el desarrollo y la explotación de la red, la creación y gestión de los servicios: se precisa el concepto de la globalidad documental, la aplicación de soluciones integrales en la gestión de información documental.

Como consecuencia del crecimiento exponencial de usuarios "SMTP"[11], se tendrá que potenciar el desarrollo de la mensajería electrónica, en base al servicio "InfoMail"[12], orientado al mercado empresarial, residencial, destinado a usuarios de InfoVía y la Red "IP"[13], con altas cotas de seguridad, confidencialidad, disponibilidad y fiabilidad.

La ínter conectividad cuenta ya, cara al futuro, con una serie importante de recursos y de medios, para la prestación de servicios multimedia, como son el satélite y el cable, la Web-televisión, la TDT (TV Digital Terrestre), la FTTH (Fibre To The Home), el MMDS (Multipoint Microwave Distribution Service), el xDSL (any Subscriber Loop), etc.

[11] Simple Mail Transfer Protocol
[12] Servicio Público de Mensajería Multimedia en Red.
[13] Internet Protocol.

1. 2. COMPORTAMIENTO DE LOS PROVEEDORES DE SERVICIOS DE INTERNET

1. 2. 1. ISP Y LA ARQUITECTURA DE INTERNET

El éxito de Internet se debe al uso del sistema de comunicaciones TCP/IP que permite la interconectividad entre cualquier tipo de ordenadores como se muestra en la **Figura 1.4**. Este sistema establece una arquitectura propia que garantiza el funcionamiento distribuido de redes y equipos en el mundo. Existen máquinas dedicadas a tareas específicas por tanto especializadas.

El eje central físico, en la práctica esta formado por un conjunto de líneas de alta velocidad que al inicio cruzaban de costa a costa los Estados Unidos, que después se extendió para cubrir el mundo, a él se conectan las pasarelas de Internet.

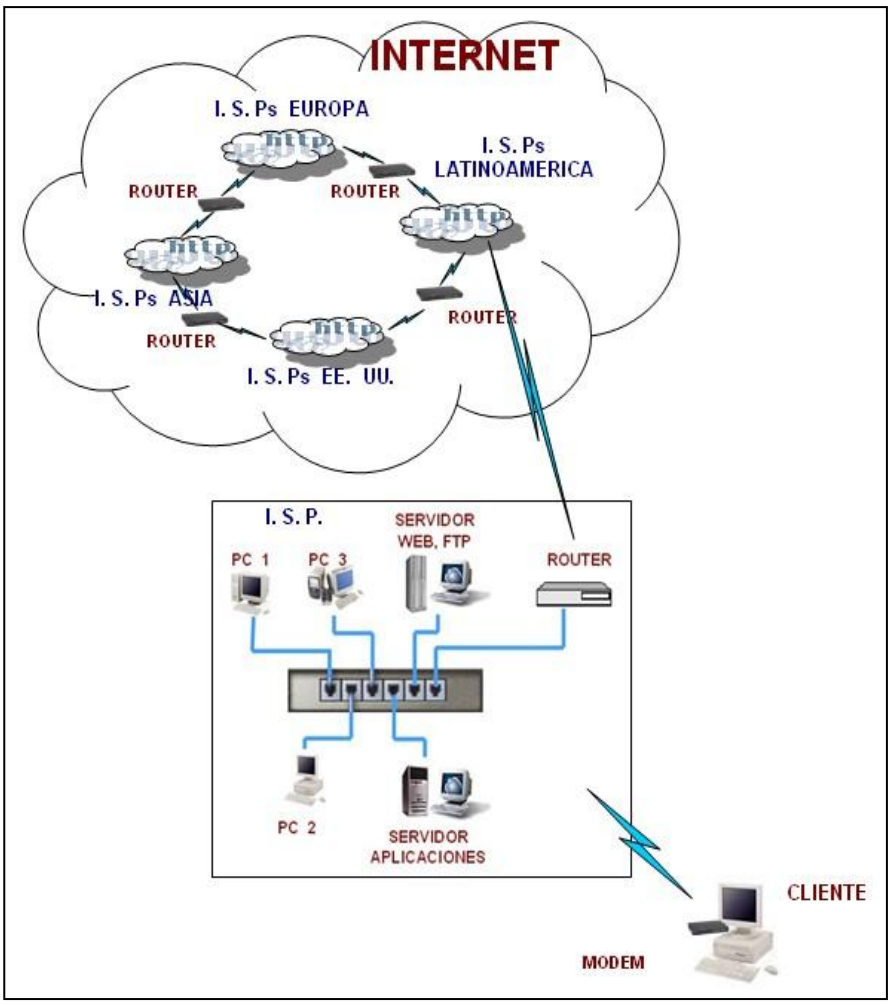


Figura 1.4 Arquitectura Internet

Las pasarelas, utilizando su propio protocolo (dentro de TCP-IP) son encargadas del enrutamiento de paquetes de datos. Para ello, se almacena información relacionada con sub-redes de todas las pasarelas de Internet. Así, conocen la situación de la red y encaminan los paquetes por rutas mas adecuadas.

En la conexión de estas pasarelas puede haber otro tipo de pasarelas de nivel inferior cuya función es parecida a las principales pero que

conforman la sub-red que esta bajo la pasarela principal y tienen su propio protocolo de funcionamiento.

Servidores. Son las máquinas que residen las aplicaciones de los diferentes servicios que se pueden utilizar en Internet. Por ejemplo: servidores de World Wide Web, servidores de correo electrónico, servidores de Chat, servidores de FTP, servidores de audio, servidores de vídeo, etc., etc.

DNS (servidores de nombre de dominio): Su función consiste en relacionar las direcciones IP con los nombre de dominio.

Usuarios finales: Forman una red local, conectándose a sus servidores que son los proveedores de acceso a Internet. Generalmente la conexión se realiza mediante una llamada de la Red Telefónica Básica (RTB).

Cliente: Son programas que residen en los equipos de los usuarios finales, que, conectados al correspondiente servidor, les permiten utilizar servicios que existen en la red.

1. 2. 2. ISP EN LOS NEGOCIOS

Los ISP se han convertido en la solución para las empresas. Internet ha producido cambios en todos los órdenes de la vida, uno de los aspectos

que está experimentando las consecuencias de su existencia, sin duda, es la forma de hacer negocios.

El exponencial avance tecnológico y el constante crecimiento de Internet, ha provocado que los costos de transporte y comunicación tiendan a cero. Implementando la tecnología de **Internet** en empresas, disminuye drásticamente los costos de comunicación, comercialización, marketing, distribución de información, etc.

La globalización de la economía mundial rompe las fronteras de mercado tradicionales, las empresas compiten directamente con todo el mundo. Casualmente Internet es global por definición, convirtiéndose entonces en herramienta estratégica del negocio. El auge de las empresas tendrá relación con el crecimiento de la publicidad y comercio electrónico, las dos fuentes de ingresos principales en Internet.

1. 2. 3. ISP Y APLICACIONES EMPRESARIALES EN INTERNET

DOMINIO PROPIO

Los ISP tramitan y administran dominios propios de cada empresa mejorando la imagen de su empresa en Internet.

CORREO ELECTRÓNICO

Por cantidades mínimas de dinero o muchas de las veces de forma gratuita los ISP proveen la cuenta de correo electrónico. Se trata de la herramienta de comunicación más eficiente y revolucionaria. Por medio de ella los usuarios pueden enviar/recibir mensajes a/de cualquier parte del mundo.

Con respecto a los métodos tradicionales de comunicación (fax, courier, correo postal, etc.), el correo electrónico Internet ofrece las siguientes ventajas/beneficios:

Velocidad: Llega a su destino en pocos segundos, aunque éste se encuentre en un punto distante del planeta.

Seguridad: Si el mensaje no llega a destino (casilla de correo inexistente, etc.) el remitente recibe la notificación correspondiente.

Privacidad: El mensaje puede ser leído por el destinatario en su computadora.

Envío de archivos: Adjunto a un E-mail, pueden enviarse archivos que contengan planillas de cálculo, documentos de texto, gráficos, fotos, reportes, etc.

Listas de distribución: Un mismo E-mail puede enviarse simultáneamente a más de un destinatario.

Reducción de costos: Su costo casi insignificante, frente a su insuperable velocidad y potencialidad, lo convierten en la herramienta de comunicación por excelencia.

Portabilidad: Un correo electrónico es ajeno a la plataforma de la computadora que lo envía/recibe, por lo que no existen incompatibilidades entre diferentes sistemas operativos, hardware, etc.

ACCESO FULL INTERNET

Con cuotas mensuales, dependiendo de los planes, incluyendo una casilla de correo electrónico Internet, las empresas pueden acceder a Internet On-Line y todos sus servicios:

WWW: (World Wide Web) Navegando por las millones de páginas Web del mundo, Ud. podrá buscar información de todo tipo, hacer compras On-Line, obtener y actualizar software para su computadora, leer periódicos y escuchar radios de todo el mundo, recorrer museos, contactar empresas y organismos, etc.

FTP: (File Transfer Protocol) Transferencia de archivos, Foros y Newsgroups: Áreas de discusión donde se intercambian mensajes de acuerdo a una temática específica.

Telnet: Conexión como terminal a un Servidor.

IRC: (Internet Relay Chat) Teleconferencia.

VideoConferencia: Si posee una cámara de video, puede realizar videoconferencias por Internet con otros usuarios.

WEB MAIL: Si se encuentra de viaje, en un Cybercafe o en otra computadora con acceso a Internet, puede manejar su correo electrónico desde un navegador.

ACCESO PERMANENTE DIGITAL

El ancho de banda de su empresa es importante, los ISP disponen de un servicio especial que consiste en conexiones permanentes al nodo. Que alcanzan altas velocidades con disponibilidad del servicio 24 horas al día, 365 días al año. Por medio de la misma, puede conectar a Internet varios puestos de trabajo simultáneos, e-mail de toda la empresa, acceso a la Intranet (Extranet), hostear las páginas Web de cada empresa, etc.

E-MAIL CORPORATIVO

El servicio que permite proveer de casillas de correo electrónico a cada puesto de trabajo de red en su empresa. Las direcciones de E-mail contendrán el dominio propio de su empresa. (Ej. mailto:ventas@empresa.com.ec, etc.). Los ISP Proveen herramientas para

la administración de cuentas, permitiendo agregar/modificar/borrar usuarios de correo sin depender de la participación de los mismos.

FULL INTERNET CORPORATIVO

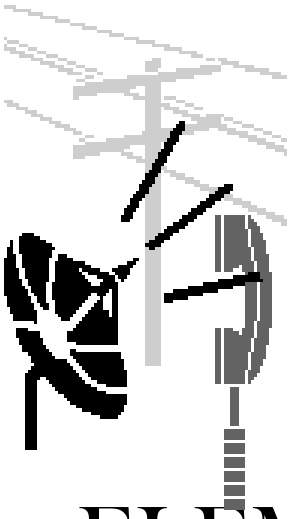
La misma filosofía que el E-mail corporativo, consiste en brindar conexión Full Internet (WWW, Telnet, FTP, E-mail, etc.) a los puestos de trabajo en las empresas utilizando un solo modem y una línea telefónica. Para no degradar la velocidad al compartir más de un usuario una misma línea telefónica, se provee también un Servidor Proxy que funciona en todas las instalaciones mejorando la performance del servicio.

HOSTING DE PAGINAS WEB

Contando con poderosos servidores de páginas Web, gran ancho de banda nacional e internacional, las últimas tecnologías a nivel servidor, potentes herramientas de administración de Web Sites, programas ya desarrollados para uso de los sitios que albergan los ISP (Foros, Chat, Guestbook, Mailing lists, etc.), extensiones de Front-Page para actualización de las páginas, línea de publicación dedicada, cuenta de acceso full gratuita, direcciones de E-mail ilimitadas.

HOUSING

Cuando los proyectos de las empresas en Internet no justifican la instalación y mantenimiento de un acceso permanente digital dedicado, los ISP proveen el servicio de Housing, albergando el servidor de cada empresa en el nodo del ISP.



CAP. II

ELEMENTOS ACTIVOS

Y SU

COMPORTAMIENTO

CONCEPTOS Y TERMINOLOGÍA

FUNCIONES DE LOS ELEMENTOS ACTIVOS

TECNOLOGÍAS DE ACCESO A UN ISP

COMO ACCEDE UN USUARIO A UN ISP

2. ELEMENTOS ACTIVOS Y SU COMPORTAMIENTO

2. 1. CONCEPTOS Y TERMINOLOGÍA.

Una red (Intranet, Extranet e Internet) de computadoras consta de hardware y software. Como hardware se incluyen: estaciones de trabajo y/o clientes, servidores, tarjeta de interfaz de red, cableado y equipo de conectividad (MODEM, PBX, ROUTERS, SWICTH, PULL DE MODEMS, PORTMASTER), Ver Figura 2.1. Como Software se encuentra el sistema operativo de red (Network Operating System) NOS.

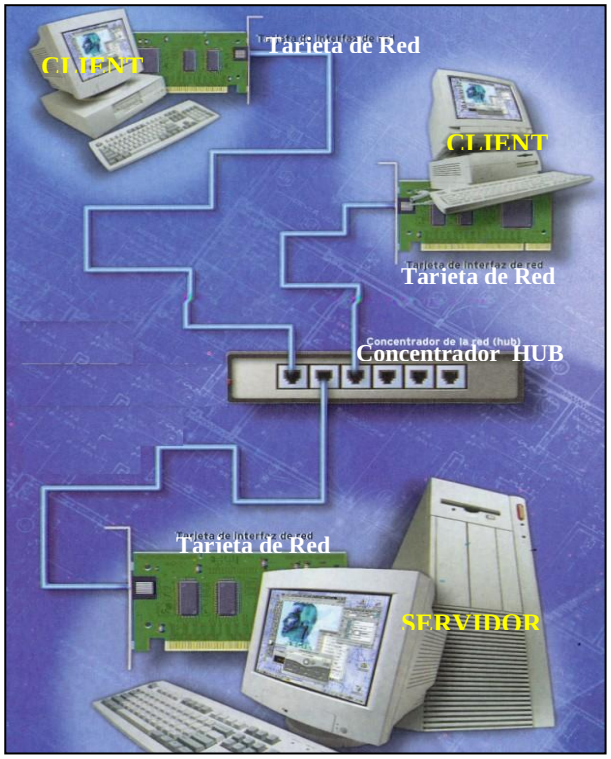


Figura 2.1 Hardware de Conectividad

La conexión de un usuario más allá de navegar a través de un browser, incluye estudiar los equipos de conectividad, que facilitan la navegación al cliente de un ISP, resultando transparente a su vista.

2. 1. 1. ESTACIONES DE TRABAJO Y/O CLIENTES

Una estación de trabajo no comparte sus recursos con otras computadoras. Esta puede ser desde una PC XT hasta una Pentium IV, equipada según las necesidades del usuario; independientemente de su arquitectura.

2. 1. 2. SERVIDORES

Aquellas computadoras capaces de compartir recursos con otras. Cuyos recursos pueden incluir impresoras, unidades de disco, CD-ROM, directorios en disco duro e incluso archivos individuales. Los tipos de servidores obtienen el nombre dependiendo del recurso que comparten.

2. 1. 3. TARJETAS DE INTERFAZ DE RED

Adaptadores de red o sólo tarjetas de red. La mayoría de tarjetas se adaptan en la ranura de expansión de la computadora, algunas son unidades externas que se conectan a un puerto serial o paralelo.

La tarjeta obtiene la información de la PC, la convierte en formato adecuado y la envía por el cable a otra tarjeta de interfaz de la red local.

2. 1. 4. EQUIPOS DE CONECTIVIDAD

Existen dispositivos que extienden la longitud de red, donde cada uno tiene un propósito específico.

MODEMS

Módem es un Modulador-De modulador; es decir, dispositivo que transforma las señales digitales del ordenador en señal telefónica analógica y viceversa, lo que permite al ordenador transmitir y recibir información por la línea telefónica.

PBX

Un PBX (Central de Ramificación Privado) un sistema telefónico de propiedad privada que permite telecomunicaciones dentro de un negocio.

Las extensiones de un teléfono individual se emplean para acceder al PBX, el cual enrutará la llamada internamente o conmutará a la línea externa de menor costo, según se requiera. Se cablea en una topología de estrella con cada extensión cableada de regreso al PBX. El subsistema es típicamente un cable de par trenzado no apantallado, de

pares múltiples (múltiplos de 25 pares), y el cableado horizontal consta de cables individuales de 4 pares a cada ubicación telefónica. Un ejemplo de interconexión entre los diferentes elementos activos se muestra en la Figura 2.1

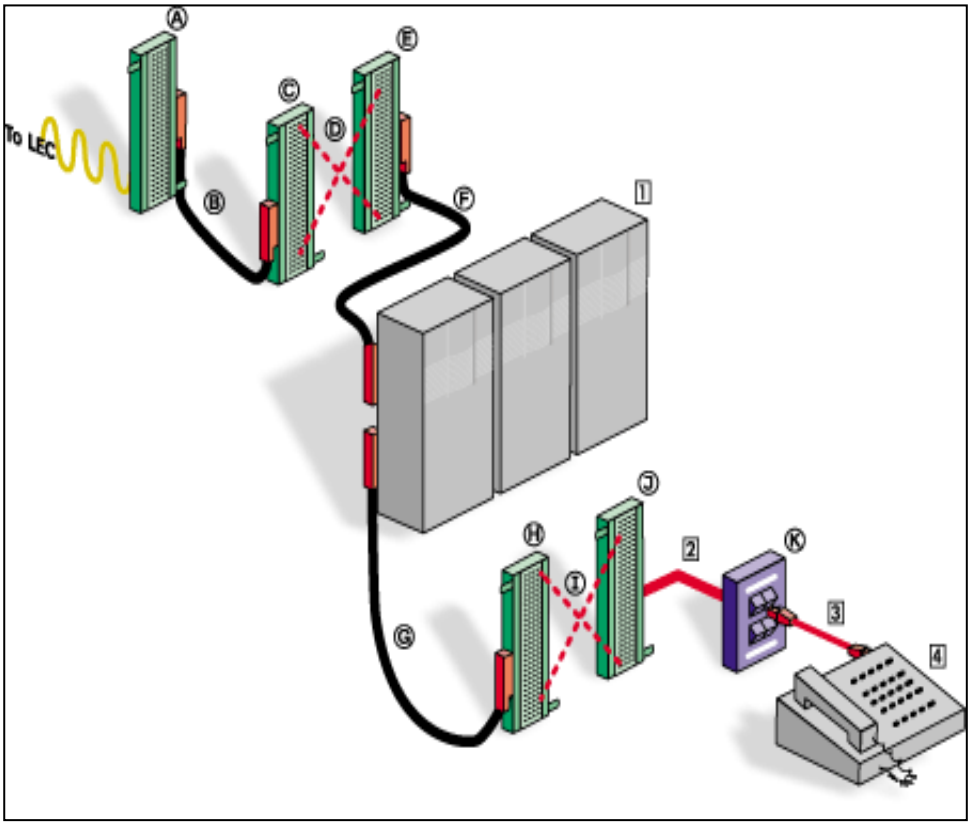


Figura. 2.1 Conjunto de Equipos de Interconectividad

DETALLES
(A) S66^{TM} Productos
(B) Cable Ensamblado

(C) S66^{TM} Productos
(D) Conexiones Cruzadas
(E) S66^{TM} Productos
(F) Cable Ensamblado
(G) Cable Ensamblado
(H) S66^{TM} Productos
(I) Conexiones Cruzadas
(J) S66^{TM} Productos
(K) Área de Trabajo Ensamblado
(1) PBX
(2) 4-Cableado Par Horizontal
(3) Cordón modular(abastecido con el teléfono)
(4) Teléfono

Tabla 2.1 Nomenclatura de Equipos de

Interconectividad.

Central telefónica privada (PBX). Sistema telefónico situado en las instalaciones de un cliente que atiende llamadas entrantes y realiza llamadas salientes.

Un PBX es considerado un conmutador telefónico localizado en el equipo terminal del usuario estableciendo circuitos a través de líneas conectadas entre usuarios individuales y la Red telefónica conmutada.

ROUTERS

Son dispositivos inteligentes que trabajan a Nivel de Red del modelo de referencia OSI, y enlazan los tres primeros niveles de este modelo por lo que son dependientes del protocolo particular de cada red. Envían paquetes de datos de un protocolo común, desde una red a otra.

Los ruteadores son similares a los puentes, operan a un nivel diferente. Requieren por lo general que cada red tenga el mismo sistema operativo de red, para poder conectar redes basadas en topologías lógicas completamente diferentes como Ethernet y Token Ring, etc.

En general un dispositivo que conecta dos redes locales, es el responsable de controlar el tráfico entre ellas y de clasificarlo.

SWITCH O CONMUTADOR

Es un dispositivo de switcheo modular que proporciona conmutación de alta densidad para interfaces Ethernet y Fast Ethernet. Posibilita trabajar en redes LAN virtuales y la posibilidad de incorporar conmutación múltiple con el Sistema Operativo.

El diseño modular permite dedicar conexiones Ethernet de 10 Mbps y conexiones Fast Ethernet de 100 Mbps a segmentos LAN, estaciones de alto rendimiento y servidores, usando par trenzado sin apantallamiento, par trenzado apantallado y fibra óptica. Permiten una amplia velocidad de conmutación entre Ethernet y Fast Ethernet a través de una gama de interfaces que incluyen Fast Ethernet, Interfaces de Distribución.

PULL DE MODEMS

El PULL de modems tiene la particularidad de permitir que varias redes públicas se conecten simultáneamente al ISP, autorizando que varias personas accedan simultáneamente a información proporcionada por un mismo ISP.

PORTMASTER

El PortMaster ofrece la manera más razonable para Corporaciones Proveedoras de Servicio de Internet (ISPs), para suministrar acceso a grandes grupos de usuarios que usan líneas telefónicas analógicas estándar.

El PortMaster combina modems digitales, servidor de comunicaciones, y routers en un espacio único. Tiene ranuras de expansión que apoyan hasta diez modems por ranura.

2. 2. FUNCIONES DE LOS ELEMENTOS ACTIVOS

2. 2. 1. INTRODUCCIÓN

Los elementos activos de red en un Proveedor de Servicios de Internet (ISP) mantienen diversas funciones, de acuerdo a la estructura y tecnología del mismo, dependiendo de las necesidades de cada uno de los clientes requiere.

2. 2. 2. MODEM

La función principal del módem, es modular su señal portadora, con datos binarios del ordenador y extraer los datos binarios de la citada señal portadora.

2. 2. 3. ROUTER

Un router entre las funciones principales tiene:

- Un Router tiene puertos de entrada para los paquetes y puertos de salida para enviar aquellos paquetes a su destino. Cuando llega un paquete al puerto de entrada, el Router examina la cabecera del

paquete y comprueba el destino en una tabla de encaminamiento (base de datos que le dice al Router cómo enviar paquetes a varios destinos).

- Basándose en la información de la tabla de encaminamiento, el paquete se envía al puerto de salida determinado, enviando al Router más próximo de destino.

- Si los paquetes llegan al puerto de entrada más rápidamente de que el Router pueda procesarlos, se envían a la cola de entrada. Después el Router procesa los paquetes de la cola para que se reciban. Si el número de paquetes recibidos sobrepasa la capacidad de la cola (longitud), los paquetes se pueden perder. Cuando esto ocurre, el protocolo TCP en la computadora emisora y en la receptora solicitará su reenvío.

- En una Intranet simple, red completamente independiente, y en la que no hay conexiones a otra red o Intranet, sólo se necesita hacer encaminamiento mínimo, y así la tabla de encaminamiento en el enrutador es sumamente simple con muy pocas entradas.

- En una Intranet ligeramente más complicada que esté compuesta de un número de redes basadas en TCP/IP, y conectada con número limitado de redes basadas en TCP/IP, se requiere encaminamiento

estático. En el encaminamiento estático, la tabla de encaminamiento posee métodos específicos de encaminar datos a otras redes. Sólo se pueden usar esos caminos. Los administradores de Intranets pueden añadir rutas a la tabla de encaminamiento.

2. 2. 4. SWITCH

El equipo incorpora una tabla de direcciones con varias entradas. Cada entrada se usa para guardar la información de los nodos de la red, incluyendo el número de puerto y las direcciones MAC[14] (Control de Acceso al Medio).

APRENDIZAJE

Cuando un paquete se recibe desde cualquier puerto el Switch guarda la dirección origen, número de puerto y otras informaciones relacionadas con la tabla de direcciones. Esta información será usada para decidir entre enviar o filtrar futuros paquetes.

ENVIAR Y FILTRAR (FORWARDING & FILTERING)

Cuando se recibe un paquete por cualquier puerto el Switch comprueba la dirección de destino con las que tiene almacenadas como direcciones origen en la tabla de direcciones. Si no coincide con alguna de las almacenadas el paquete se envía por todos los puertos menos por el

[14] Médium Access Control

que se recibió. Si la dirección se encuentra en la tabla en un puerto distinto del que se recibió el paquete, el paquete se envía solo por ese puerto. Pero si la dirección se encuentra en el mismo puerto por el que se recibió el paquete entonces este se filtra (no se envía). De esta manera se incrementa el rendimiento de la red.

2. 2. 5. PBX

En el sistema PBX, la comunicación entre diversos computadores y periféricos que integran la red local se efectúa a través de una central telefónica privada, funciona únicamente con dispositivos electrónicos que operan sobre la base de división de tiempo.

Un PBX se encarga de establecer conexiones entre terminales de una misma empresa, o de hacer que se cursen llamadas al exterior. Hace que las extensiones tengan acceso desde el exterior, el interior, y ellas a su vez tengan acceso a otras extensiones y a una línea externa. Algunas de las funciones disponibles en un PBX son:

- Transferencia de llamadas
- Sistema para conocer el estado de las extensiones
- Sistema de espera: si alguien llama a una extensión ocupada, el sistema espera al llamante hasta que la extensión quede libre.

- Conferencias, que permite que llamadas del exterior lleguen a hablar con varias extensiones a la vez

- Mantener un archivo con información sobre las comunicaciones

- Sistema de contraseñas

- Desviar llamadas a petición de los usuarios, por si se van a mover de su puesto

Un PBX constará como mínimo de una línea externa, colocada para que los usuarios puedan comunicarse con el exterior. Y también, como mínimo, habrá una línea desde el exterior, para que el exterior pueda comunicarse con los usuarios.

2. 2. 6. PULL DE MODEMS

Contratados los servicios de un ISP, el computador personal de quienes se conectan a la red pública (Andinatel, Pacifictel, etc.) por medio de MODEM, acceden al número telefónico asociado con el ISP.

La red telefónica se conecta a la red del ISP contratado por medio de un PULL de modems, mediante estas conexiones el computador y el ISP transfieren información en uno y otro sentido.

2. 2. 7. PORTMASTER (ACCESO REMOTO)

Los tipos básico de acceso a un PortMaster son los denominados nodo remoto y control remoto. En el escenario de nodo remoto, un usuario se conecta a un servidor de acceso remoto, que controla el acceso a la red. El usuario queda conectado exactamente como si estuviese en la oficina, con acceso a todos los servicios y archivos.

Por el contrario, un usuario de control remoto controla un único PC. La ventaja del control remoto es que de archivos enteros se transfieren por el enlace de comunicaciones las pantallas y las teclas. Eso es ideal para aplicaciones no móviles. Tecnologías de conectividad remota más veloces (módem 56 Kbps y RDSI, ADSL, XDSL) permitirán a los usuarios trabajar transparentemente.

2. 3. TECNOLOGÍAS DE TRANSMISIÓN PARA ACCEDER A UN ISP

2. 3. 1. INTRODUCCIÓN

La conexión de computadores a redes se realiza a través de los llamados Proveedores de Servicios Internet (ISP). Ellos ofrecen diversos tipos de conexiones y servicios que cubran necesidades de cada usuario (individuos, pequeñas y grandes instituciones, redes corporativas, etc.)

Importante conocer las diversas maneras de conexión, existen dos tipos de enlaces: directos e indirectos. Un enlace directo es veloz y eficiente, pero requiere de equipo muy especial y tiene un costo elevado. Los usuarios particulares generalmente utilizan enlace indirecto, permitiéndoles acceder a la red con bajo costo, sin equipo adicional.

2. 3. 2. TIPOS DE ACCESO A INTERNET

La forma de acceso a un ISP esta acorde con el avance de la tecnología. Ver **Figura 2.2**

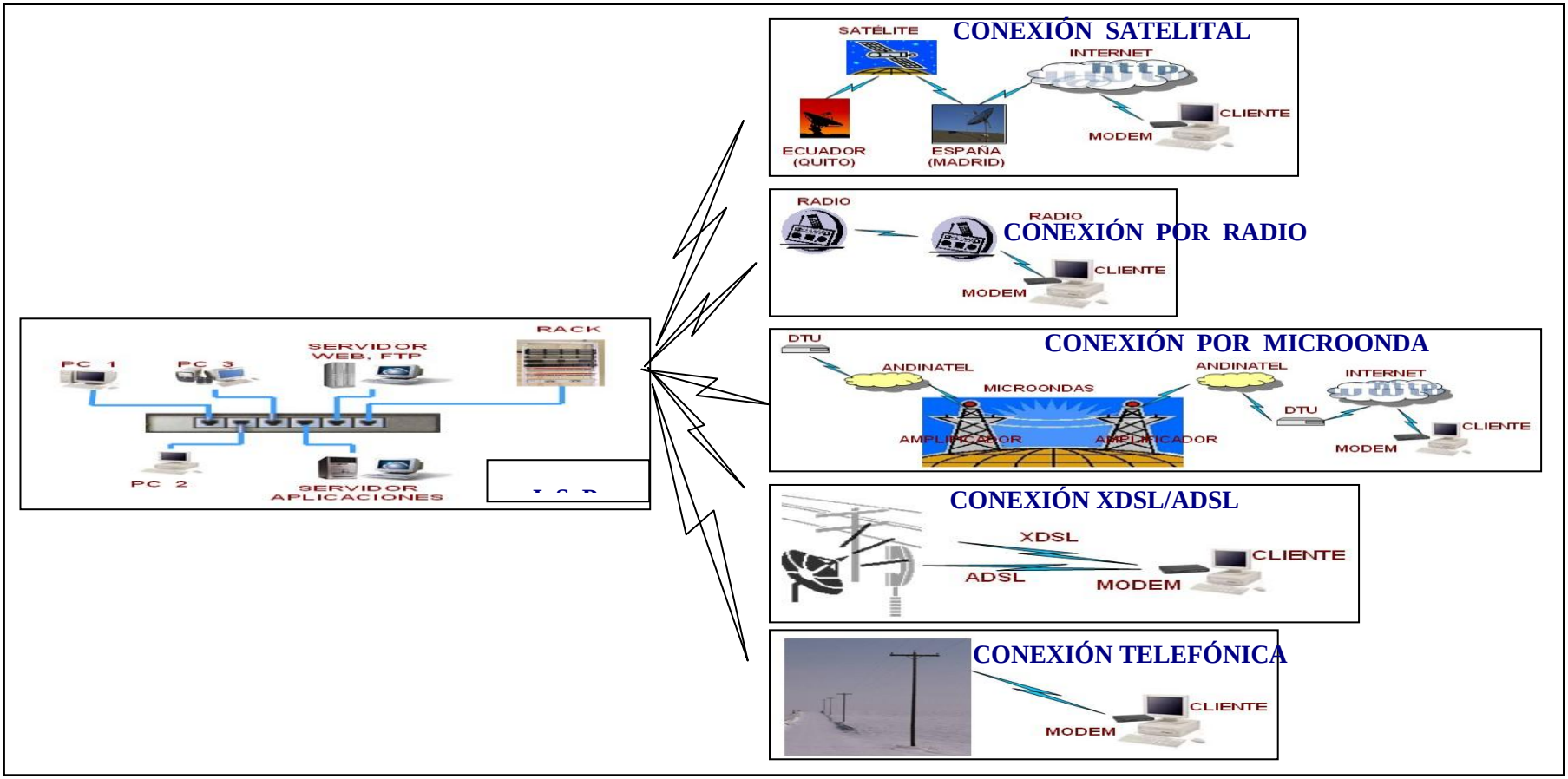


Figura. 2.2 Tipos de Conexión a Internet

CUENTA SHELL

Es el acceso más rudimentario a Internet. Utilizando una cuenta shell, el usuario no necesita tener tipo de software especial alguno para hacer uso Internet. Basta contar con un programa de telecomunicaciones como los que generalmente vienen incluidos con un módem.

Al utilizar una cuenta shell, nuestro computador personal actúa como terminal del proveedor de acceso, por lo que es imposible utilizar las características de nuestra máquina, como gráficas y sonido. Este acceso tiene las siguientes desventajas:

- Debido a que nuestra máquina solamente funciona como terminal, la información únicamente puede visualizarse a través de texto. No es posible ver imágenes, sonidos o gráficos.

- Para utilizar este tipo de conexión es necesario que el usuario adquiera conocimientos de UNIX, un S.O.[15]. no muy común entre usuarios convencionales.

- Para transferir programas o manipular información, es necesario utilizar como puente la máquina de la compañía que le proporciona su cuenta para volver a transferirla a su computador.

SLIP Y PPP

[15] Sistema Operativo.

Una conexión SLIP o PPP permite conectar un computador a una red local enlazada a Internet. Por ejemplo, usted se conecta a su proveedor, que se encuentra dentro de Internet. Con conexión SLIP o PPP, su computador se enlaza a Internet mientras dure la llamada telefónica, lo que permite acceder a todos los servicios de Internet con el ambiente gráfico de la máquina. Para realizar esta conexión se requiere tener software que soporte el protocolo TCP/IP. Este servicio tiene las siguientes características:

- Acceso gráfico y amigable a Internet, utilizando el potencial de su computador.
- Correo electrónico Mundial.
- Ideal para usuarios individuales o empresas.

LAN CONMUTADO

Es un servicio que conecta una red local (LAN), a través de una línea conmutada a Internet. Este servicio requiere una línea dedicada. Se caracteriza por:

- Permite conexiones múltiples bajo una línea conmutada.
- Ejecuta el protocolo PPP.

- Acceso completo a Internet.

- Transferencia rápida de archivos utilizando el protocolo PPP.

- Permite controlar los costos de comunicación.

- Excelente opción para empresas que quieran crecer poco a poco dentro del mundo de Internet.

- Conveniente para redes de 10 a 30 personas.

LÍNEA DEDICADA

Es un enlace dedicado de las oficinas del proveedor de servicio a su compañía, utilizando microonda digital o RDI (Red Digital Integrada). Sus características son:

- Permite a la empresa estar conectada a Internet las 24 horas del día, los 365 días del año.

- Acceso de alta velocidad utilizando comunicaciones digitales.

- Este tipo de enlaces es para empresas que deseen un ancho de banda amplio.

- Acceso completo a Internet para toda la compañía.

- Intercambio de información con tiempos de respuesta rápidos.

- Conexión de alta velocidad para el traspaso de archivos y el acceso a la información.

- Es fácil aumentar ancho de banda.

- Ideal para conexiones de "LAN"[16] y "WAN"[17].

Para acceso dedicado, un usuario necesita:

- Contratar, junto con un proveedor de medios, una "LPCD"[18]

- Pedir a su proveedor de acceso que instale conectividad IP a través de la línea, convirtiendo el computador conectado en un nodo permanente de Internet, con dirección única y divulgado mundialmente

- Las LPCDs pueden variar en velocidad, como 64.000 bps (64 Kbps) o 2 millones de bps (2 Mbps), o incluso más, de acuerdo a la velocidad contratada y a la distancia entre el usuario y el proveedor.

[16] Red de Área Local.
[17] Red de Área Extendida
[18] Línea Privada de Comunicación de Datos

2. 4. COMO ACCEDE UN USUARIO A UN ISP

Actualmente aparecen nuevos adelantos en tecnología, servicios y funcionalidades que todos queremos hacer uso, pero… ¿Qué hay por detrás de la tecnología? ¿Cómo funciona?. Ver **Figura 2.3**

En el momento que decide contratar servicio de Internet, debe llamar a las compañías proveedoras de este servicio, llamadas ISP[19] (Internet Service Provider).

[19] Proveedor de Servicios de Internet

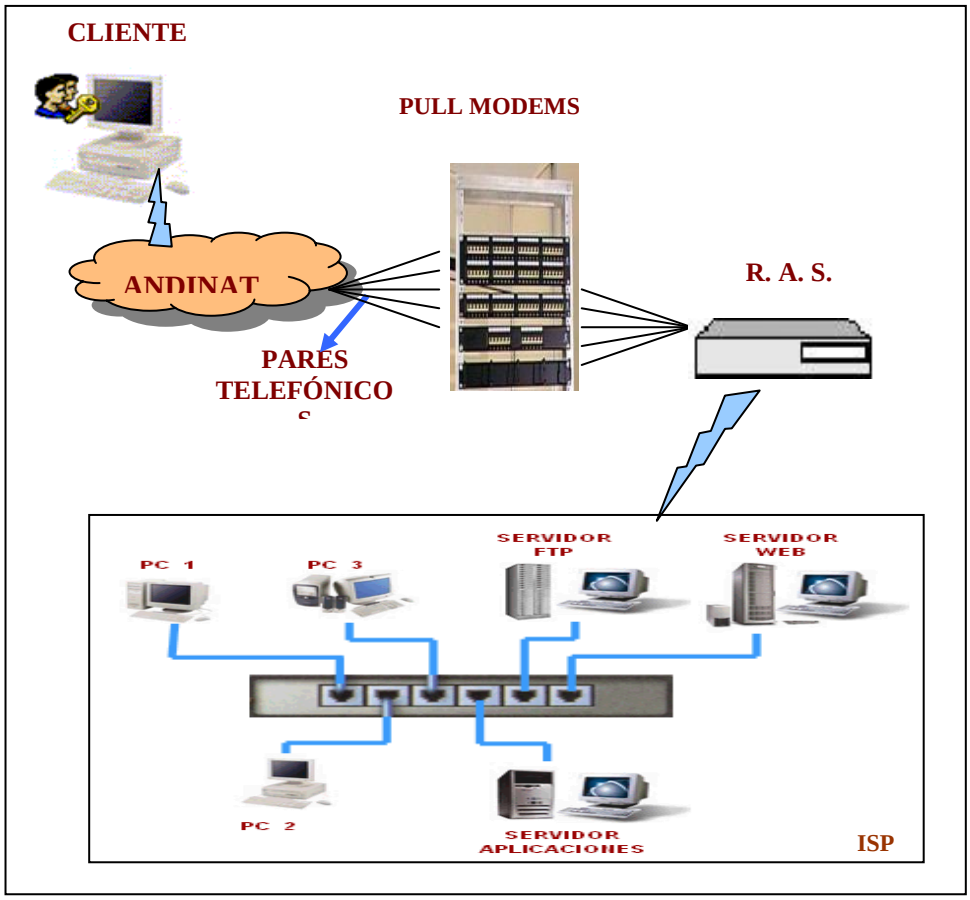


Figura 2.3 Acceso a un ISP

Contratado el servicio, su computador debe ser configurado. Además, comienza a pagar por el servicio, el costo depende del plan contratado.

2. 4. 1. ¿QUÉ TIPOS DE PLANES EXISTEN?

El plan y el valor varia según el ISP, todos los planes se pueden agrupar dentro de dos categorías:

- Planes de Costo Variable

- Planes de Costo Fijo

2. 4. 2. ¿CÓMO ES QUE MI COMPUTADOR RECIBE INFORMACIÓN DESDE LA RED MUNDIAL INTERNET?

Contratados los servicios de un ISP, su computador se conecta a la red pública telefónica (ANDINATEL, ETC.) por medio de un modem, para tener acceso al ISP.

2. 4. 3. PERO… ¿QUÉ INFORMACIÓN SE TRANSFIERE?

La red de comunicaciones del ISP, obtiene información de una serie de páginas Web que se conectan a ella. Las páginas Web, son la parte gráfica de Internet que permiten una comunicación diversa al presentar texto, gráficos, animación, fotos, sonido y video. Entre ellas encontramos:

Servicios de correo (mail)

Servicios de Chat

Servicios de noticias

Páginas Web publicadas por clientes (personas o empresas), etc.

El ISP se conecta a la Red Mundial Internet Figura 2.4. A esta última red se conectan todos los ISP del mundo, produciéndose un gran intercambio de información. Así el ISP contratado, recibe información de todas partes del mundo, que es transmitida a su computador personal, mediante la cadena de conexiones.

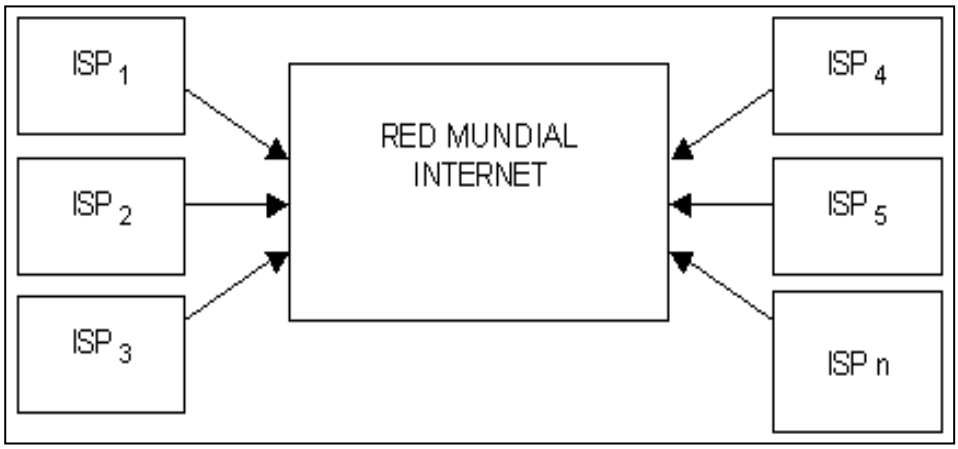


Figura. 2.4 Interconexión de ISPs

Todos los casos de acceso a Internet, mediante la conexión con otro computador, por medio de línea telefónica.

Desde un punto de vista conceptual no es difícil. Se ejecuta un Software de comunicación, que necesita un módem, hardware que actúa de intermediario (interfaz) entre el computador y sistema telefónico.

CAP. III

PROTOCOLOS DE CONEXIÓN

PROTOCOLOS VS. TARIFACIÓN

3. PROTOCOLOS DE CONEXIÓN

3. 1. DEFINICIONES

3. 1. 1. INTRODUCCIÓN

La Organización Internacional de Estandarización, "OSI"[20]. Tiene por objetivo normalizar la creación de productos. El problema al implantar OSI fue que algunas compañías poseían procedimientos propios para interconectar Hardware y Software a otros Sistemas.

Los fabricantes de Hardware y Software solicitaron un soporte para el estándar OSI, sus métodos estaban inmutables, y el acercamiento con OSI, era lento o inexistente. Novell y otras compañías expidieron sus estándares de soporte a otros sistemas, OSI ofrece formas de evaluación para interconexión de redes.

Existen protocolos de comunicación comerciales, los cuales son utilizados de forma transparente, en transferencias por módem, comunicación inteligente de algún banco, etc. Ver **Figura 3.1.**

[20] International Organization for Standarization

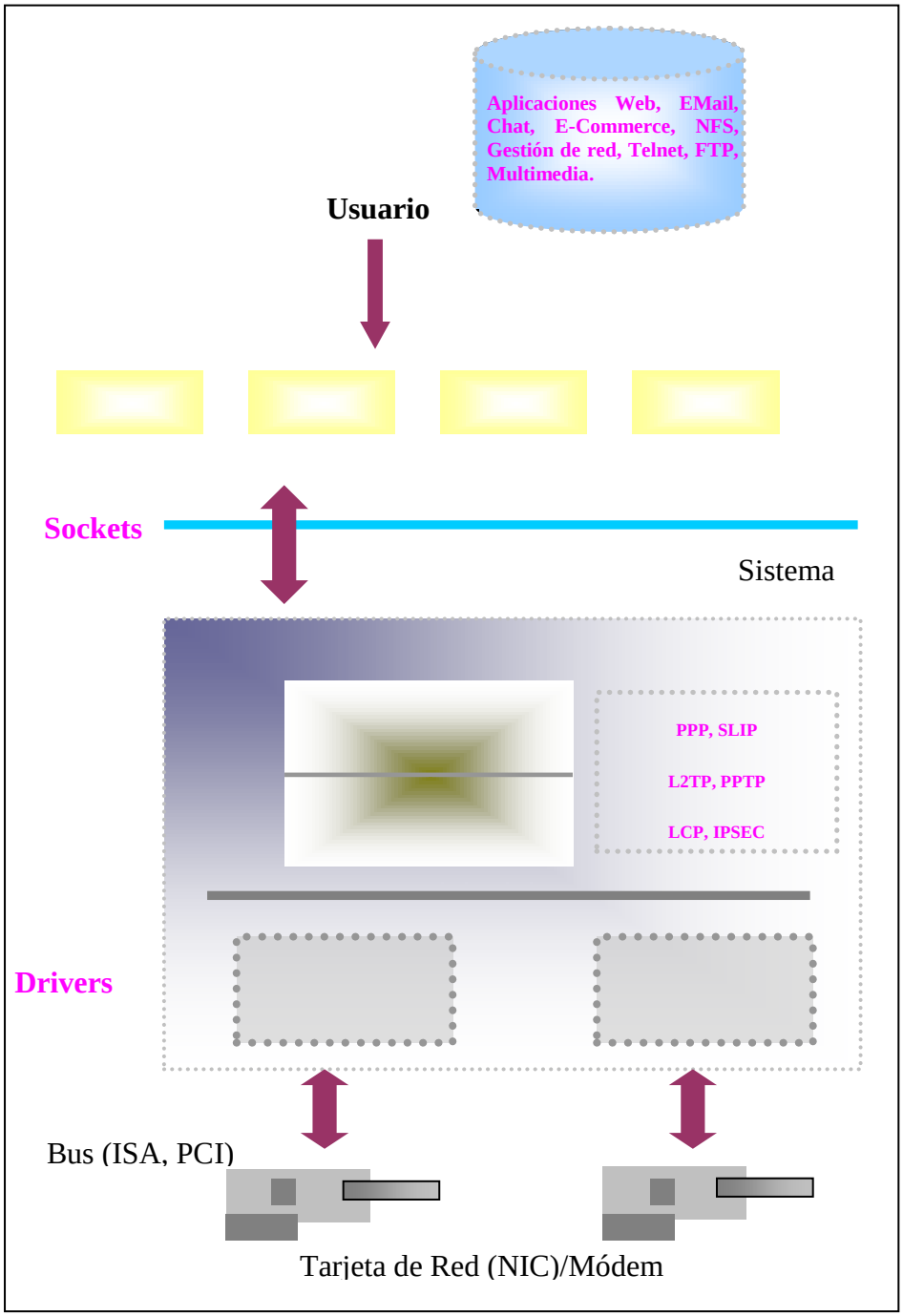


Figura 3.1. Arquitectura Protocolos de Comunicación

3. 1. 2. PROTOCOLO

DEFINICIONES

"Normas que rigen las comunicaciones entre ordenadores para intercambiar información" [21]

Las capas de protocolo intercambian información, añade datos propios de control, para transferirlos en conjunto. Forma unidades de datos que contienen datos tomados de la capa anterior junto a datos propios, al conjunto obtenido se le llama "PDU" [22]

"Los son reglas utilizadas en una red para establecer comunicación entre nodos" [23]

En los protocolos se definen niveles de comunicación. Las reglas de nivel más alto definen ¿cómo se comunican las aplicaciones?, mientras las de nivel inferior definen ¿cómo se transmiten? las señales por cable

"Protocolo es un conjunto de reglas que sirven para realizar una acción"[24]

Los protocolos de Internet son estándares aprobados por la comunidad mundial, representada en el "IETF"[25] . Estos permiten realizar funciones en ambientes diferentes.

[21] Uyless BLACK. Redes de Computadoras, Pág. 68
[22] Unidad de Datos del Protocolo
[23] www.microsoft.com/software/protocolos
[24] www.redes.com/documentos/protocolos.htm

Los protocolos gestionan dos niveles de comunicaciones. Las reglas de alto nivel definen como se comunican las aplicaciones, mientras que las de nivel inferior definen como se transmiten las señales por cable

NIVEL DE PROTOCOLO

En los protocolos de red de área local podemos distinguir dos grupos. Los protocolos de nivel físico y de enlace, que definen funciones asociadas con el medio de transmisión: envío de datos a nivel de bits y trama, y modo de acceso al medio. Los protocolos vienen determinados por el tipo de red. El segundo grupo realiza la función de los niveles de red y transporte, es decir se encargan del encaminamiento de información y de garantizar una comunicación extremo a extremo libre de errores.

Transmiten información a través de la red en segmentos llamados paquetes. Los protocolos definen su propio formato de paquetes, el que especifica el origen, destino, longitud y tipo del paquete, así como información redundante para el control de errores.

Protocolos de nivel 1 y 2 dependen del tipo de red, mientras que en los niveles 3 y 4 hay diferentes alternativas. Los protocolos OSI presentan una solución técnica potente y flexible, que actualmente esta escasamente implantada en redes de área local.

[25] Internet Engineering Task Force

PROTOCOLOS PARA REDES E INTERCONEXIÓN DE REDES.

El protocolo de red incluye los niveles de red y transporte; define la conexión de redes similares y encaminamiento entre redes similares o distintas. En este nivel es posible filtrar paquetes sobre una LAN en una interconexión de redes, de manera que no necesiten saltar a otra LAN cuando no es necesario.

PROTOCOLOS DE APLICACIONES.

La interoperatividad se define en niveles superiores de los protocolos. Otras aplicaciones ínter operativa incluyen paquetes de correo electrónico. Esta permite a los usuarios intercambiar archivos de correo en sistemas distintos (DOS, Macintosh, UNIX, etc.).

3. 1. 3. CARACTERÍSTICAS

Los elementos que definen un protocolo son:

- Sintaxis: formato, codificación y niveles de señal de datos.
- Semántica: información de control y gestión de errores.
- Temporización: coordinación entre la velocidad y orden secuencial de las señales.

Las características más importantes son:

DIRECTO / INDIRECTO

Los enlaces punto a punto son directos, los enlaces entre diferentes redes son indirectos ya que intervienen elementos intermedios.

MONOLÍTICO / ESTRUCTURADO

El emisor tiene el control en una sola capa del proceso de transferencia. En protocolos estructurados, varias capas se coordinan y dividen la tarea de comunicación.

SIMÉTRICO / ASIMÉTRICO

Simétrico

La comunicación sincrónica, sucede al transmitir bits a ritmo constante. Esta técnica permite transmitir datos entre dos dispositivos por medio de una línea de transmisión donde los datos se transmiten en forma de bloques.

La transmisión sincronía puede estar orientada a bit, carácter o en bloque.

Asincrónica

La comunicación Asincrónica, transmitir bits en cualquier instante. La información transmitida se da por caracteres individuales. Cada carácter va precedido de una señal de inicio y termina con una parada en el cual el receptor establece la sincronización.

Los bits especiales son:

- Stara avisa la llegada de un carácter.
- Stop avisa que el carácter ha terminado.

3. 1. 4. FUNCIONES

SEGMENTACIÓN Y ENSAMBLADO

Es necesario dividir los bloques de datos en unidades pequeñas iguales en tamaño, este proceso se llama segmentación. El bloque básico de segmento en una capa de protocolo se llama PDU. La utilización del bloque se da por:

- La red sólo admite la transmisión de bloques de un cierto tamaño.
- El control de errores más eficiente para bloques pequeños.
- Evitar monopolización de red.

- Con bloques pequeños, la necesidad de almacenamiento temporal es menor.

- Cuantas más PDU, más tiempo de procesamiento.

ENCAPSULADO

Es el proceso de adherir información de control al segmento de datos. Esta información es el direccionamiento del emisor/receptor, código de detección de errores y control de protocolo. Ver Figura 3.2

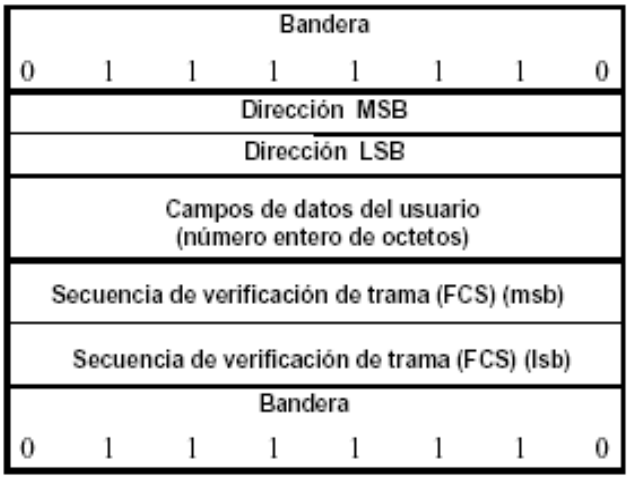


Figura 3.2 Encapsulado

CONTROL DE CONEXIÓN

Hay bloques de datos de control y otros de datos y control. Cuando utilizan datagramas, los bloques incluyen control y datos. En circuitos virtuales hay bloques de control que son encargados de establecer la conexión del circuito virtual.

Si utilizan circuitos virtuales hay que numerar los PDU y llevar un control en el emisor y en el receptor de los números.

ENTREGA ORDENADA

El envío de PDU puede acarrear el problema, si existen algunas rutas posibles, lleguen al receptor PDU desordenados o repetidos, el receptor debe reordenar los PDU. Hay sistemas que tienen mecanismos de numeración; esto hace que el módulo sea eficaz para hacer imposible que haya dos segmentos en red al mismo tiempo y con el mismo número.

CONTROL DE FLUJO

Existen controles de flujo de parada y espera. El control de flujo es necesario en varios protocolos, el problema de saturación del receptor se produce en cualquier capa del protocolo.

CONTROL DE ERRORES

Generalmente se utiliza un temporizador para retransmitir una trama. Cada capa de protocolo debe tener su propio control de errores.

DIRECCIONAMIENTO

Cada dispositivo intermedio de almacenamiento posee una dirección única. En cada terminal existen varios agentes que utilizan la red, ellos tienen asociado un puerto.

Hay ocasiones que se usa un identificador de conexión; cuando dos estaciones establecen un circuito virtual. La utilización de identificadores simplifica los mecanismos de envío de datos.

MULTIPLEXACIÓN

Es posible multiplexar las conexiones de una capa hacia otra, es decir que de una conexión de capa superior, se establecen varias conexiones en una capa inferior.

SERVICIOS DE TRANSMISIÓN

Los servicios que presta un protocolo son:

- Prioridad: hay mensajes (los de control) que deben tener prioridad respecto a otros.
- Grado de servicio: hay datos que deben de retardarse y otros acelerarse (vídeo)
- Seguridad.

3. 2. PROTOCOLOS TCP/IP (IPV4 VS. IPV6)

3. 2. 1. INTRODUCCIÓN

Los procesos que conducen al cambio se manifiestan con un incremento, en tamaño y carga que obliga a mejorar los recursos para mantener el servicio, como aplicaciones nuevas que demandan más de la tecnología que hace posible proporcionar nuevos servicios.

Para definir la próxima generación de protocolo de Internet se han generado varías propuestas, Ha surgido un acuerdo para adoptar una propuesta conocida como Simple IP Plus como estándar para el "IPng"[26]. El protocolo propuesto se conoce a menudo como "IPv6"[27] para distinguirlo del protocolo actual, IPv4.

3. 2. 2. ¿QUÉ ES EL IPV6?

IPng o IPv6 es un protocolo diseñado por la "IETF"[28] para reemplazar la versión actual del protocolo IP.

Se espera que el IPv6 gradualmente reemplace al IPv4, coexistiendo ambos algunos años durante un período de transición.

3. 2. 3. DIFERENCIAS DE IPV6(IPNG) VS. IPV4(TCP/IP)

[26] Next Generation Internet Protocol.
[27] Internet Protocol Version 6
[28] Internet Engineering Task Force

Cuando IPv4 fue estandarizado, hace unos quince años, nadie imaginó que se convertiría en una arquitectura de amplitud mundial, con un número de usuarios superior al centenar de millones y que crece de forma exponencial. Aquel primer *INTERNET* fundado, sobre todo, con fines experimentales, científico-técnicos y con objetivos militares, no se parece en nada a la actual.

El número de direcciones es el cambios más importantes que afectan a la versión 6 del protocolo IP, teóricamente serían 2^{128} direcciones posibles. Que significa más de 665.000 trillones de direcciones.

- IPv6 posee una mayor capacidad de Ruteo y Direccionamiento.
- Soporte de estructuras Jerárquicas.
- Posee una cabecera de 40 bytes.
- Menor número de capos en la cabecera respecto a IPv4. (de 12 a 8)

FORMATO DE LA CABECERA DE IPV6

La cabecera tiene un tamaño de 40 bytes se ha simplificado omitiendo algunos campos y haciendo que otros sean opcionales. Los campos son los siguientes: Ver **Figura 3.3.**

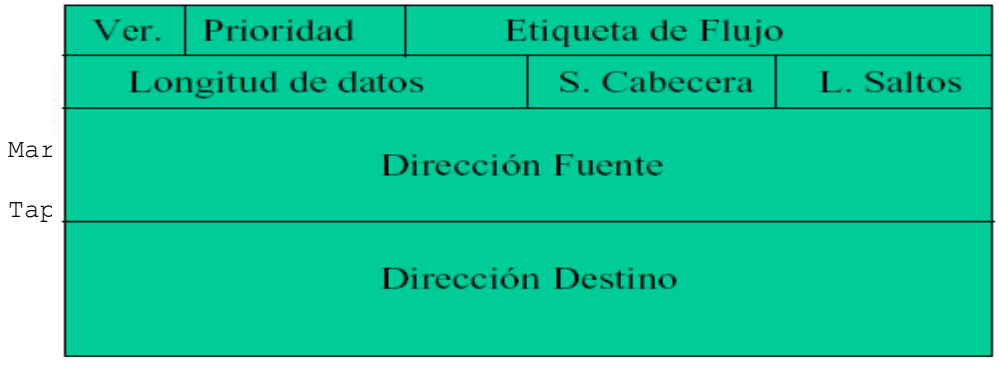


Figura 3.3. Formato de la Cabecera de IPv6

Versión: Este campo ocupa 4 bits, contiene el número de versión del IP, en este caso 6.

Prioridad: Ocupa 4 bits, indica la importancia del paquete que se esta enviando.

Etiqueta de Flujo: Ocupa 24 bits. Indica si el paquete requiere un tratamiento especial por parte de los routers que lo soporten.

Longitud: Ocupa 16 bits. Indica la longitud en bytes de los datos del mensaje

Siguiente Cabecera: Ocupa 8 bits e indica a que protocolo corresponde la cabecera que esta a continuación de la actual.

Tiempo de vida: Ocupa 8 bits, tiene similar función de la versión 4.

Dirección de origen: Ocupa 128 bits (16 octetos), es el número de dirección del origen.

Dirección de Destino: Ocupa 128 bits (16 octetos). Es el número de dirección del destino.

Las extensiones que permiten añadir esta versión del protocolo se sitúan inmediatamente después de la cabecera normal, y antes de la cabecera que incluye el protocolo de nivel de transporte. El tamaño de la cabecera no esta limitado a un valor fijo de bytes.

LAS PRINCIPALES CARACTERÍSTICAS DEL NUEVO IPv6, COMO DIFERENCIAS RESPECTO A IPv4

- Protocolo diseñado para ser ampliado, con funcionalidades adicionales, sea a través de nuevas cabeceras de extensión o de opciones incluidas en cabeceras ya existentes.

- Los nuevos números IP constan de 128 bits, lo cual permite efectuar una división muy jerárquica del espacio de direcciones. Ello posibilitará incluir la dirección física de la máquina en la propia dirección IP, facilitando el proceso de autoconfiguración.

- Incluye cabeceras destinadas a la autentificación y encriptación de datagramas.

- Permite a la fuente encaminar directamente sus datagramas.

- El soporte de encapsulado es transparente, dado su diseño de cabeceras encadenadas.

- La fragmentación, la realiza la fuente.

- La gestión de Multicasting y Anycasting (IGMP) ha pasado a formar parte del nuevo ICMP.

- Para acelerar el cálculo de enrutamiento y atender las necesidades de las aplicaciones en tiempo real, cada datagrama puede contener un *identificador de flujo*. Esos identificadores son, equivalentes al concepto de circuitos virtuales.

- IPv6 no incluye una suma de control en la cabecera. Para asegurar la validez de la información la capa "UDP"[29] está obligada a utilizar su opción de suma de control.

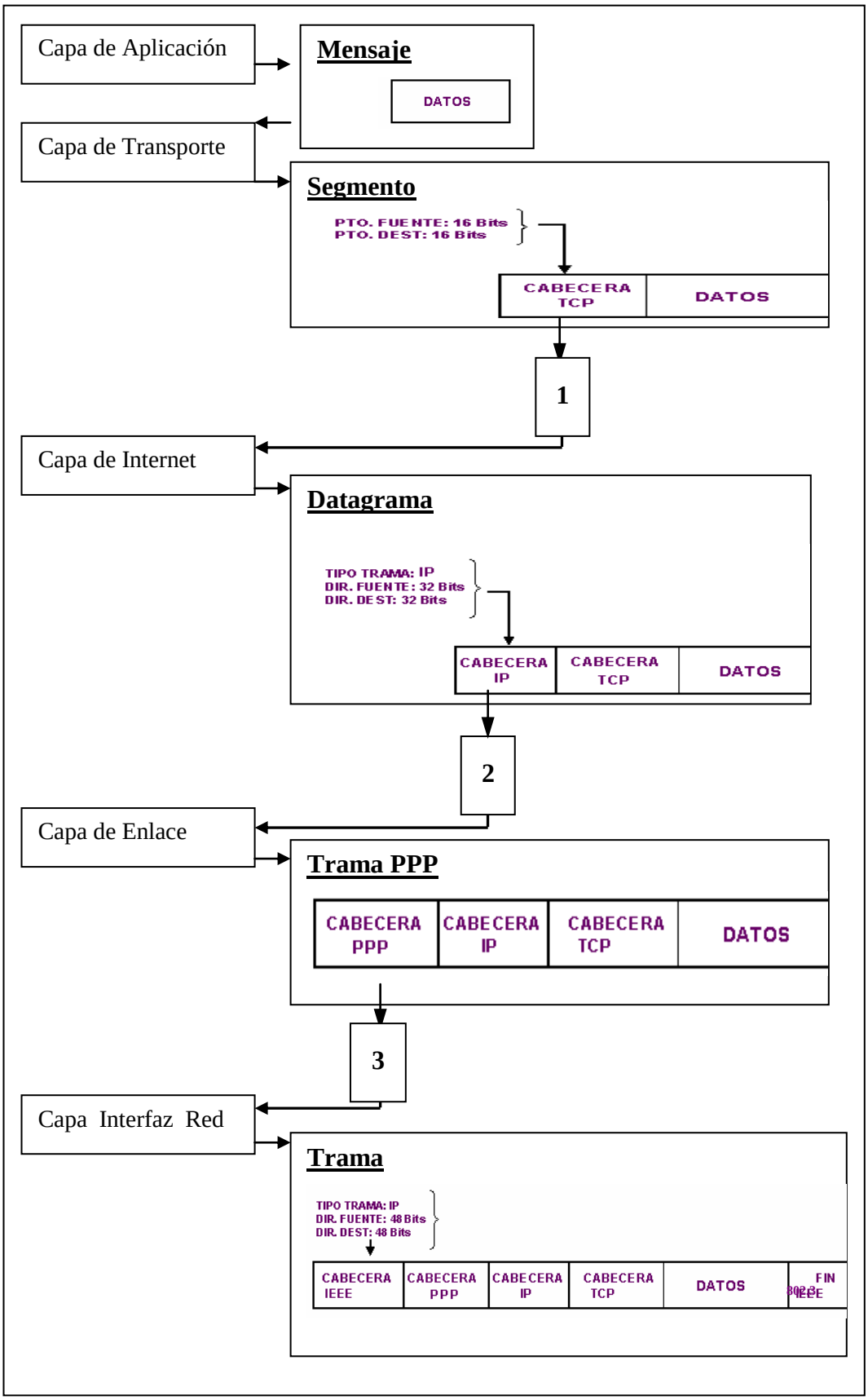
- Las nuevas direcciones IP, constan de 128 bits. IPv6 utiliza notación hexadecimal en grupos de 16 bits, separándolos por el carácter de dos puntos (*:*).

Queda un largo trecho hasta que IPV6 se implante de forma mayoritaria, pero sin duda incorpora numerosas características que lo hacen atractivo, como el soporte de comunicaciones en tiempo real, autoconfiguración de sistemas, seguridad, etc.

3. 3. PROTOCOLOS EN LA TARIFACIÓN

[29] User Datagram Protocol

En la siguiente figura se muestra una ilustración de los protocolos que intervienen en el proceso de conexión del cliente Dial-up y el ISP; ver la Figura. 3.4


Capa de Aplicación
Mensaje
DATOS
Capa de Transporte
Segmento
PTO. FUENTE: 16 Bits
PTO. DEST: 16 Bits
CABECERA TCP
DATOS
1
Capa de Internet
Datagrama
TIPO TRAMA: IP
DIR. FUENTE: 32 Bits
DIR. DEST: 32 Bits
CABECERA IP
CABECERA TCP
DATOS
2
Capa de Enlace
Trama PPP
CABECERA PPP
CABECERA IP
CABECERA TCP
DATOS
3
Capa Interfaz Red
Trama
TIPO TRAMA: IP
DIR. FUENTE: 48 Bits
DIR. DEST: 48 Bits
CABECERA IEEE
CABECERA PPP
CABECERA IP
CABECERA TCP
DATOS
FIN

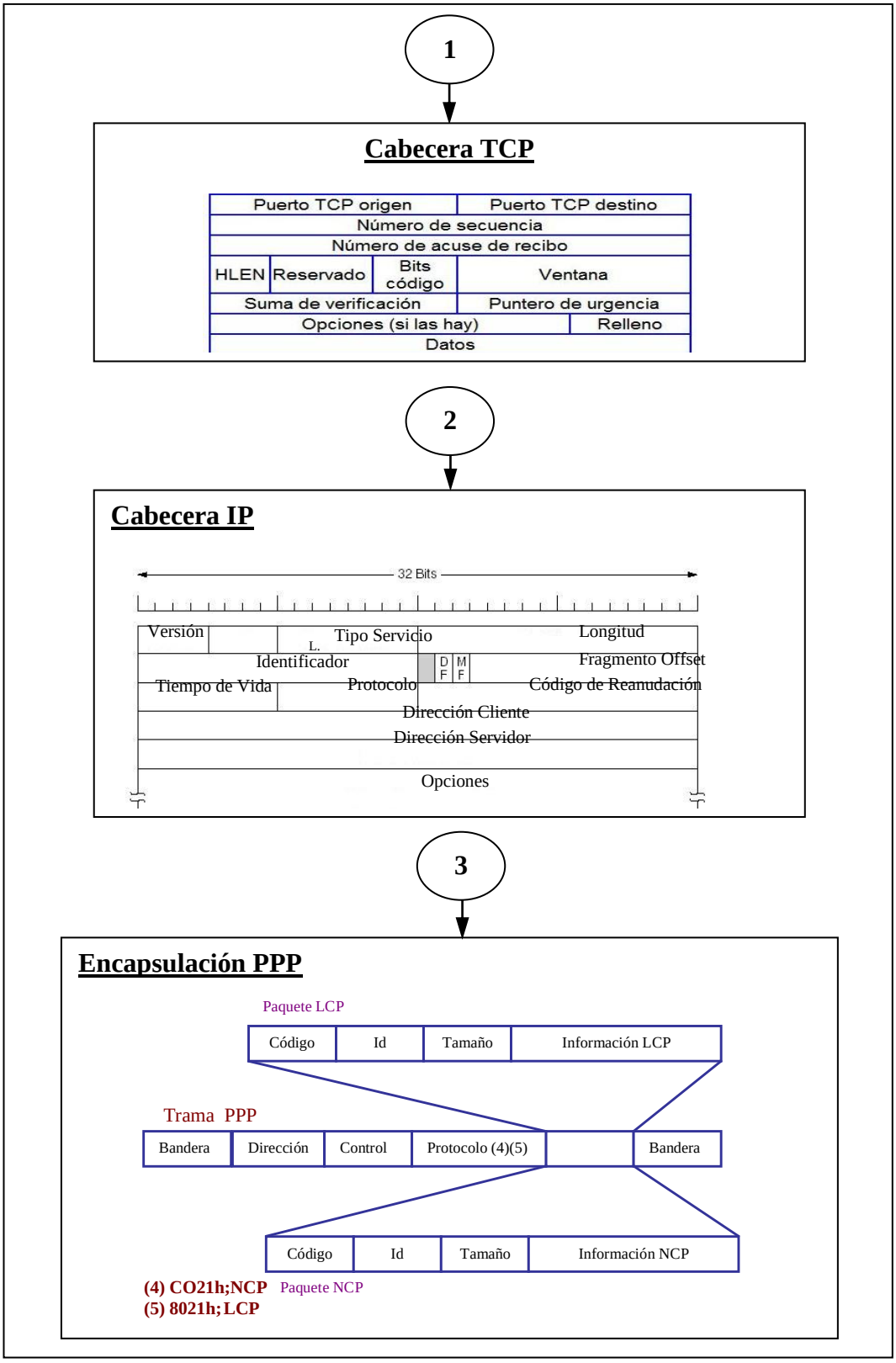


Figura 3.4 Protocolos en la Tarifación

3. 3. 1. PROTOCOLO PPP

Es un protocolo avanzado para transmisiones de red sobre conexiones entre dos puntos. Diseñado para enlaces simples que transportan paquetes entre dos máquinas. Se permite transmisión full-duplex.

CARACTERÍSTICAS

Incluye características como:

- Discar bajo demanda.
- Rediscar si está ocupado.
- Negociación de opciones.
- Comprensión de encabezados, uso de más de un protocolo de capa de red, etc.
- PPP trasforma un puerto serie de computadora en adaptador de red, transmite datagramas al igual que un adaptador de red por la encapsulación del data grama.

PPP proporciona un modo para la asignación automática de direcciones IP necesita estar configurado para autentificar al usuario mediante los protocolos “CHAP” [30] o “PAP” [31].

[30] Autentificación criptográfica o no criptográfica
[31] Protocolo de Autentificación de Contraseña

TRAMA

La trama PPP, se representa en la Figura 3.3 contiene información que identifica lo siguiente:

Delimitadores. Marcan el principio y el fin de la trama.

Dirección. Contiene la dirección destino.

Control. Contiene el número de secuencia para asegurar una adecuada administración.

Protocolo. Identifica si la trama contiene IP, IPX, Apple Talk u otra.

Información. Contiene los datos, que pueden variar en longitud.

Secuencia de verificación de la trama **Figura 3.5**. Calcula un código de paridad para la comprobación de errores.

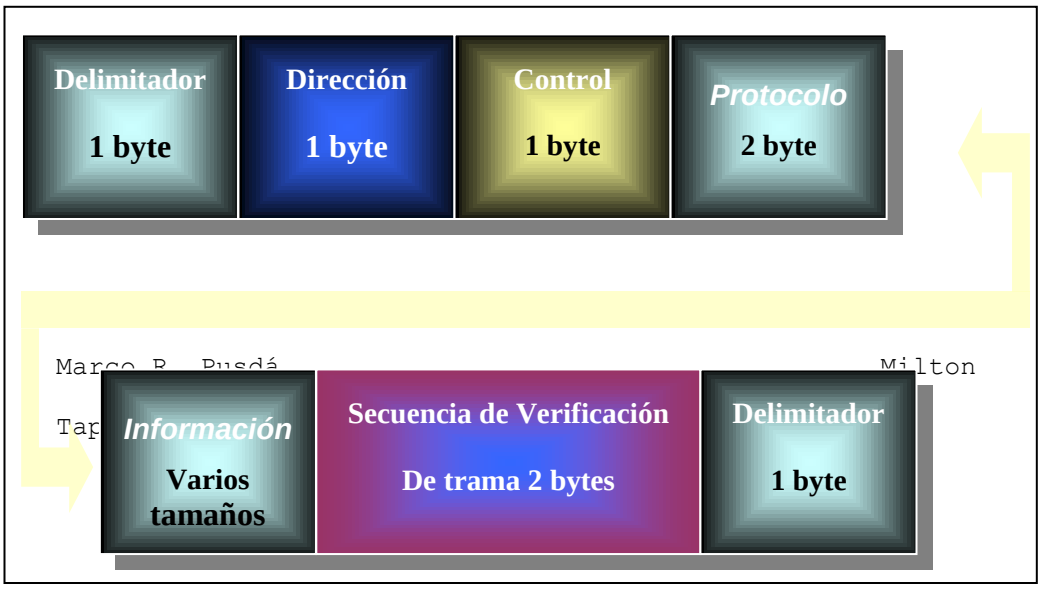


Figura 3.5. Formato de trama del protocolo punto a punto.

PILA DEL PROTOCOLO

PPP esta conformado por una pila de protocolos, se detalla en la Figura 3.6

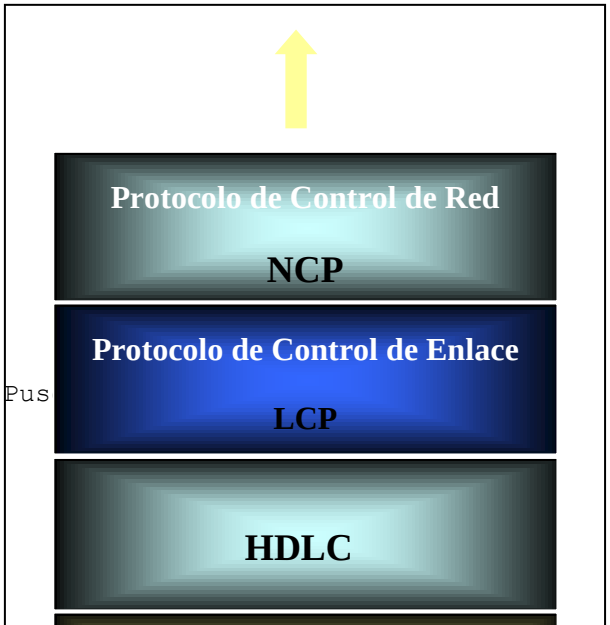


Figura 3.6. Pila de protocolos punto a punto.

Nivel Físico. Define la transmisión sobre lineas asincronas y sincronas mediante el uso de los protocolos de comunicación.

Nivel de Enlace de Datos. Se basa en la estructura de la trama definida en el nivel de enlace de datos. El protocolo de control de enlace "LCP"[32], establece y administra enlaces entre las estaciones conectadas. Especifica metodos de encapsulacion, tamaños de paquetes y comprueba para asegurarse de que los enlaces funcionan adecuadamente. Los paquetes LCP se usan para el establecimiento, mantenimiento y finalización de conexiones.

Nivel de Red. Contiene un conjunto de protocolos denominados Protocolos de Control de red "NCP"[33], cada uno con propios procedimeintos de control.

COMPONENTES DEL PROTOCOLO PPP

[32] Link Control Protocol
[33] Network Control Protocols

1) Un método de encapsulado sin ambigüedades que identifica claramente el inicio de un datagrama y el final del anterior.

2) Un protocolo de control de enlace, para activar y probar líneas; negociar opciones y desactivar el enlace ordenadamente cuando ya no es necesario.

3) Una familia de NCPs para negociar opciones de capa de red con independencia del protocolo de red usado.

PROCEDIMIENTO DE CONEXIÓN

El procedimiento típico de conexión es:

- El computador llama al enrutador del proveedor a través de módem.
- El módem del enrutador contesta y establece una conexión física
- El computador y el enrutador intercambian una serie de paquete LCP para seleccionar los parámetros PPP por usar.
- Se envía una serie de paquetes NCP para configurar la capa de red.
- Se asigna al PC una dirección IP a través de NCP para IP.
- El enlace continúa configurado para comunicaciones, hasta que LCP, NCP , algún evento externo lo tumbe.
- Se usa NCP para desmantelar la conexión en la capa de red y liberar la Dirección IP.

- Se usa LCP para eliminar la conexión a nivel de enlace.

- El módem cuelga liberando la capa física.

FUNCIONES

Autenticación

"PPP suele utilizar para conectar un usuario a una red. Mediante conexión telefónica. Se usan las conexiones telefónicas para conectar a un grupo de trabajo a una LAN mediante un encaminador desde la filial a las oficinas centrales"[34]

[34] TCP/IP. Dr. Sidnie Feit, Pág. 46

CONTROL AUTOMÁTICO DE CALIDAD DEL ENLACE

"PPP proporciona una forma muy simple de comprobar la calidad de un enlace. El proceso de control de enlace simplemente cuenta el numero de tramas y actetos enviados y recibidos. También se cuenta las tramas descartadas y los errores. Periodicamente, se envia un informe al otro extremo del enlace"[35]

3. 3. 2. PROTOCOLO DE INTERFAZ DE LÍNEA SERIE (SLIP)

"SLIP"[36], es una forma de encapsulación para datagramas IP; diseñado en 1984 por Rick Adams para conectar estaciones de trabajo al Internet a través de una línea de discado usando Modem.

FORMATO:

Cada datagrama IP se termina mediante el carácter C0.

Si el carácter C0 se presenta en el contenido del datagrama; se utiliza la secuencia de dos bytes DB, DC el carácter DB es el carácter de escape de SLIP.

Si en el contenido se presenta el carácter de escape; se reemplaza por la secuencia DB, DD. SLIP deja a las capas superiores la detección y recuperación de marcos perdidos.

[35] Tecnología Física y de enlace de Datos. Ing. Eccotty Wilians, Pág. 47
[36] Serial Line IP

CSLIP

Debido al gran tamaño de la cabecera de IP y TCP, para enviar información, se creó una nueva versión de SLIP llamada "CSLIP"[37]. Reduce la cabecera típica de 40 bytes a 3 o 5 bytes, los campos de la cabecera no varían durante una conexión.

CARACTERÍSTICAS

1) SLIP permite conectar un computador a una red mediante un enlace de acceso telefónico.

2) SLIP no proporciona secuencia de comprobación de trama y deja la comprobación de errores a las capas superiores.

3) SLIP no contiene ningún protocolo que no sea IP.

4) SLIP se puede utilizar para la comunicación entre host, host a encaminador o entre encaminadores.

[37] compressed SLIP

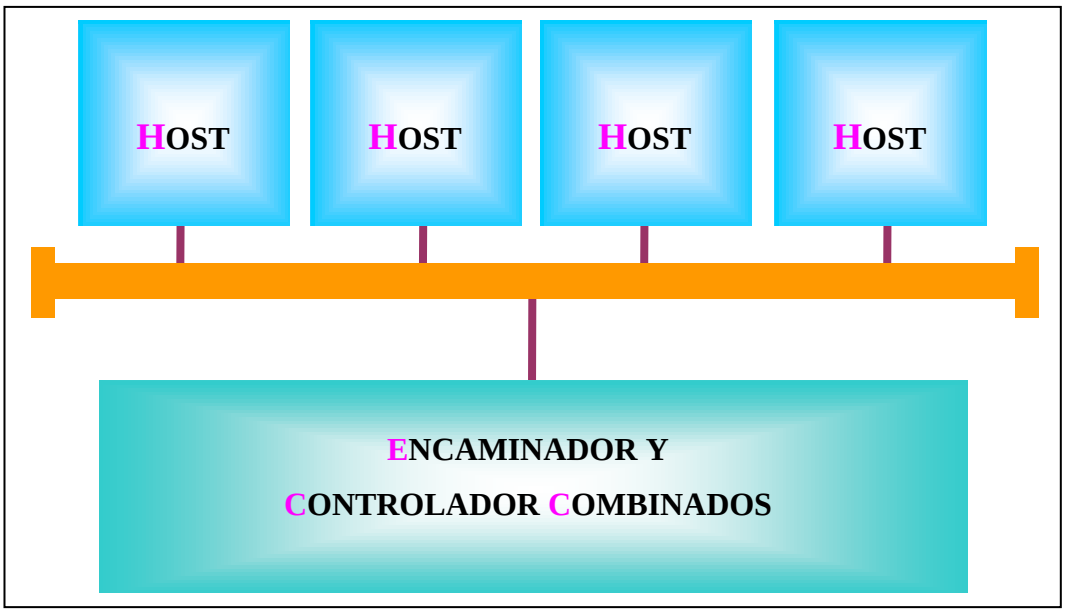


Figura 3.7. Conexiones SLIP.

La **Figura 3.7** muestra un servidor de comunicaciones que admite tanto terminales Ascii <<*sin inteligencia*>> como acceso telefónico con SLIP. El dispositivo actua como un encaminador IP para tráfico SLIP.

3. 3. 3. PROTOCOLO TUNNELING NIVEL 2 (L2TP)

L2TP encapsula datos de aplicación, datagramas e información de tramas punto a punto, contiene una cabecera de entrega, una cabecera IP y una cabecera Genérica Ruteo Encapsulación (GRE).

Para crear un túnel, L2TP emplea dos funciones básicas: LAC y LNS. "LAC" [38] realiza funciones de servidor en línea para el cliente, mientras que "LNS" [39], actúa como servidor de red en el servidor.

[38] Concentrador de Acceso

CARACTERÍSTICAS

1) El protocolo estándar de Tunneling de Nivel 2 garantiza la interoperatividad entre fabricantes, incrementa flexibilidad del cliente y la disponibilidad del servicio.

2) Proporciona un método de túnel sólido.

3) L2TP soporta autenticación de túnel y usuario.

4) L2TP proporciona un completo soporte de asignación dinámica de direcciones IP, en un rango de direcciones IP, incluyendo soporte para direcciones privadas definidas.

5) L2TP proporciona copias de seguridad, permitiendo que múltiples participantes LNS puedan configurarse.

6) L2TP admite un ilimitado número de sesiones en cada LAC y soporta más de 2.000 sesiones.

[39] L2TP Server Network

7) L2TP simplifica la implementación de “VPN”[40].

8) L2TP es un protocolo de comunicación transparente a las aplicaciones de usuarios.

VENTAJAS

L2TP es un protocolo estándar, la interoperatividad entre los fabricantes garantizan la implementación de un servicio estándar VPN de acceso.

La implementación L2TP es una solución que ofrece ventajas a los usuarios de empresas: Estas ventajas incluyen:

- Seguridad y prioridad garantizada para la mayoría de aplicaciones esenciales de trabajo.
- Una mejor conectividad, costes reducidos y libertad para redistribuir los recursos en núcleos de funciones
- Un entorno de acceso de red remoto, flexible y ampliable sin comprometer la seguridad corporativa o poner en peligro las aplicaciones esenciales.

TÉRMINOS PRINCIPALES DE L2TP

Términos principales L2TP

[40] Redes PrivadasVirtuales

L2TP Access Concentrador (LAC)

Añade un dispositivo LAC a componentes físicos de la red conmutada; se coloca con un sistema de terminación PPP capaz de gestionar el protocolo L2TP. Un LAC necesita implementar el medio sobre el cual opera, para admitir tráfico de una o más LNS. Puede *tunelizar* cualquier protocolo que incluya PPP. LAC es el iniciador de llamadas entrantes y el receptor de llamadas salientes. También se conoce como el servidor de acceso a red en el protocolo Layer 2 Forwarding (L2F).

L2TP Network Server (LNS)

Un LNS opera sobre cualquier plataforma con capacidad de terminación PPP. Puede tener únicamente interfaz LAN o WAN, aunque es capaz de terminar las llamadas entrantes en cualquier gama de interfaces PPP. LAC es el iniciador de llamadas entrantes y receptor de llamadas salientes.

Network Access Server

Este dispositivo proporciona a los usuarios acceso temporal a la red. Este acceso es punto a punto, de uso típico en líneas de red telefónica convencional.

3. 3. 4. PROTOCOLO DE CONTROL DE ENLACE (LCP)

LCP se usa para acordar automáticamente las opciones del formato de encapsulación, los límites de manipulación del tamaño, detectar un

enlace y terminar el enlace. Facilidades opcionales provistas son: autenticación de la identidad de ***pares*** de enlace, y determinación de funcionamiento del enlace está funcionando apropiadamente y cuándo está fallando.

FORMATO DE LOS PAQUETES LCP

Hay tres clases de paquetes:

1) Paquetes para configurar enlaces: usados para establecer y configurar el enlace (solicitud de configuración, reconocimiento de configuración, no reconocimiento de configuración y rechazo de configuración).

2) Paquetes para determinar enlaces: usados para terminar el enlace (solicitud de terminación y reconocimiento de terminación).

3) Paquetes de mantenimiento del enlace: usados para manejar y depurar el enlace (rechazo de código, rechazo de protocolo, solicitud de eco, respuesta de eco, solicitud de descarte).

Un paquete LCP es encapsulado en el ámbito PPP, como se muestra en la **Figura 3.8**. El formato de LCP:

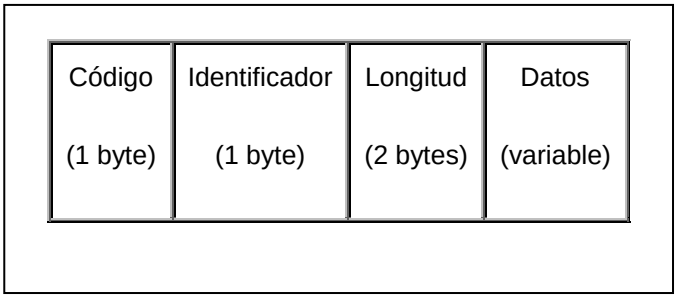


Figura 3.8 Formato de un paquete

Los principales paquetes utilizados por el LCP son:

Solicitud de configuración

Debe transmitirse para abrir una conexión. En el campo de datos se incluirán opciones de configuración que el transmisor desee negociar. Todas estas opciones son negociadas simultáneamente.

Reconocimiento de configuración

Si cada opción de configuración recibida en ***solicitud de configuración*** es reconocida y sus valores son aceptados, la implementación receptora debe transmitir un paquete de ***reconocimiento***.

No reconocimiento de configuración

Si cada opción de configuración es reconocido, contiene valores erróneos, se debe transmitir un paquete de ***no reconocimiento de configuración***. El campo de datos se completa sólo con las opciones no aceptadas de la ***solicitud de configuración***.

Al recibir un paquete de ***no reconocimiento***, el campo de identificación debe ser comparado con la última ***solicitud de configuración***, cuando se envía una ***solicitud de configuración***, las opciones de la mismas deberán ser modificadas.

Rechazo de configuración

Este paquete será transmitido al recibir una ***solicitud de configuración*** en la que algunas opciones no son reconocibles o aceptables para ser negociadas. El campo de datos se completa con las opciones de configuración no aceptables.

Al recibir un ***rechazo de configuración***, el campo identificador se compara con de la última solicitud de configuración.

Solicitud de terminación y reconocimiento de terminación

Son utilizadas para terminar una conexión. Primero se debe transmitir una ***solicitud de terminación***. Estas solicitudes se transmiten hasta recibir un ***reconocimiento de terminación***, en lo cual la capa inferior indique que se perdió la conexión.

Rechazo de código

La recepción de un paquete LCP con un código desconocido indica que el ***par*** está operando con una versión diferente del protocolo. Esto debe ser reportado al transmisor del código desconocido por medio de un

rechazo de código. Al recibir un paquete de este tipo, se deberá reportar el problema y cesar la transmisión.

El campo de datos contiene una copia del paquete LCP que está siendo rechazado.

Rechazo de protocolo

La recepción de paquete PPP con campos de protocolo desconocido indica que el ***par*** está intentando usar un protocolo no aceptado. Esto ocurre cuando el ***par*** intenta configurar un nuevo protocolo.

Solicitud y respuesta de eco

Proveen al LCP un mecanismo para detectar ciclos en la capa de enlace, puede ser utilizado en ambos sentidos. Es útil en la depuración, la determinación de calidad de enlace, la performance, etc.

Luego de recibir una ***solicitud de eco***, se debe transmitir la respuesta correspondiente.

El campo de datos contiene 4 bytes que son utilizados para enviar un número llamado ***mágico***, que es utilizado para detectar enlaces con ciclos. A continuación puede ser transmitido cualquier valor binario elegido por el transmisor.

Solicitud de descarte

El LCP incluye estos paquetes para proveer un mecanismo de *hundimiento* de la capa de enlace de datos, desde el sitio local hacia el remoto. Este mecanismo se utiliza cuando se desea enviar paquetes para realizar alguna prueba, sin que el *par*, realice ninguna acción en función de los mismos. Esto es útil para ayudar en la depuración, el testeo de performance y algunas otras funciones.

Los paquetes de *solicitudes de descarte*, deben ser ignorados al ser recibidos.

Opciones de configuración de LCP

Estas opciones permiten la negociación o modificación de las características por defecto de un enlace punto a punto. Si no se incluyen opciones de configuración en un paquete de solicitud de configuración, se asumen los valores por defecto para las mismas. El permitir valores por defecto para cada opción otorga al enlace la capacidad de funcionar correctamente sin negociaciones, pero sin embargo sin alcanzar una performance óptima.

3. 3. 5. POINT-TO-POINT TUNNELING PROTOCOL (PPTP)

PPTP es, de hecho, un protocolo de túnel industrial estándar que se incorporó por primera vez en Windows NT 4.0. PPTP es una extensión

del Protocolo punto a punto (PPP) y aprovecha las ventajas de los mecanismos de autenticación, compresión y cifrado de PPP.

CARACTERÍSTICAS

Una característica importante en el uso del PPTP es su soporte para VPN.

La mejor parte de esta característica es que soporta VPN`s sobre public-switched telephone networks (PSTNs) que son los comúnmente llamados accesos telefónicos a redes.

PPTP encapsula el paquete PPP encriptado y comprimido en datagramas IPs.

ARQUITECTURA PPTP

En esta parte estudiaremos los siguientes campos:

- Comunicación PPTP
- Control de conexión PPTP
- Tunneling de datos PPTP

La comunicación segura que es establecida usando PPTP involucra tres procesos, cada uno de los cuales requiere la completa realización del proceso anterior. Ahora explicaremos estos procesos y como funcionan:

Conexión y Comunicación PPTP

Un cliente PPTP utiliza PPP para conectarse a un ISP usando una línea telefónica normal o una línea RDSI. Esta conexión usa el protocolo PPP para establecer la conexión y encriptar los paquetes de datos.

Control de Conexión PPTP

Usando la conexión a Internet establecida por el protocolo PPP, el PPTP crea una conexión controlada del cliente PPTP al Servidor PPTP en Internet. Esta conexión usa TCP para establecer la comunicación y esta llamada PPTP Túnel.

Tunneling de datos PPTP

El protocolo PPTP crea datagramas IP conteniendo paquetes PPP encriptados que son enviados a través del Túnel PPTP al Servidor PPTP. El Servidor PPTP desensambla los datagramas IP y desencripta los paquetes PPP, y enruta los paquetes desencriptados a la red privada.

CONTROL DE CONEXIÓN PPTP

El protocolo PPTP especifica una serie de mensajes que son usados para la sesión de control. Estos mensajes son enviados entre el cliente PPTP y el servidor PPTP. Los mensajes de control establecidos, mantienen y terminan el Túnel PPTP.

Los mensajes de control son enviados dentro de los paquetes de control en un datagrama TCP. Una conexión TCP es activada entre el cliente PPTP y el Servidor. Este path es usado para enviar y recibir mensajes de control. El datagrama contiene una cabecera PPP, una TCP, un mensaje de control PPTP y sus apropiadas reglas. La construcción es como se presenta en la **Figura 3.9:**

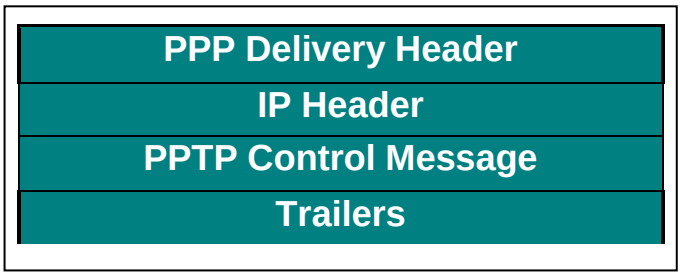


Figura 3.9 Formato de un Datagrama

Autentificación

La autentificación inicial en la llamada puede ser requerida por un ISP de servidor de acceso a la red. Un servidor PPTP es un gateway a tu red, y necesita la base estándar de *login*, en WindowsNT. Todos los clientes PPTP deben proporcionar un login y password. De todas formas, el login de acceso remoto usando un PC bajo NT Servidor o Workstation es tan seguro como hacer un login en un PC conectado a una LAN (teóricamente). La autentificación de clientes remotos se realiza usando los métodos de autentificación PPP usados para cliente RAS.

Control de acceso

Después del ***auth***, el acceso a la red privada, continúa usando las estructuras de seguridad basadas en NT. El acceso a recursos en NTFS u otros recursos de la red, requieren los permisos correctos, tal como si estuvieses conectado dentro de la LAN.

FUNCIONES

Encapsulación

Las tramas PPP se empaquetan con un encabezado de Encapsulación de enrutamiento genérico (GRE, *Generic Routing Encapsulation*) y un encabezado IP. El encabezado IP contiene direcciones IP de origen y destino que corresponden al cliente VPN y al servidor VPN.

La siguiente ilustración **Figura 3.10.** Muestra la encapsulación PPTP para una trama PPP.

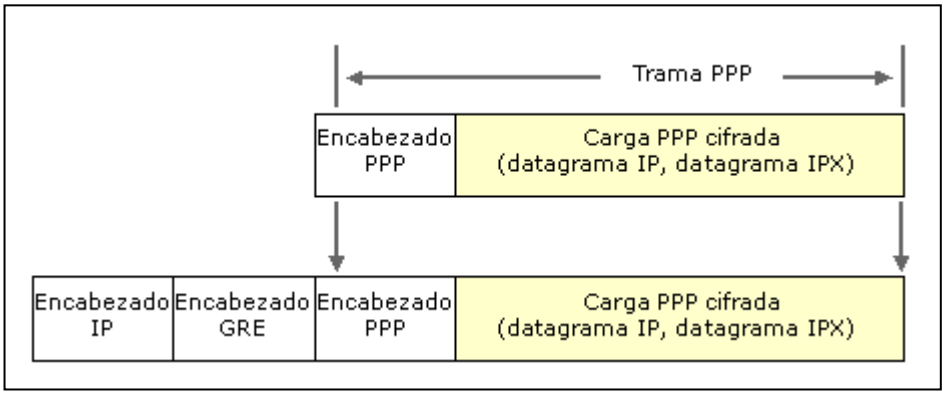


Figura 3.10. Encapsulación PPTP

Proceso de autenticación para este escenario

Los componentes de red determinan el proceso de autenticación. Con la instalación y configuración, la autenticación se realiza de la siguiente forma:

Al iniciar el servidor PPTP, se envía un paquete de cuenta activada.

La conexión de un usuario, tiene el siguiente proceso. Ver Figura 3.11, que registra todas las solicitudes y respuestas:

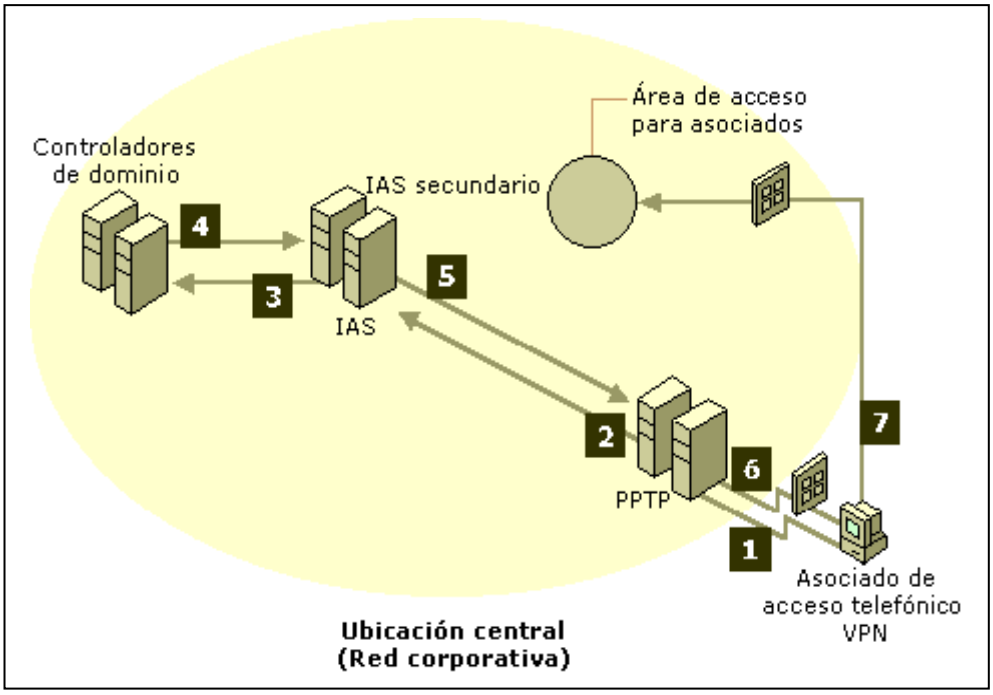


Figura 3.11. Registro de Solicitudes y Respuestas

1) Con acceso mediante tarjeta inteligente, el usuario se enlaza con el servidor PPTP corporativo.

2) El servidor PPTP envía la solicitud de autenticación RADIUS al servidor “IAS”[41].

3) El IAS reenvía la solicitud de autenticación al controlador de dominio, donde se comprueban las credenciales del usuario.

4) El IAS evalúa las directivas de acceso remoto y los atributos para determinar si se permite el acceso telefónico.

5) Si cumple la directiva de acceso remoto y el perfil no rechaza al usuario, el IAS enviará un paquete de aceptación de acceso.

6) Se concede acceso VPN al usuario, según la configuración de conexión especificada en el paquete de aceptación de acceso. La configuración de la conexión contiene un filtro adecuado para el acceso permitido, y PPTP aplica dicho filtro a los paquetes de la conexión.

7) A continuación, el servidor PPTP asigna una dirección IP y otros parámetros al cliente y comienza a enrutar los paquetes enviados al cliente y recibidos del cliente.

[41] Servicio de Interconexión Abierto

3. 3. 6. PROTOCOLO DE SEGURIDAD IP (IPSEC)

IPSec es un grupo de extensiones del protocolo IP. IPSec provee servicios criptográficos de seguridad. Lo que permiten la autenticación, integridad, control de acceso, y confidencialidad. IPSec provee servicios a nivel de red, de un modo que es completamente transparente para sus aplicaciones. Es transparente porque sus aplicaciones no necesitan ningún conocimiento de IPSec para usarlo. Puede usar protocolos IP sobre IPSec, crea túneles cifrados (VPNs), o cifrado entre computadoras (ordenadores).

IPSec funciona en cualquiera de estos tres modos:

- Huésped-a-Huésped
- Huésped-a-Red
- Red-a-Red

IPSec es usado para el tráfico de «Redes Privadas Virtuales». Su utilidad va más allá, con un registro central de «Intercambio de Claves de Internet» (IKE, *Internet Key Exchange*), cada máquina en Internet se comunica con otra y usa un cifrado y autenticación fuerte.

El protocolo de seguridad de IP (IPSec), es una tecnología que protege los paquetes IP en la capa de red, forma una capa segura entre nodos de red.

El protocolo no determina cómo autentificar los pares ni cómo se intercambian las claves de sesión. Para cifrar los paquetes, incluyendo los paquetes sin conexión y paquetes de control IP, IPSec es una buena elección.

CARACTERÍSTICAS DE IPSEC

Son las siguientes: Ver **Figura 3.12.**

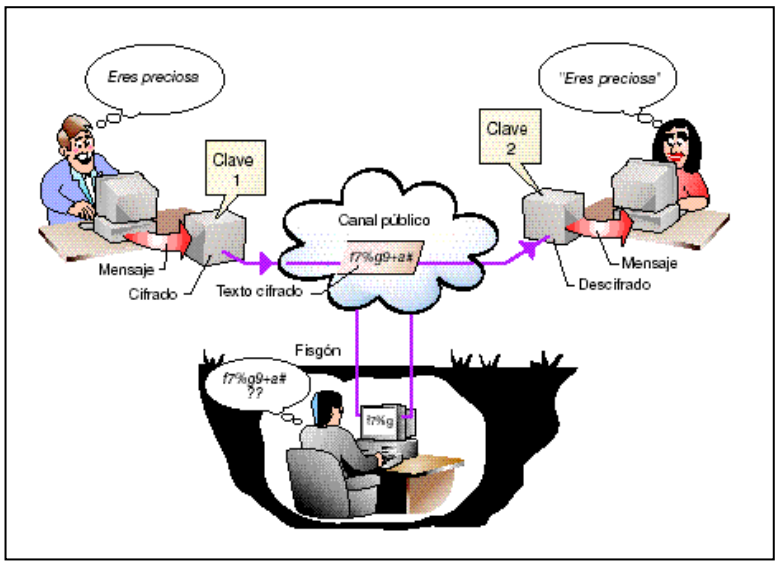


Figura 3.12. Protección de transferencia de datos.

Confidencialidad

Es importante asegurar que datos y contraseña enviados, son invisibles para todos, excepto para el receptor.

Integridad

Garantiza que los datos no sean alterados durante la transmisión de información entre PCs.

Autenticidad

Adjunta un identificador a los datos, de modo que los receptores puedan verificar la autenticidad de los datos, como de su emisor.

Protección a la réplica

Brinda la seguridad que una transacción se ejecutará una vez, a menos que autorice un reenvío. Nadie debería poder grabar una transacción, y luego replicarla al pie de la letra.

CONTROL DE PAQUETES IPSEC

El controlador IPSec recibe la lista de filtros IP activos, del Agente de directivas IPSec, y comprueba la coincidencia de los paquetes de entrada y salida con los filtros de esta lista, Ver **Figura 3.13**. Cuando un paquete coincide con un filtro, aplica la acción de filtrado.

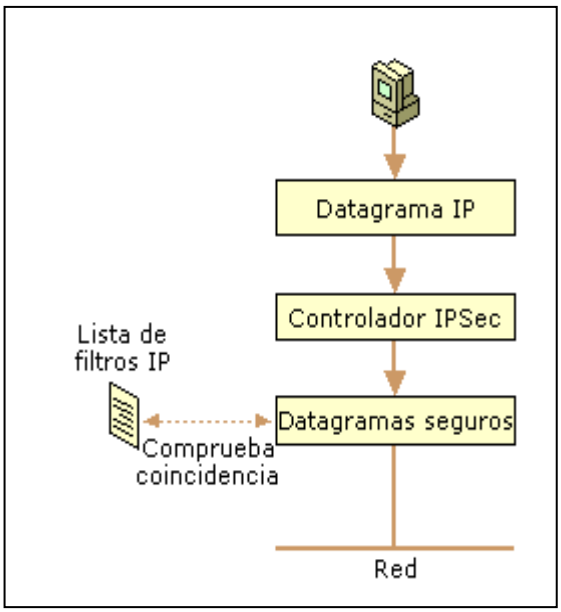


Figura 3.13. Comprobación de paquetes.

Si la acción de filtrado permite la transmisión, se recibe o envía el paquete sin modificaciones. Si la acción bloquea la transmisión, se descarta el paquete. El proceso de salida y entrada utiliza la "SA"[42] y claves negociadas. El controlador IPSec almacena las SA actuales en una base de datos interna. Si hay múltiples SA, el controlador utiliza el Índice de parámetros de seguridad (SPI) para la correspondencia de la SA correcta con el paquete correcto.

Cuando un paquete IP de salida coincide con una acción de la lista de filtros IP para negociar la seguridad, el controlador IPSec pone en cola el paquete, luego, notifica a Intercambio de claves de Internet (IKE, Internet Key Exchange), que comienza la negociación de seguridad con

[42] Asociación de Seguridad

la dirección IP destino de ese paquete. Si varios paquetes de salida con el similar destino coinciden con el mismo filtro antes que IKE haya finalizado la negociación, se guardará el último paquete enviado.

Finalizada correctamente la negociación, IKE proporciona al controlador IPSec parámetros para la asociación de seguridad, incluidas las claves de sesión. El controlador IPSec asegura el paquete IP de salida en cola y lo envía a la tarjeta de red para su transmisión. Si la negociación es negativa, el controlador IPSec descarta el paquete.

Si un paquete de entrada asegurado con IPSec coincide con la lista de filtros IP, el controlador IPSec comprueba la integridad del paquete, descifra el paquete si es necesario y lo convierte en formato IP normal. El controlador IPSec comprueba la coincidencia del paquete IP con el filtro para asegurarse que no ha recibido tráfico distinto durante la negociación. Si el paquete coincide con el filtro, el controlador IPSec envía de nuevo a TCP/IP para la entrega a la aplicación.

COMUNICACIONES REMOTAS: IPSEC

Al combinar el Protocolo de túnel de nivel 2 (L2TP) e IPSec se crea una comunicación remota segura. L2TP se utiliza como vía de transporte, en el cual viaja la información, que IPSec asegura.

Clientes itinerantes

Un requisito es asegurar las comunicaciones entre los clientes remotos y la red de la empresa.

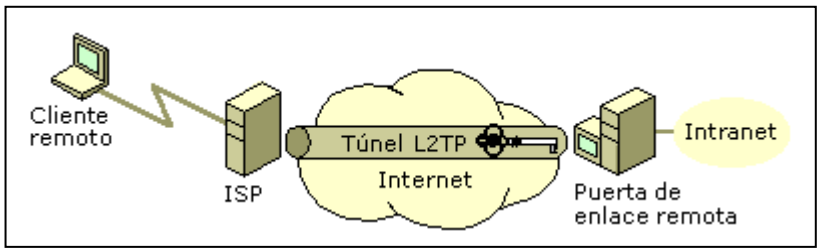


Figura 3.14. Aseguramiento de comunicaciones

La puerta de enlace remota es un servidor que proporciona seguridad para la Intranet de la empresa. Ver Figura 3.14 El cliente remoto representa un usuario itinerante que necesita obtener acceso regularmente a los recursos de la red y la información. L2TP combinado con IPSec proporcionan un modo simple y eficaz para construir el túnel y proteger la información por Internet. El túnel se establece entre el cliente remoto y la puerta de enlace remota, que se utiliza para proteger la comunicación por Internet.

Sucursales

L2TP se combina con IPSec para proporcionar el túnel y proteger la información entre distintas terminales. Ver **Figura 3.15.**

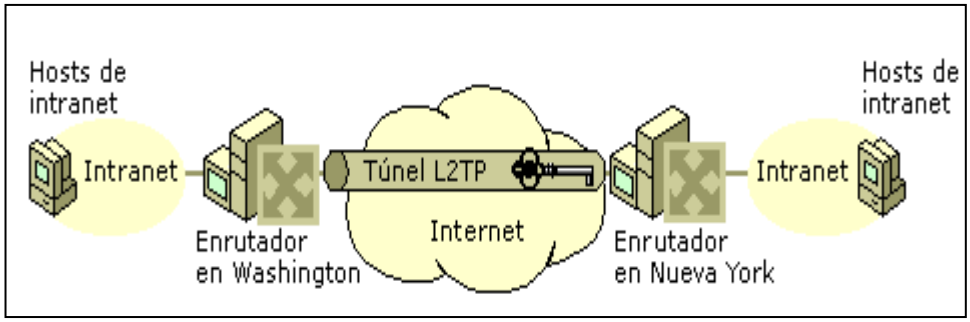


Figura 3.15. Protección de Información entre diversos

En la ilustración, los enrutadores proporcionan seguridad y una ruta de comunicación entre los dos sitios. Es posible que los enrutadores presenten una línea de alquiler, marcado a petición u otro tipo de conexión. El túnel funciona entre las rutas, ya que es utilizado para proteger la comunicación por Internet. La red privada virtual (VPN) se extiende entre los equipos de Intranet de los sitios que intercambian información.

Asegurar una comunicación remota

Los escenarios de comunicación remota requieren la configuración de las propiedades de seguridad L2TP. Cuando se configura L2TP para utilizar IPSec como seguridad:

- El filtro IP y las listas de acción de filtros requeridos se establecen dinámicamente en Agente de directivas IPSec durante la duración de la conexión.

- La autenticación se determina mediante L2TP, que requiere un certificado de clave pública y la clave privada asociada.

- La configuración predeterminada de intercambio de claves está vigente.

- El nivel de seguridad de Protocolo de Internet utilizado durante la duración de la conexión depende de la configuración de seguridad de L2TP:

3. 3. 7. PROTOCOLO CHAP

El protocolo de autenticación Challenge Handshake (***CHAP – Challenge Handshake Authentication Protocol***), se usa para verificar periódicamente la identidad del otro extremo de la conexión. CHAP no previene el acceso desautorizado. La verificación se produce inmediatamente después de la fase de establecimiento de conexión, y puede repetirse en cualquier momento, con el enlace ya establecido.

El procedimiento que utiliza el CHAP es el siguiente:

1) El extremo verifica la identidad de su par, enviando un mensaje de prueba.

2) El par responde con un valor calculado mediante un algoritmo.

3) El autenticador compara la respuesta de su par con su propio cálculo del valor correcto. Si los valores coinciden, el autenticador envía un mensaje, indicando su conformidad. Si no se ha recibido el valor correcto, la conexión debe cerrarse.

4) A intervalos aleatorios, el autenticador envía un nuevo mensaje a su par, y se repiten los pasos 1 y 3.

En la Figura 3.16. se describe el funcionamiento de CHAP.

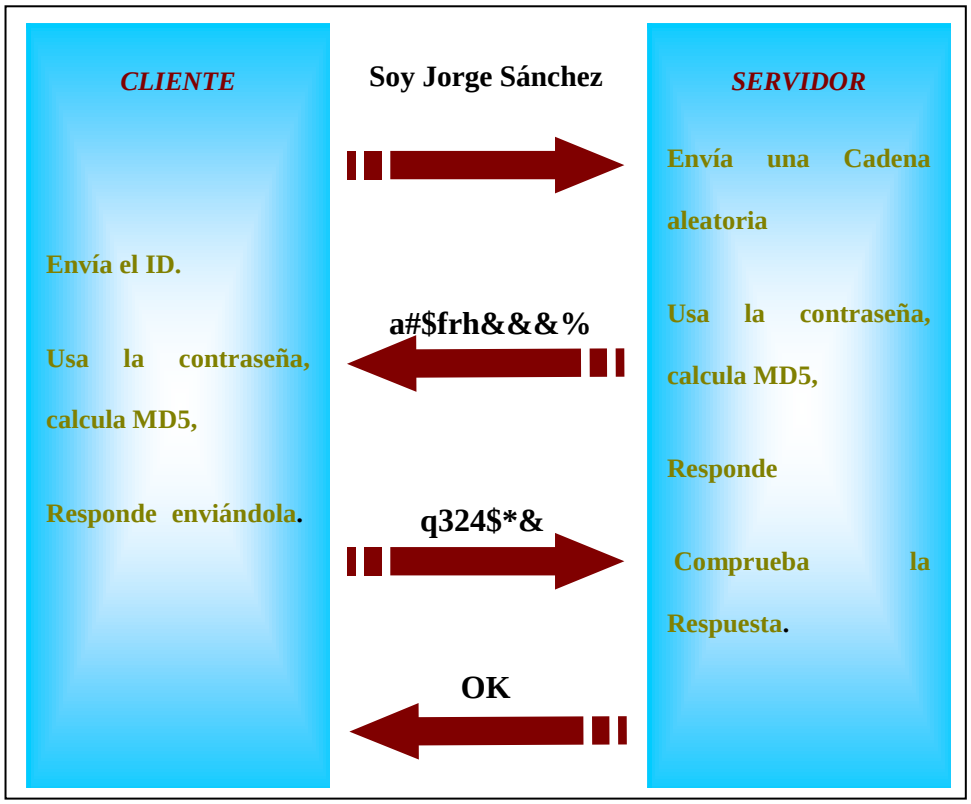


Figura 3.16. Challenge Handshake de PPP.

Ventajas de CHAP

- CHAP provee protección contra la repetición de intentos mediante un identificador, que es incrementado en cada mensaje y un valor variable para la prueba. El tiempo que transcurre entre una autenticación y otra es el límite para un intento de violar la protección. El autenticador decide la frecuencia de mensajes de prueba.

- Este método de autenticación depende del autenticador y el par, este secreto no es enviado por el enlace. El protocolo CHAP funciona en un solo sentido.

Desventajas de CHAP

CHAP requiere que el *secreto* no esté encriptado. Cuando se desee autenticar todas las conexiones que se producen en grandes instalaciones, cada *secreto* debe estar presente en todos los extremos. Es recomendable que los mensajes de prueba y sus respuestas sean examinadas en un servidor central. Si no, los *secretos* deben enviarse a cada posible extremo mediante alguna forma de encriptación.

3. 3. 8. PROTOCOLO PAP

PAP (Password Authentication Protocol) el protocolo simple de autenticación de contraseña, que permite PPP para la autenticación de

un usuario. El equipo remoto que intenta conectarse al servidor de un ISP requiere enviar una petición de autenticación. Al contrario CHAP, PAP pasa las contraseñas encriptadas. PAP no previene el acceso desautorizado, pero meramente identifica el extremo remoto. El servidor de acceso determina entonces si a ese usuario se le permite el acceso o no.

Se envía una trama con el texto del identificador del usuario y su contraseña durante el establecimiento del enlace.

En caso que el servidor de acceso requiera PAP como protocolo para realizar la autentificación de una conexión, durante el establecimiento de sesión LCP de PPP se negociará dicho protocolo, es decir, establecida la conexión, realiza el envió del nombre de usuario y clave. PAP es un protocolo poco seguro, que envía la clave sin cifrar, libre, que puede ser leída por alguien que analice la línea de transmisión.

3. 4. NOTA

El proceso de conexión entre el cliente Dial-up y el Proveedor de Servicios de Internet, que va desde la petición de conexión hasta la asignación de un IP al cliente, se vera reflejado en el momento que se incremente el valor a cancelar por los servicios de conexión.

La tarifación de conexión se lleva a cabo desde el momento en el que el ISP asigna la dirección IP dinámicamente.

Durante este proceso los protocolos que intervienen en la tarifación se encapsulan e intercambian tramas y mensajes con el servidor del ISP, en este intercambio de información se establecen permisos, autorizaciones, puerto, protocolos, configuración de enlaces, configuración de protocolos, etc.

Este proceso se explica con detalle en la **Figura 3.4**

CAP. IV

FUNCIONES GENERALES DE UN RAS

DEFINICIONES

HERRAMIENTAS Y OPERABILIDAD

4. DEFINICIONES

4. 1. INTRODUCCIÓN

El adquirir un RAS, implica automáticamente acceso a varias herramientas ***Software***, que permiten administrar, el funcionamiento, rendimiento y efectividad de su RAS.

El Software que tendrá que manipular es:

ComOS

Es el sistema operativo, Software de comunicación que se carga en la llamada al RAS. Se puede usar las órdenes del ComOS para configurar el RAS desde una consola.

PMVision

Interfaz grafica del usuario (GUI) el ingreso de comandos, para la configuración, supervisión que ponen a punto un RAS.

Pmd o in.pmd

Software opcional que se instala en ordenadores LINUX, permite conectar impresoras y módems al RAS.

RADIUS

El servidor RADIUS, se ejecuta en sistemas LINUX mientras proporciona la administración centralizada de usuarios que marcan la entrada.

ChoiceNet

Tecnología de seguridad, proporciona flexibilidad en el acceso proporcionado a los usuarios.

4. 2. HERRAMIENTAS Y OPERABILIDAD

4. 2. 1. GESTIÓN DE AUTENTIFICACIÓN DE USUARIOS

AUTENTIFICACIÓN DE LOS USUARIOS AL INICIAR CONEXIÓN INTERNA

Un RAS se lo puede configurar para realizar tres tipos de autentificación de usuarios, que tienen conexiones internas, según las decisiones de los administradores, los tres tipos de configuraciones son:

- PAP
- CHAP
- LOGIN

Los usuarios de conexiones internas se autentifican con PAP cuando PPP es detectado. Si los usuarios son rechazados se autentificaran con CHAP.

Al fijar PAP en fuera de servicio o apagado y CHAP en estado encendido. Las conexiones internas se autentifican, mediante el uso de un identificador (username/password).

Para establecer una autentificación PAP se ejecutara la siguiente instrucción:

Comando> **set pap on|off**.

Para establecer una autentificación CHAP se ejecutara la instrucción:

Comando> **set chap on|off**

AUTENTIFICACIÓN AL INICIAR LA LLAMADA POR CLAVE

Se puede habilitar los servicios sin autentificar al usuario en la entrada del RAS, el comando show global permite determinar si la llamada por chequeo esta habilitada en el RAS.

Para habilitar el chequeo de una llamada en ComOS, se debe configurar las entradas del usuario en el servidor RADIUS.

Para habilitar la comprobación de una llamada en RADIUS se usa el siguiente comando:

Comando> set call-check on|off

La configuración de una llamada esta inhabilitada por defecto, si la característica de chequeo de llamada esta habilitada, RAS envía un mensaje resonante al interruptor mientras la información de servicio se busca en el RADIUS.

RADIUS procede con el siguiente mecanismo:

- Rechaza el mensaje con un signo de ocupado.

- Reconoce la llamada y permite completarla.

Permite la creación de un canal TCP, esta conexión usa el perfil de usuario de RADIUS.

La llamada por chequeo hablita al RAS mediante RADIUS, para verificar el número de teléfono antes de contestar la llamada, alternativamente el RAS puede rechazar las llamadas para descongestionar el número dado.

4. 2. 2. GESTIÓN DE CONFIGURACIONES

EL NOMBRE DEL SISTEMA RAS

El nombre tendrá que ser válido para su red. El nombre del sistema puede tener hasta 16 caracteres, sugerencia para productos de un

PortMaster. Para establecer el nombre del sistema, se usa la siguiente orden:

Comando>nombre del sistema (cadena)

LA CONTRASEÑA ADMINISTRATIVA RAS

El RAS (PortMaster) que se instala por primera vez se adquiere sin una contraseña. Al presionar enter se visualizar la sugerencia de contraseña de acceso al RAS. La contraseña es un ASCII de longitud máxima de 16 caracteres, que será utilizada para la administración.

Para poner la contraseña, use el orden siguiente:

Comando> la contraseña

Antes de que el PortMaster pueda ser configurado o conectado al área de banda ancha, es prioritario instalar el hardware que usa el sistema.

Los parámetros que un administrador, deberá tener en cuenta para la configuración del RAS(PortMaster) son:

¿Qué configuración quiere llevar a cabo?

¿Usted quiere configurar una conexión síncrona a una línea de gran velocidad?

¿Sus líneas de gran velocidad usarán el Frame Relay, ISDN, Switched 56 Kbps, o PPP?

¿Si usted quiere la asignación de ruta de la frecuencia de salida en demanda, usted quiere carga-equilibrio de la multilínea?

¿Usted quiere Multienlace PPP (RFC 1717 *Requerimientos para los comentarios*)?

¿Usted quiere filtrar paquetes en las conexiones de Internet?

¿Usted quiere filtrar paquetes en las oficinas?

¿Si usted usa PPP, O NECESITA PAP o autenticación CHAP?

¿Usted ha obtenido las direcciones de la red necesarias?

¿Usted está ejecutando IP, IPX, o ambos?

¿Usted quiere habilitar SNMP por el red supervisar?

¿Cómo usted quiere configurar usuarios dial-up?

¿Usted quiere usar ChoiceNet para filtrar el tráfico de la red?

PAUTAS DE LA CONFIGURACIÓN

La configuración de RAS puede estar dirigida a diferentes fases o etapas porque puede configurar las escenas para un puerto, un usuario, o una situación remota.

PASOS DE LA CONFIGURACIÓN BÁSICOS

La configuración del RAS (PortMaster) no depende del hardware, ni la red. Los pasos generales para la configuración en general son:

1) Instalar el hardware del RAS (PortMaster) y asigne una dirección IP y una contraseña.

2) Iniciar el sistema e ingresar la contraseña del administrador.

   Puede configurar el RAS (PortMaster) por una sesión de Telnet administrativa, o por una conexión de red.

3) Al usar el software PMVision (Software de configuración de equipos Livingstong) para configurar un RAS (PortMaster), instalar el software en un puesto de trabajo en red.

4) Configure las propiedades de Ethernet, IP e IPX para su red.

5) Configurar RAS (PortMaster(asíncrono)).

6) Configurar RAS(PortMaster(síncrono)), si disponible.

7) Configure “ISDN” [43], “BRI” [44], ISDN o conexiones “PRI” [45].

8) Configurar la línea-entrada y la línea-salida a los usuarios de escritorio.

9) Configurar ChoiceNet, si está usándolo.

10) Configurar la frecuencia de salida.

11) Configurar los filtros en la mesa del filtro.

4. 2. 3. GESTIÓN DE RENDIMIENTO

La gestión de rendimiento en un RAS se refleja en la configuración propia del mismo, el RAS permite establecer un tipo de algoritmo, capas de establecer y resolver problemas, que puedan suscitarse en el momento de atender una solicitud de conexión.

Este algoritmo permite resolver conflictos de atención, por ejemplo, resolver un cuello de botella.

Cuando el Backboon de la central de comunicaciones recibe más de una solicitud de conexión el algoritmo decide como y cuando atender a

[43] Servicios integrados de Red Digital
[44] Interfase de programación básica
[45] Interfase de programación primaria

cada una de estas peticiones, de forma que el tiempo de espera sea casi imperceptible.

4. 2. 4. GESTIÓN DE ESTADÍSTICAS

El sistema de estadísticas de un RAS depende de las necesidades administrativas del administrador, la gestión de estadísticas se realiza ya sea por, puerto, conexión o peticiones que atiende la central de comunicaciones.

El RAS permite examinar flujos de datos a través de los puertos del Backboon.

Para visualizar estadísticas el administrador puede elegir mirar en forma grafica o en forma de texto en el archivo que desee.

4. 2. 5. GESTIÓN DE SEGURIDADES

Una buena seguridad, se gestiona al establecer filtros, se puede determinar la entrada y rendimiento a través de un filtro, para cada dirección, los filtros se definen en la consola de administración de filtros, antes de agregarse a la consola de direcciones.

Si un filtro se altera o modifica, deben restablecerse los puertos, que están en uso de la dirección especificada, para que los cambios se ejecuten.

Si el filtro no se encuentra en la consola, el filtro no se establece y se permite el tráfico por completo.

APRECIACIÓN GLOBAL DE LA FILTRACIÓN

La filtración de paquetes puede aumentar la seguridad y disminuir el tráfico en la red, se usan filtros para impedir o negar el transporte de algunos paquetes a través de la red. Con filtros apropiados se puede negar el acceso a los servidores específicos, redes y servicios de red.

La seguridad en una conexión puede reforzarse limitando las actividades autorizadas a ciertos organizadores. Los filtros permiten un máximo de 255 reglas de filtración, esto depende del RAS a instalarse, el RAS genera un tipo de error cuando las reglas exceden el límite.

Si un paquete es rechazado por un filtro, un mensaje se envía a la dirección de la fuente, este muestra la regeneración inmediata al usuario que intenta el acceso desautorizado.

OPCIONES DE UN FILTRO

La siguiente tabla detalla las diferentes opciones:

OPCIÓN	DESCRIPCIÓN
Restricting packet traffic	*Trafico de paquete restringido.* Puede asignarse a cada usuario, un filtro de entrada y un filtro de salida.
Restricting access based on source and destination address	*Restricción de acceso basado en la fuente RAS y dirección del destino USUARIO.* Usted puede crear filtros que evalúen la dirección tanto de la fuente como del destino, con una lista de reglas. Él número de bits significativos usados en una dirección IP, se pueden comparar permitiendo la filtración del Ordenar o un grupo de ordenadores cuyas direcciones estén dentro de un límite.
Restricting access to particular protocols.	*El acceso restringido a los protocolos particulares.* Pueden permitirse paquetes de ciertos protocolos o pueden negarse por un filtro, incluso IPX, SAP, TCP, UDP, y paquetes

	de ICMP.
Restricting access to network services.	*El acceso restringido a servicio de red.* Usted puede crear filtros que usen la fuente y números de puerto de destino para controlar el acceso a ciertos servicios de la red. La evaluación puede ser basada respecto al número del puerto que es menor de, igual a, o mayor que un valor especificado. .
Restricting access based on TCP status.	*Acceso restringido basado en el estado TCP.* Usted puede crear filtros que usen el estado de las conexiones TCP como la parte del conjunto de reglas. Este rango puede permitirles a los usuarios de la red abrir las conexiones a las redes externas sin permitir a los usuarios externos acceder a la red local.

Tabla 4.1 Opciones de un Filtro

FILTROS DE ENTRADA

Los filtros de entrada tienen por objetivo, evaluar los paquetes recibidos de la conexión, permitiendo la aceptación de paquetes establecidos en los filtros.

Para establecer el filtro de entrada que valide una conexión se ejecutara el siguiente comando:

Comando> **set location** [nombre_local]**ifilter** [nombre-filtro]

FILTROS DE SALIDA

Los filtros de salida permiten evaluar los paquetes emitidos por una conexión, a través de validar las reglas establecidas en el filtro de salida. Esto permitirá establecer los paquetes que se entregaran a dicha conexión.

Para establecer un filtro de salida a una conexión ejecute la siguiente orden.

Comando> **set location** [nombre_local] **ofilter** [nombre-filtro]

4. 2. 6. GESTIÓN DE VELOCIDADES

LA VELOCIDAD DE LA LÍNEA

El circuito físico entre el punto A y la red, debe tener cierta velocidad en la línea, esta velocidad es el máximo ancho de línea física para su conexión de red. La expansión más allá de este límite, no es posible sin un cambio de Hardware y una nueva instalación del circuito.

LA VELOCIDAD DEL PUERTO

La conexión a la red del proveedor de telecomunicaciones debe establecerse a una velocidad particular que es el máximo que brinden las telecomunicaciones.

Esta velocidad es la máxima a la cual usted puede transmitir paquetes. La velocidad del puerto solo difiere de la velocidad de línea en que esta puede actualizarse a través de software sin una instalación del circuito o cambio de hardware.

VELOCIDAD DE INFORMACIÓN ENTREGADA (CRI) Y VELOCIDAD DEL ESTALLIDO

Cada "PVC"[46] tiene una propiedad que representa el ancho de banda mínima garantizada.

Esta velocidad representa la proporción con lo cual los datos pueden fluir por encima de un PVC, sin tener en cuenta la disponibilidad de banda máxima.

4. 2. 7. GESTIÓN DE PARIDADES

Los puertos pueden configurarse para varias funciones diferentes, dando mayor flexibilidad a la configuración del RAS. Cada puerto puede llevar a cabo una función en un momento. El puerto esta entonces disponible para un corte de conexión o petición de desconexión.

PUERTOS ASÍNCRONOS

Algunos usos para los puertos asíncronos se detallan a continuación:

Las conexiones entre oficinas, pueden lograrse a través de una conexión asíncrona dependiendo de su aplicación.

Para agregar banda ancha a la red, puede configurarse los puertos adicionales para equilibrar la carga. Estos puertos pueden configurarse

[46] Circuito Virtual Permanente

cuando el tráfico de red excede un nivel específico. Esta configuración permite conectar los puertos múltiples durante el tiempo, en el cual el tráfico de la red se vuelve pesado.

Se puede configurar un puerto asíncrono para realizar conexiones continuas a un ISP, de forma que tenga conexión hacia fuera. En la cual si la línea de conexión exterior se deja caer, el RAS restablece la conexión automáticamente.

Deben configurarse ciertas escenas para cada puerto asíncrono, sin tener en cuenta el tipo del puerto y configuración seleccionada por el administrador.

Si configura el puerto como un dispositivo miembro del servidor, el administrador puede especificar que dispositivo del servidor puede atropellar o violentar ciertas escenas del puerto. Característica que permite al servidor alterar los parámetros activos a través del software de mando, usando el sistema operativo. Las escenas que el servidor puede pasar por alto son velocidad, paridad, y mando de flujo.

ESTABLECIENDO LA PARIDAD

Al establecer la paridad debe configurarse de manera que se empareje la paridad en el MODEM enlazado.

El valor predefinido de paridad, debe usarse en puertos configurados para la conexión de entrada. La tabla muestra las opciones de paridad.

Opción	Descripción
Ninguna	Asume 8 bits de datos, un bit de parada y un bit de paridad.
Constante	Asume 7 bits de datos, un bit de parada y uno constante para la paridad.
Impar	Asume 7 bits de datos, un bit de parada y un impar de paridad
Quitar	Asume 8 bits de datos y un bit de parada. El bit de paridad desaparece cuando es receptado por el RAS

Tabla 4.2 Opciones de Paridad

Para establecer la paridad en un MODEM o puerto, use el comando:

Comando> El SO paridad even | none | odd | strip

4. 2. 8. GESTIÓN DE DIRECCIONAMIENTO DINÁMICO (DHCP)

Los "DHCP"[47] denominados servidores de apoyo fijo. Utiliza una base de datos para la pista de direcciones IP que ha asignado el servidor.

DHCP utiliza con frecuencia el Registro para el almacenamiento de definiciones de ámbito y las reservas.

DHCP almacena el ámbito y la información para la configuración en la clave del registro, DHCP mantiene varios archivos que se relacionan con la base de datos de cada servicio.

[47] Protocolo de configuración dinámica de ordenadores

CAP. V

ESTUDIO DE PLATAFORMAS

DEFINICIONES

CARACTERÍSTICAS

VENTAJAS / DESVENTAJAS

5. DEFINICIONES

5. 1. INTRODUCCIÓN

El Sistema Operativo o conjunto de programas que permiten administrar los recursos de hardware y software de un computador.

CM/P (Control de Programa para Microcomputadores), desarrollado por Gary Kildall fue el primer Sistema Operativo que podía ejecutarse en PCs de diferentes fabricantes.

A finales de 1997 nadie tenía en mente otro sistema operativo que no fuera de la plataforma Windows. La plataforma LINUX estaba relegada a equipos de laboratorio, y los equipos montados en Internet eran más una promesa que una realidad.

Hoy en día existe un gran número de Plataformas tanto de software como de hardware, en este capitulo analizaremos las Plataformas Windows y Linux, que son las más usuales en el mundo informático.

5. 1. 1. CLASIFICACIÓN DE SISTEMAS OPERATIVOS

LINUX

Cuando Linux Torvalds comenzó a trabajar sobre Minix para obtener su propio sistema operativo no tenía ni la más remota idea de lo que su

trabajo llegaría a ser en todo el mundo. Este sistema operativo es totalmente distinto a los vistos anteriormente por un montón de razones. He aquí algunas de ellas:

No fue desarrollado por una gran empresa

Linux Torvalds desarrolló el kernel (el corazón) del sistema y luego liberó el código fuente del mismo en Internet para que cualquier programador que se animara pudiera modificarlo y agregarle lo que quisiera. Así, el Linux que hoy se conoce fue creado por cientos de programadores ***libres***, alrededor del mundo y no por una empresa.

Es gratis y abierto

Todo el sistema operativo es totalmente gratuito, si posee una conexión a Internet es posible descargarlo a su máquina. Lo que algunas empresas hacen es ***empacar***, el sistema y grabarlos en CD's, que junto con algún manual es lo que ***venden***.

Junto con el sistema vienen los códigos fuentes del mismo para que pueda ser modificado a gusto del usuario, es por esto que se dice que es ***abierto***.

Nació a partir de otro sistema operativo

Es una modificación del sistema Minix, que a su vez nació como una ***reducción*** de UNIX, un ***sistema operativo verdadero***, a partir del cual se crearon los demás.

Este sistema operativo es el elegido por las empresas que proveen acceso a Internet, debido a su gran estabilidad y eficiencia, aparte de ser gratuito. Además, posee un muy buen manejo de redes y seguridad, lo que está haciendo que muchas empresas e instituciones lo tengan en cuenta para reemplazar sus sistemas actuales.

En un principio, Linux también era una pantalla negra en modo texto y muy poco intuitivo. Pero desde hace un tiempo se desarrollaron entornos gráficos (varios: KDE, Gnome, etc.) que no tienen nada que envidiarle a las plataformas Windows que atraen a más usuarios.

Por lo anterior y el gran auge de Internet este es el sistema operativo que más crecimiento ha tenido en los últimos años, y el que se perfila quizá como el sistema operativo del futuro.

WINDOWS

Windows: Una Máscara

Las dos primeras versiones de este ***Entorno Operativo***, no tuvieron mucho éxito entre el público.

El despegue de Windows se produjo con su versión 3.0 cuando comenzó a aprovechar las capacidades de los procesadores ***386***, y le dio un mejor manejo a la memoria.

Fue simplemente un ***shell***, para DOS, ya que sin este no funcionaba. Y por esa razón no es un sistema operativo, sino un ***entorno operativo***.

Un tiempo más tarde se le agregaron capacidades para trabajar con redes y pasó a la versión 3.11. Esta fue la última versión comercial que salió al mercado antes de que Windows 95 hiciera su aparición.

Windows 95: Mitad Verdad, Mitad Mentira

Windows 95 un sistema operativo de 32 bits, porque no necesitaba de ningún otro programa para poder funcionar. Muchas de las ***partes***, de este sistema operativo fueron de 16 bits como sus antecesores. Esto se explicó diciendo que era así por la cantidad de programas ***heredados***, de las versiones anteriores (Windows 3.1).

Windows 98: Casi un Cambio

Windows 98 no representó ningún cambio significativo. Sólo un poco de ***maquillaje***, gráfico y alguna que otra utilidad nueva o mejorad. Pero si trajo algunas utilidades: el soporte completo para los 32 bits, y la ***eliminación*** del DOS como sistema independiente.

Su gran estabilidad, su soporte para varios procesadores, su alto nivel de seguridad, es rápido y lo suficientemente fácil de configurar casi para cualquier persona.

Windows XP: La Nueva Generación del Escritorio

Este sistema operativo es la mejora mas importante técnicamente que ha realizado Microsoft, contra Windows NT/2000 para usuarios corporativos con requerimientos de trabajo en redes de alto nivel.

Se destaca por su alto grado de integración con las redes e Internet, además de proveer una nueva interfaz gráfica que se hace notar ni bien se comienza a utilizar. La diferencia real con sus predecesores esta dada por el soporte LAN, software de grabación de CDs, multimedia, escritorio remoto y manejo de usuarios.

5. 2. CARACTERÍSTICAS

Todas las plataformas, son diferentes: en interfaz, la forma de acceso a recursos, administración de procesos, soporte de hardware, e incluso una marcada diferencia en costos.

	LINUX			WINDOWS		
CARACTERÍSTICAS	Si	No	De	Si	No	De
Actualizaciones de Núcleo	X				X	
Administración de Procesos	X			X		
Administración Directa	X					
Compartición de Memoria	X			X		
Compatibilidad de Hardware	X			X		
Control						
• Control de Procesos	X			X		
• Control de Tareas	X			X		
Disposición del Código Fuente	X			X		

Escalabilidad						
• Múltiples Placas Base	X			X		
• Soporte de Múltiples Plataformas	X			X		
Estabilidad	X					X
Facilidad de Uso						
• Interfaz de Escritorio Gráfica	X			X		
• Configuración de Dispositivos		X		X		
Idiomas de Instalación	X			X		
Instalación Sencilla	X			X		
Interoperabilidad H/S	X			X		
Memoria Virtual	X			X		

Multiprocesador	X			X		
Multiprocesamiento	X			X		
Multitarea	X			X		
Multitud de Software Disponible						
• Pagado			X	X		
• Gratis	X					X
Multiusuario						
• En Tiempo real	X			X		
• Tiempo Compartido	X				X	
• Multiprogramación	X			X		
Planificador de Procesos	X					X
Procesamiento por Lotes	X			X		

Protección de Memoria	X			X		
Rendimiento						
• Estable	X					X
• Menos Administración		X		X		
• Lectura / Escritura a Disco	X			X		
Seguridad						
• Antivirus	X			X		
• Herramientas	X					X
Servidor de Comunicaciones	X			X		
Sobre El Escritorio						
• Rápidos	X			X		
• Baratos	X				X	

• Estables	X					X
• Seguros	X				X	
Soporte de Librerías						
• Librerías Dinámicas	X			X		
• Librerías Estáticas	X				X	
Soporte de Red	X			X		

Tabla 5.1 Comparación de Plataformas

5. 3. FACILIDADES

5. 3. 1. LINUX

- Soporta un espectro de aplicaciones o paquetes de programación tales como X Windows, Emacs, redes de datos bajo protocolos TCP/IP (incluyendo SLIP, PPP, ISDN).

- Linux está disponible en Internet en cientos de servidores FTP y en distribuidores en discos CD-ROM de revendedores que lo ofrecen

empacado con manuales e información que es realmente la del costo, el software es gratuito. Algunos sitios son: Caldera, Debian, Slackware, Red Hat, etc.

- Linux incluye compiladores, ensambladores, debuggers, editores de texto, paquetes de mail, lectores de noticias, navegadores, servidores y programas para la creación y edición gráfica.

- Linux, maneja archivos de forma jerárquica, de la misma forma que DOS, con la diferencia que DOS está diseñado para procesadores x86 que no soportan capacidades de múltiples tareas.

- Las plataformas que soportan Linux son 386-, 486-. Pentium, Pentium Pro, Pentium II, Pentium III, Pentium 4, AMD, también existen versiones para su utilización en otras plataformas, como Alpha, ARM, MIPS, PowerPC y SPARC.

- Linux, entre los sistemas operativos alternos que existen, es una opción interesante.

5. 3. 2. WINDOWS

- Una mejor interfaz grafica.

- El número de aplicaciones se adaptan con flexibilidad a los Sistemas Windows, que hace posible que usuarios, administradores se familiaricen sin dificultad con el manejo y utilización.

5. 4. VENTAJAS / DESVENTAJAS

Los sistemas Windows y Linux pueden compartir el mismo Computador.

5. 4. 1. LINUX

VENTAJAS

- Los sistemas Linux protegen a sus usuarios y protegerse a sí mismo.

- Muchos administradores de ISPs mantienen el servidor de datos corporativo, donde se requiere una plataforma de alto rendimiento que actúe como servidor de bases de datos, confían en Linux

- Linux es mucho más estable y requiere menos recursos

- La búsqueda para ***Linux***, es mayor a los Sistemas Windows en los buscadores Web. En Google rinde 1,080,000 resultados. Una búsqueda para ***Windows 2000***, rinde 1,050,000.

- Linux es un Sistema Operativo POTENTE, ESTABLE y SEGURO y usted no paga por licencia de uso.

- Los Servidores Linux, brindan servicios de: Paginas Web, Correo Electrónico, INTERNET - Proxy, conferencias, Bases de Datos, además de los servicios de Archivos e Impresoras.

- Tener acceso al código de linux es una ventaja que ofrece al usuario, desarrollador, administrador para solucionar problemas.

DESVENTAJAS

- El problema de Linux son pocos fabricantes de Drivers, situación que esta cambiando. linux soporta una cantidad impresionante de hardware que cubre las necesidades de la mayoría de usuarios.

- Linux no posee mayor cantidad de aplicaciones gráficas que faciliten la administración de Servidores en los ISP.

5. 4. 2. WINDOWS

VENTAJAS

- Windows por ser un estándar esta en la mayoría de computadoras del mundo, por esta razón los desarrolladores de aplicaciones/programas utilizados en ISPs son realizadas para que corra en cualquier sistema Windows

- La versatilidad del Windows es uno de sus mejores puntos, puede hacer gran variedad de actividades en distintas áreas desde entornos gráficos hasta base de datos.

- En el soporte de hardware debemos admitir la eficiencia de Windows. Todos los fabricantes de hardware crean Drivers para Windows.

DESVENTAJAS

- La estabilidad de Windows es su peor punto de análisis.

- En instalaciones grandes, Windows tiene un papel secundario, de servidor de aplicaciones departamentales (servidor de archivos, servidor de aplicaciones, servidor de e-mail, etc.).

- Los sistemas Windows son atacados por su vulnerabilidad. Si el usuario no tiene cuidado y dispone de Internet, se ve amenazado por la falta de seguridad de su sistema operativo.

- Microsoft® monopolizo la venta de Sistemas Operativos eliminando del mercado a sus competidores, esto hace que los usuarios normales o administradores de Proveedores de Servicios de Internet se vean casi con la necesidad de utilizar sistemas Windows.

- Windows no permite saber lo que pasa dentro del sistema operativo, permitiendo intranquilidad enorme ya que se resuelve todo siempre dependiendo de algo o alguien.

Por el análisis expuesto anteriormente hemos tomado la decisión de utilizar la Plataforma Linux como software base para el desarrollo del aplicativo planteado en el Proyecto de Tesis.

CAP. VI

HERRAMIENTAS DE DESARROLLO

CARACTERÍSTICAS

LENGUAJES DE PROGRAMACIÓN VISUAL

BASES DE DATOS EN LINUX

6. HERRAMIENTAS DE DESARROLLO

6. 1. INTRODUCCIÓN

A la gratuidad de Linux, se suma la existencia de Software de desarrollo, los mismos que poseen un bajo costo, fiabilidad, y soporte a bases de datos. Permitiendo desarrollar aplicaciones comerciales a gran escala.

Este entorno, ha permitido obtener un estándar de herramientas de programación para desarrollar aplicaciones utilizadas en ISP.

Analizaremos herramientas de desarrollo, para determinar la conveniencia o no de cada una de ellas. Luego del análisis se determino que PHP, un modulo de Apache es la herramienta mas idónea.

6. 2. CARACTERÍSTICAS

Durante mucho tiempo los usuarios de programas libres encontraron dificultades para desarrollar sus aplicaciones.

Los proyectos KDE y GNOME aportaron sus entornos de desarrollo al estilo Windows. Los entornos desarrollados por KDE, son programas complejos de programación visual, que cuentan con varias herramientas para la concepción de interfaces y generación automática de código. Este orientado al desarrollo de software libre.

Linux tiene una variedad impresionante de herramientas de desarrollo desde la más simple hasta la más evolucionada.

6. 3. LENGUAJES DE PROGRAMACIÓN VISUAL

6. 3. 1. C++ (KDEVELOP)

Una herramienta útil y comprensible para el programador de sistemas, bajo LINUX en un entorno grafico es C++(KDEVELOP), las principales características son:

- Estable
- Posee librerías que incluyen controles tales como: botones, cuadros de texto, etc.
- Funciona en entorno de ventanas.
- Es gratuito.

6. 3. 2. DELPHI (KYLIX)

Linux ha revolucionado el ambiente corporativo, su confiabilidad, escalabilidad. La integración de un ambiente de desarrollo líder, un depurador interactivo, un diseñador visual intuitivo y un conjunto de

componentes completo le brinda las herramientas que usted necesita para desarrollar sus aplicaciones rápidamente.

La poca utilización en el diseño de aplicaciones con esta herramienta es consecuencia del costo.

Las versiones gratuitas que se encuentran en el Internet no son compatibles con bases de datos.

Las principales características de este entorno visual son:

- Instalación Sencilla
- Permite el acceso a diferentes Bases de Datos: MySql, Interbase, PostgreSQL, Oracle, Microsoft SQL Server y IBM DB2.
- Posee componentes para de servicio de Internet.
- Soporte a varios tipos de protocolos, tales como: TCP, UDP, FTP, HTTP, ICMP, IMAP, IRC, POP3, SMTP, etc.
- Ambiente de Desarrollo Visual.
- Desarrollo con el Servidor Web Apache.
- Arquitectura de Base de Datos Abierta.

- Aplicaciones Compiladas Nativamente.

- Desarrollo con Librerías de Componentes Multiplataforma.

- Depurador Totalmente Integrado.

- Implementación de Aplicaciones sin Licenciamiento.

6. 3. 3. PHP (KDEVELOP)

Introducción

PHP fue creado por Rasmus Lerdorf a finales de 1994, la primera versión la llamo *Personal Home Page Tools.*

Al principio estaba compuesto por algunos marcos que facilitaban la creación de paginas Web, hacia mediados de 1995 se creo el analizador sintáctico y se llamo PHP/F1 versión 2, que reconocía únicamente el texto HTML y algunas directivas de mSQL. A partir de este momento, la contribución al código fue pública.

El crecimiento de PHP desde entonces ha sido exponencial y han surgido nuevas versiones nuevas como las actuales, PHP3 o PHP4.

Que es PHP

PHP un procesador de Hipertexto, con la diferencia que su código se ejecutara siempre en el servidor Web.

Dispone de múltiples herramientas que permiten el acceso a Bases de Datos, por lo que es ideal para la creación de aplicaciones Web.

PHP es equiparable a un CGI. La capacidad de PHP para soportar accesos a diferentes Bases de Datos.

Su funcionamiento es el siguiente:

- Escribir paginas HTML, con código PHP dentro.
- Se publican en el servidor Web.
- El browser solicita la página al servidor.
- El servidor interpreta el código PHP.
- El servidor envía el resultado del conjunto de código HTML

En ningún caso se envía código PHP al navegador, por lo que las operaciones realizadas son transparentes para el usuario, esto tiene mucha utilidad.

6. 4. BASES DE DATOS EN LINUX

6. 4. 1. MySQL COMO MOTOR DE BASE SE DATOS

"MySQL no es un proyecto Open Source, ya que en ciertas condiciones necesita de una licencia"[48]. No obstante disfruta una gran aceptación.

MySQL tiene gran compatibilidad con la mayoría de herramientas visuales, podemos mencionar por ejemplo: Apache y PHP, Perl, C, C++, etc.

Las principales características de MySQL son:

- Su velocidad
- Facilidad de uso
- Costo
- Capacidad de gestión de lenguajes de consulta
- Capacidad para soportar multiaccesos
- Portabilidad

[48] Edición Especial MySQL, PAUL DUBOIS, Pág. XXIV

- Es un software de respuesta rápida, multi_inserción, multiusuario, con un robusto servidor de base de datos. El servidor de MySQL, se utiliza para sistemas de producción pesados.

- El software de MySQL tiene licencia doble. Se puede usar el servidor de MySQL libre de acusación o delito bajo GNU. se puede comprar el servidor de MySQL comercial autorizado por la MySQL AB.

- Seguridad. Todo el sistema de permisos MySql lo guarda en una Base de Datos llamada MySql, la cual se compone de cinco tablas: **host**, **user, db, tables_priv, colums_priv.**

- Acceso a Usuarios Remotos

- Crea y altera Tablas e Índices

- Los archivos de búsqueda usan el criterio de búsqueda múltiple.

- Genera conexiones locales a bases de datos ubicadas en el servidor de remoto.

CAP. VII

ESTUDIO DE SISTEMAS DE TARIFACIÓN

INTRODUCCIÓN

ESTUDIO DE RADIUS

7. ESTUDIO DE SISTEMAS DE TARIFACIÓN

7. 1. INTRODUCCIÓN

Radius (Remote Authentication Dial-In User Service) es un protocolo de seguridad para accesos remotos. Ha sido propuesto como estándar por el IETF (Internet Engineering Task Force), y sus componentes principales están definidos en las normas: *RFC 2138: Remote Authentication Dial-In User Service (RADIUS)* y *RFC 2139: RADIUS Accounting*.

La arquitectura del protocolo es cliente/servidor. Cuando se produce un intento de acceso de un usuario, el cliente Radius, que reside en los servidores de terminales, intermedia entre el usuario y un servidor Radius, que tiene la potestad de denegar o autorizar los intentos de conexión.

7. 2. ESTUDIO DE RADIUS

7. 2. 1. CARACTERÍSTICAS

Radius (cliente/servidor), se caracteriza por las diferentes funcionalidades que desempeña como Servidor Radius (administrar, crear, etc.) en un Proveedor de Servicios de Internet (ISP).

SEGURIDAD

En las redes grandes, puede dispersarse la información de seguridad a lo largo de la red en los dispositivos diferentes. RADIUS permite guardar la información del usuario en un host, minimizando el riesgo de trucos de seguridad. Toda la autenticación y acceso para servicios de red son manejados por el host que funciona como el servidor Radius.

FLEXIBILIDAD

El software de Radius se obtiene desde el sitio Remoto de Lucent, para la versión 2.0 y superior. Puede usarse con cualquier servidor de comunicaciones que soporte el protocolo Radius con tal de que usted posea un producto de hardware de Acceso Remoto Lucent, mediante la autorización de Livingston Enterprises Software: ftp://ftp.livingston.com/pub/le/LICENSE.

MULTIPLATAFORMA:

El software Radius se suministra para las plataformas más populares: SUN/Solaris, Linux y Microsoft Windows

BASES DE DATOS DE USUARIOS:

La base de datos de usuarios puede consistir en un simple archivo plano que se suministra por defecto, o bien, en una base de datos dbm,

a la que se accede mediante una librería dinámica que también se incorpora por defecto en el servidor Radius.

Así mismo, el cliente puede utilizar bases de datos distintas a las ofrecidas por defecto, mediante el desarrollo de librerías dinámicas para el acceso a dichas bases de datos. El servidor Radius incorpora fuentes necesarias para el desarrollo de dicha librería

CONTABILIDAD:

La información de contabilidad se guarda en un archivo denominado Detail ***detalle***, en un directorio configurable.

MONITORIZACIÓN DEL SERVIDOR:

Se genera un archivo ***logfile***, en el servidor Radius, que contiene un registro de los mensajes de error producidos por el sistema. Por otra parte, existe la posibilidad de depuración de la ejecución mediante los archivos de tramas. Estas pueden tener distinto nivel de detalle, según se especifique en los parámetros de lanzamiento del servidor, o bien posteriormente, mediante la ejecución de un comando desde la línea de comandos.

Existen comandos que permiten ver el estatus actual del servidor, gestionar las direcciones IP conectadas, incluso parar la ejecución del servidor.

ASIGNACIÓN DE DIRECCIONES/ASIGNACIÓN DE CALIDADES DE ACCESO A INTERNET:

En el caso de que el servidor Radius se utilice para servicio InfoVía, las direcciones IP se asignarán a partir de los datos contenidos en un archivo de configuración o se podrán asignar distintas calidades de acceso a Internet a distintos usuarios.

CONFIGURACIÓN DE CLIENTES RADIUS:

Dependiendo del servicio que preste el Servido, existe la posibilidad de configurar el número de clientes Radius. Ejemplo: InfoVía Plus Básico, existe la posibilidad de configurar hasta 256 clientes Radius.

HERRAMIENTA DE DESCONEXIONES:

Por iniciativa del gestor del servidor Radius, se puede desconectar a cualquier usuario en base a su dirección IP.

7. 3. VENTAJAS Y DESVENTAJAS

La singularidad del servidor Radius en un Proveedor de Servicios de Internet se basa en dos factores:

- Su fácil funcionamiento con las Redes IP para la prestación de los servicios InfoVía está garantizado.

- Admite una gran variedad de configuraciones.

A continuación se detallan los aspectos más importantes del estudio:

- La plataforma Windows NT es, con diferencia, la que menos rendimiento ofrece (el PC empleado en las pruebas es el mismo que en el caso de la plataforma Linux).

- Para clientes con pocos usuarios (menos de 1.000) la opción más adecuada (por sencillez, coste y prestaciones) es utilizar Radius con archivo plano de texto en plataformas Linux.

- La utilización de archivo plano como base de datos de usuarios cuando el número de estos es significativo penaliza las prestaciones. El proceso Radius tiene que hacer una búsqueda secuencial del perfil del usuario en el archivo. Cuanto más grande sea el número de usuarios en el archivo, más tiempo tardará en procesar cada petición de autentificación. Cuando el número de usuarios supera cierto valor (por ejemplo a partir de 5.000 usuarios), independientemente de la plataforma y el Hardware empleado, la capacidad máxima del sistema no será suficiente.

- La opción más adecuada para clientes con un número de usuarios superior a 5.000, es emplear la opción de base de datos de usuarios en formato dbm. Esta opción sólo está disponible en las plataformas Unix(Solaris) y Linux..

- En este caso, un aspecto importante a destacar es el tiempo de generación del archivo en formato dbm a partir del archivo plano. Esto es así ya que no sólo hay que generarlo al principio, si no que cada vez que se da de alta/baja un usuario o se modifican los perfiles de un usuario, hay que regenerar el archivo dbm por completo.

- El tiempo de generación aumenta de forma no lineal con el número de usuarios. Éste puede llegar a 6 horas con una base de datos de 1 millón de usuarios (para las plataformas Unix). En el caso de Linux sobre PC los tiempos de generación son apreciablemente mayores.

- Además, mientras se está generando el archivo en formato dbm, se accede continuamente a disco en accesos de escritura. Si esto se produce mientras el sistema está activo (admitiendo usuarios) y el disco que se utiliza para leer los datos de usuarios (archivo dbm antiguo) es el mismo que el que utiliza la herramienta de generación del nuevo archivo dbm, ambos procesos se interfieren y las prestaciones máximas de ambos se ven reducidas (puede llegar a suponer una reducción del 50% de la capacidad máxima del Radius).

- Continuando el último punto, se debería regenerar el nuevo archivo dbm en un disco distinto al empleado por el archivo dbm que se

quiere remplazar y que estará siendo utilizado por el Radius. Hay que tener en cuenta que comandos de sistema operativo como **cp**, *tar* o *ar* para copiar archivos normales no funcionan con archivos en formato dbm. Deben usarse links simbólicos *ln*, o el comando *mv*. Además, habrá que reiniciar Radius para que utilice el nuevo archivo.

- Cabe mencionar que en la actualidad, un cliente con 100.000 usuarios en su base de datos, no recibe más de 3 llamadas/segundo en la hora cargada.

7. 4. SOPORTE

7. 4. 1. FUNCIONES DE RADIUS

Radius realiza tres funciones relacionadas con la seguridad de los accesos remotos, agrupadas bajo el acrónimo inglés *AAA* (*Authentication, Authorization and Accounting*):

Las funciones de Radius se detallan en la **Figura 7.1**

- Autenticación: posibilidad de que los usuarios remotos se identifiquen mediante un identificador y una clave de acceso.

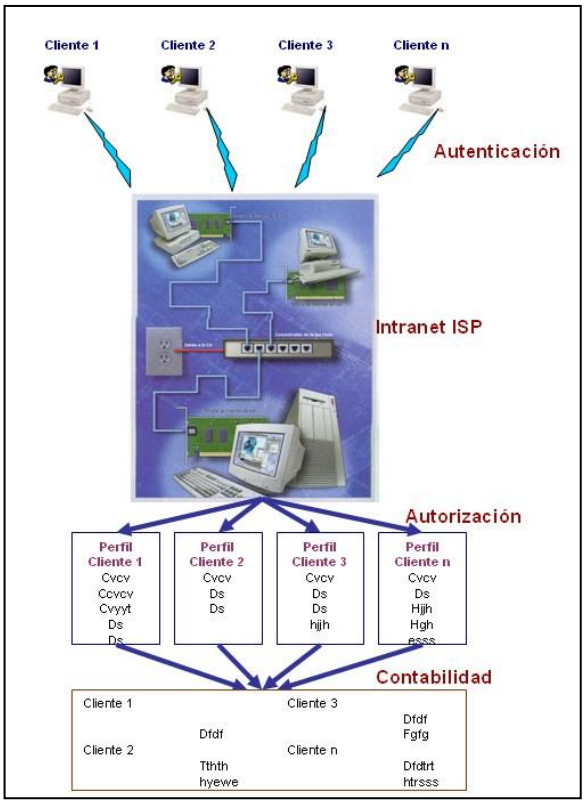


Figura 7.1 Esquema de Funciones de Radius

- Autorización: asignación de parámetros a cada acceso basándose en perfiles de usuario predefinidos y políticas de seguridad.

- Contabilidad (“Accounting”): creación de registros de uso para permitir la auditoria, la medida de prestaciones y la facturación de los accesos remotos.

AUTENTICACIÓN

Durante el proceso de autenticación, se produce el intercambio del identificador del usuario y su clave entre el usuario, el servidor de acceso y el servidor Radius. El identificador y la clave son enviados por el usuario al servidor de acceso durante la negociación de PPP, utilizando los protocolos PAP o CHAP.

El servidor de acceso, en el que reside el cliente Radius, inicia una transacción Radius con el servidor Radius y envía el identificador y la clave del usuario (cifrada con una clave secreta que comparten el cliente y el servidor). El servidor utilizará la clave para verificar la identidad del usuario, y si se comprueba que es quien dice ser, se pasa a la siguiente fase; en caso contrario, se rechaza el intento de conexión.

AUTORIZACIÓN

Después de la autenticación, la siguiente fase en las transacciones AAA es la autorización. Junto con la información de autenticación que el cliente incluye en la solicitud de acceso Radius, también se incluye información sobre el tipo de conexión que el usuario trata de establecer. El servidor Radius emplea estos datos para autorizar el acceso del usuario y emitir un mensaje de respuesta de aceptación, o denegar el acceso y emitir un rechazo.

La autorización está controlada por el perfil del usuario, que reside en una base de datos asociada al servidor Radius. Además de otros datos del usuario, desde el punto de vista de Radius el perfil incluye:

- Atributos requeridos ("check-list attributes"), que definen requisitos que debe cumplir la conexión. Como parte de la transacción de autenticación, el cliente Radius incluirá en la solicitud de acceso una serie de atributos que describen las características de la conexión. Estos atributos deben cumplir las restricciones impuestas por el perfil.

- Por ejemplo, el usuario puede estar limitado a acceder a través de la RTB; si hace una llamada a través de la RDSI, el acceso será rechazado, aunque la autenticación se pudiera realizar con éxito.

- Atributos de retorno (***return-list attributes***), que son atributos que el servidor Radius envía al cliente en el mensaje de respuesta cuando la autenticación y la autorización se realizan con éxito. La lista de retorno define parámetros de configuración que el servidor de acceso debería asignar a la conexión (típicamente durante la negociación PPP).

- Por ejemplo, se puede asignar una dirección IP específica a un usuario, o habilitar la compresión de cabeceras IP, o programar la duración máxima de la conexión.

- Atributos específicos del fabricante (***vendor-specific attributes***), que son atributos de cualquiera de los dos tipos anteriores pero que no forman parte del estándar y han sido definidos por un fabricante, por lo que sólo aplican a determinados equipos. Aunque el significado de estos atributos es libre, hay unas normas de ***sintaxis*** para codificarlos en los paquetes de Radius.

CONTABILIDAD

La función de contabilidad de Radius realiza un seguimiento de las transacciones desde su inicio hasta su fin. Para ello captura estadísticas y medidas de uso de cada sesión, que permiten al servidor Radius mantener:

- Un registro histórico de todas las sesiones, con la hora de inicio y fin y estadísticas de uso.

- Una lista de usuarios actualmente conectados, actualizable en tiempo real.

7. 4. 2. ARQUITECTURA RADIUS EN UNA RED IP (ISP)

En una Red IP se necesita de una estructura que cumpla los requisitos de disponibilidad, prestaciones y escalabilidad. En la Red IP pueden aparecer una serie de intermediarios (*proxies*) entre el cliente Radius del servidor de terminales y el servidor Radius que finalmente autoriza los accesos, formando una estructura jerárquica. Estos intermediarios concentran las peticiones hacia los elementos superiores de la jerarquía, y los descargan de algunas funciones que realizan de forma autónoma.

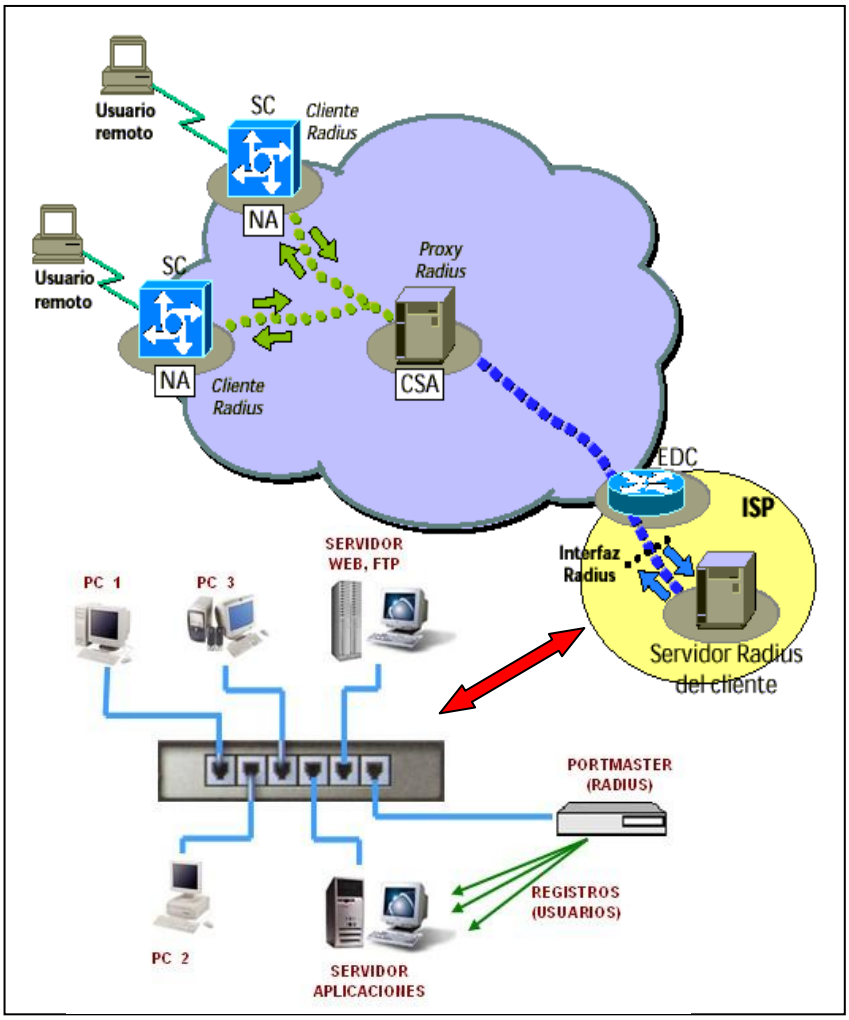


Figura 7.2 Arquitectura de Servidor Radius

7. 4. 3. REQUISITOS DE SERVIDORES

RADIUS DE CLIENTE

Antes de proceder al estudio de las diferentes alternativas en la elección del servidor Radius del cliente, para la correcta prestación de los servicios IP, ofreciéndose de este modo una visión global de los requerimientos que se han de exigir a un servidor Radius.

Se parte de un análisis inicial de los requisitos genéricos a todos los servicios, centrándose posteriormente el estudio en los requisitos específicos para un servicio en concreto, así como en otras funcionalidades Radius necesarias pero que no están incluidas en ninguno de los servicios.

REQUISITOS GENÉRICOS A TODOS LOS SERVICIOS

En los puntos que se presentan a continuación se analizan los requisitos genéricos que debe cumplir un servidor Radius comercial para la correcta prestación de los servicios.

CUMPLIMIENTO DE LAS NORMAS DEL IETF

En principio, será posible utilizar cualquier servidor Radius comercial que cumpla las normas del IETF *RFC 2138: Remote Authentication Dial In User Service (RADIUS)* y *RFC 2139: RADIUS Accounting*".

ATRIBUTOS RADIUS NECESARIOS EN LOS PAQUETES RADIUS INTERCAMBIADOS

Se recogen en este apartado los atributos Radius que, como mínimo, han de estar presentes en cada uno de los paquetes Radius intercambiados entre el servidor Radius del cliente y cada uno de los posibles clientes Radius con los que interacciona.

Se indican los atributos Radius mínimos puesto que, el resto de atributos Radius que pueden de hecho estar presentes en cada paquete Radius, depende de la arquitectura de la Red IP en la que se prestan los servicios IP, y a su vez, de las características que presente cada servicio IP en concreto, como se explica más adelante en el presente documento.

Access-Request

El paquete Radius ***Access-Request***, se envía al servidor Radius de cliente ante una petición de autenticación de un usuario, y contiene información que el servidor Radius utiliza para determinar si a dicho usuario se le permite el acceso.

Los atributos Radius que este paquete, como mínimo, debe contener son los siguientes:

- User-Name (1)

  El atributo User-Name debe llegar al servidor Radius de cliente como login@mnemonico.

- User-Password (2)/CHAP-Password (3)

  En este atributo debe cumplirse la condición para la que están definidos:

- NAS-IP-Address (4) o NAS-Identifier (32) o ambos, no deberían estar presentes los dos atributos en el mismo paquete Radius.

- NAS-Port (5) o NAS-Port-Type (61) o ambos, a menos, que el tipo de acceso que está siendo solicitado no involucre un puerto, o el nodo de acceso no distinga entre sus puertos.

Access-Accept

El paquete Radius ***Access-Accept***, lo envía el servidor Radius de cliente al correspondiente cliente Radius, validando el acceso del usuario que generó la petición de autenticación. Contiene información de configuración específica sobre el servicio que va a ser entregado al usuario.

Los atributos Radius que este paquete, como mínimo, debe contener son los siguientes:

- Proxy-State (33), caso de que este atributo Radius estuviese presente en el paquete de petición de autenticación.

Access-Reject

El paquete Radius ***Access-Reject***, es generado por el servidor Radius de cliente en caso de que el usuario que generó la petición de autenticación sea rechazado, y enviado al cliente Radius correspondiente.

Los atributos Radius que este paquete, como mínimo, debe contener son los siguientes:

- Proxy-State (33), caso de que este atributo Radius estuviese presente en el paquete de petición de autenticación.

Start Accounting-Request

El paquete Radius ***Start Accounting-Request***, se envía al servidor Radius del cliente, y contiene información utilizada para la facturación sobre el servicio que le está siendo entregado al usuario. Indica el comienzo del servicio entregado al usuario.

Los atributos Radius que este paquete, como mínimo, debe contener son los siguientes:

- Acct-Status-Type (40)

- Acct-Session-Id (44)

- NAS-IP-Address (4) o NAS-Identifier (32) o ambos, no deberían estar presentes los dos atributos en el mismo paquete Radius.

- Proxy-State (33), caso de que este atributo Radius estuviese presente en el paquete de petición de autenticación.

- NAS-Port (5) o NAS-Port-Type (61) o ambos, a menos, que el tipo de acceso que está siendo solicitado no involucre un puerto, o el nodo de acceso no distinga entre sus puertos.

Stop Accounting-Request

El paquete Radius “Stop Accounting-Request” indica el fin del servicio entregado al usuario.

Los atributos Radius que este paquete, como mínimo, debe contener son los siguientes:

- Acct-Status-Type (40)

- Acct-Session-Id (44)

- NAS-IP-Address (4) o NAS-Identifier (32) o ambos, no deberían estar presentes los dos atributos en el mismo paquete Radius.

- Proxy-State (33), caso de que este atributo Radius estuviese presente en el paquete de petición de autenticación.

- NAS-Port (5) o NAS-Port-Type (61) o ambos, a menos, que el tipo de acceso que está siendo solicitado no involucre un puerto, o el nodo de acceso no distinga entre sus puertos.

SOPORTE DE LOS ATRIBUTOS ESPECÍFICOS DE UN ISP

En la actualidad, es necesario definir una serie de atributos Radius propietarios en el servidor Radius del cliente, para el correcto funcionamiento de los servicios ofrecidos por el ISP, Por esta razón, es un requisito indispensable que el servidor Radius empleado por el cliente soporte la definición y el uso de atributos Radius propietarios. Con este objetivo, los ISPs se reservan el derecho de definir atributos Radius propietarios, para ofrecer facilidades adicionales según requiera un servicio.

CAPACIDAD DE RECUPERACIÓN FRENTE A DESCONEXIONES TEMPORALES DEL ACCESO A RED IP

Cuando se pierde temporalmente la comunicación entre el Radius de cliente y la Red IP (ISP), los paquetes de contabilidad generados por los usuarios que hasta ese momento estuviesen conectados, son almacenados en el servidor Radius de la Red IP (ISP). En el momento en que se reestablezca la comunicación con el cliente, el servidor Radius de la Red IP (ISP) le reenviará los paquetes de contabilidad que hasta ese momento tuviese almacenados. Al mismo tiempo, el cliente recibirá nuevas peticiones de autenticación de sus usuarios.

Para evitar la posible saturación del cliente consecuencia de la situación descrita anteriormente, es necesario exigir que el cliente sea capaz de cursar, por un lado, una determinada tasa correspondiente a peticiones propias del acceso de sus usuarios, y por otro, una determinada tasa para poder recibir los paquetes de contabilidad que tenga pendientes de envío como consecuencia de una desconexión previa. Esto se reflejará en un dimensionado adecuado para asegurar ese caudal, que dependerá de la arquitectura del servicio.

SOPORTE DE MÚLTIPLES CLIENTES RADIUS

El servidor Radius del cliente deberá ser capaz de trabajar con varios clientes Radius (proxies Radius o servidores de túneles que estarán

autorizados a lanzar peticiones contra el servidor del cliente) simultáneamente, sin que esto produzca inconsistencias en los procesos de autenticación o contabilidad.

7. 5. VERSIONES

Las distribuciones que existen actualmente del Radius están disponibles para los siguientes sistemas operativos:

- AIX 4.1
- Alpha Digital UNIX 3.0
- BSD/OS 2.0
- HP-UX 10.01
- IRX 5.2
- Linux 1.2.13 (ELF)
- SunOS 4.1.4
- Solaris x86 2.5.1
- Linux
- Windows NT Server 4.0

El servidor Radius puede instalarse en cualquier plataforma SUN o PC con las siguientes características:

- En plataforma SUN: Cualquier máquina (Sparc o Ultra)

- En plataforma PC: Pentium o superior

En ambos casos se requiere 32 MB de memoria RAM y 10 MB de memoria libre en disco. Para obtener un rendimiento adecuado del Servidor Radius, es recomendable que en la máquina donde se instale el Servidor ejecuten únicamente el demonio Radius, las herramientas de acceso y la base de datos de usuarios.

7. 5. 1. INSTALACIÓN DEL SERVIDOR RADIUS

A continuación el procedimiento de instalación del servidor Radius. Se indica inicialmente cómo se instala el software Radius para cada uno de los sistemas operativos para los que se distribuye.

INSTALACIÓN PARA SOLARIS

El servidor Radius para Solaris se suministra en un paquete denominado “radiuspsi”. Para realizar la instalación deberá ejecutarse como usuario root el comando: *pkgadd –d <directorio de instalación del paquete> <nombre del paquete>.* El paquete instala los archivos binarios, documentación y fuentes en el directorio /opt/radius.

INSTALACIÓN PARA LINUX

El servidor Radius para Linux se suministra por medio de un archivo con formato tar denominado “radius_lin.tar”. Para instalar el servidor debe ejecutarse el siguiente comando: *tar –xvf radius_lin.tar*

El paquete instala los archivos binarios, documentación y fuentes en el directorio /radius para la versión 4.01 del servidor Radius, y en el directorio /opt/radius/ para versiones del servidor Radius anteriores a la indicada.

INSTALACIÓN PARA WINDOWS NT

El servidor Radius se suministra en un archivo autoejecutable que se instala en el directorio c:\radius. En el directorio c:\radius se instalan los archivos binarios, documentación y fuentes del servidor Radius.

DIRECTORIOS DE INSTALACIÓN

El paquete genera los directorios que se indican a continuación en el directorio /opt/radius para Solaris, /radius para Linux, y en el directorio c:\radius para Servidores Windows :

- **bin**/ Contiene los ejecutables del servidor Radius
- **doc**/ Contiene los archivos radius-psi.pdf, atributos-radius.pdf, guia_cpi.ps y el archivo migracion.pdf.

- lib/ Contiene librerías y archivos fuente de diversas utilidades. Se incluye un archivo de documentación denominado LEEME_msj. Las librerías se emplean para poder usar diversas fuentes de datos para la información sobre los perfiles de usuario. Para el caso de Windows NT, estas librerías y archivos fuente se encuentran en el directorio c:\radius\lib, para la versión 4.01 del servidor Radius, aunque pueden también encontrarse en algunas versiones anteriores en el directorio c:\radius\src.

- raddb/ Contiene los archivos de configuración necesarios para el funcionamiento del servidor.

- bateria_infovia/ Este directorio contiene un conjunto de archivos de configuración de ejemplo, y un script denominado “bateria”. Dicho script permite realizar automáticamente un conjunto de pruebas para el servidor Radius. Las pruebas se realizan localmente utilizando las herramientas simula y rad_tool. Se simulan las peticiones que realizaría un cliente Radius para usuarios del servicio InfoVía. La ejecución deberá realizarse en este directorio, copiando previamente todos los ejecutables suministrados en el directorio bin. Si se ejecutan bateria y radiusd simultáneamente, ha de asegurarse que el puerto UDP en el archivo cfg_local_INFOVIA de bateria_infovia es distinto del de radiusd. Para ejecutar el script de pruebas basta invocarlo desde la línea de comandos con: ./bateria

- **bateria_delegado**/ Este directorio contiene un conjunto de archivos de configuración de ejemplo, y un script denominado “bateria”. Dicho script permite realizar automáticamente un conjunto de pruebas para el servidor Radius. Las pruebas se realizan localmente utilizando las herramientas simula y rad_tool. Se simulan las peticiones que realizaría el servidor Proxy Radius de la Red IP para usuarios del servicio InfoVía Plus Básico (Modalidad Delegada). La ejecución deberá realizarse en este directorio, copiando previamente todos los ejecutables suministrados en el directorio bin. Si se ejecutan batería y radiusd simultáneamente, ha de asegurarse que el puerto UDP en el archivo cfg_local_INFOVIA de batería _ delegado es distinto del de radiusd. Para ejecutar el script de pruebas basta invocarlo desde la línea de comandos con: ./batería.

CAP. VIII

DISEÑO DE LA APLICACIÓN

INTRODUCCIÓN

INVESTIGACIÓN PRELIMINAR

DETERMINACIÓN DE LOS REQUERIMIENTOS

ESTUDIO DE FACTIBILIDAD

DISEÑO Y DESARROLLO DEL SISTEMA

8. DISEÑO DE LA APLICACIÓN (TARNET)

8. 1. INTRODUCCIÓN

El desarrollo de un Software diferente, que tarife a los usuarios del ISP, nació por el grado de dificultad que un administrador debía librar a diario.

Esta es la razón fundamental, por la cual se emprendió la tarea de proporcionar una aplicación distinta a la estándar, que nos brinde un mejor entorno grafico, tanto para el administrador como para el usuario final (responsable de cobrar), además sea igual o más confiable que el Software existente.

8. 2. INVESTIGACIÓN PRELIMINAR

Toda la investigación se centro en como funciona el RADIUS con respecto a la tarifación de tiempos de conexión, que archivos crea, que archivos usa, y lo más importante, el tipo de información que queremos generar, que datos tendrá TarNet, para generar información.

8. 2. 1. COMO FUNCIONA

Como funciona el RADIUS se explica con detalle en el Capitulo VII.

Acotaremos que RADIUS es muy usado en los servidores de comunicación para la validación de las entradas de los usuarios que

usan el servicio de Internet, y que guarda los archivos de la contabilidad de cada entrada.

RADIUS consta de dos partes, un servidor y un cliente, el servidor es el que se instala en la computadora que va a realizar el manejo de los archivos de usuario y contabilidad, y el cliente viene con el equipo se acceso al servidor (Livingston, Cisco, etc.),

El servidor de RADIUS consta de un sistema de archivos, en los cuales se configura el usuario, tipo de tarifa, que usuarios paga o no IVA, etc.

Para el diseño de TarNet se emplea o se utilizara el archivo de contabilidad, este archivo se genera automáticamente al registrarse el intercambio de información entre el usuario y el proveedor del servicio de Internet.

Este archivo se encuentra ubicado en el directorio **/var/adm/radacct**.

Bajo este subdirectorio se encuentra el archivo de nombre **Detail,** archivo plano que contiene información de cada entrada de un usuario. Este se detalla en la **Tabla 8.1**

```
Mon May 29 00:06:00 2000

Acct-Session-Id = "2800159D"

User-Name = "jdvb"

Client-Id = 204.225.204.7

Client-Port-Id = 22

NAS-Port-Type = Async

Acct-Status-Type = Start

Acct-Authentic = RADIUS

User-Service-Type = 2

Framed-Protocol = PPP

Framed-Address = 204.225.204.37

Acct-Delay-Time = 0
```

Mon May 29 00:01:46 2000
Acct-Session-Id = "2800159C"
User-Name = "orquera"
Client-Id = 204.225.204.7
Client-Port-Id = 16
NAS-Port-Type = Async
Acct-Status-Type = Start
Acct-Authentic = RADIUS
User-Service-Type = 2
Framed-Protocol = PPP
Framed-Address = 204.225.204.49
Acct-Delay-Time = 0

Tabla 8.1 Detalle de archivo Detail

Estas tramas contienen toda la información necesaria para determinar los requerimientos, determinar si es factible o no el diseño de TarNet.

8. 2. 2. DETERMINACIÓN DE LOS REQUERIMIENTOS

El determinar los requerimientos para el diseño de TarNet, fue una tarea por demás importante.

Para determinar los requerimientos nos enmarcamos en dos áreas específicas, el Hardware y el Software.

El las dos áreas se tuvo en cuenta parámetros esenciales como:

- Rendimiento del equipo.
- Costo
- Disponibilidad
- Información existente
- Funcionalidad

Estos como parámetros generales.

Establecido los parámetros, se determino el Software necesario, la Base de datos ***MySQL***, eficiente, con gran capacidad de almacenamiento, con capacidad de ejecutar consultas, con una arquitectura

cliente/servidor con un costo mínimo, que permitiera la conexión con PHP.

PHP como herramienta para el diseño de los formularios de TarNet, que al igual que MySQL, permite generar código para la conexión a la base de datos, permite manipular datos, sin costo, se encuentra en todas las versiones actuales de LINUX, etc.

Lo que afianzo su uso en el diseño e implementación de TarNet fue su compatibilidad con el sistema LINUX.

8. 2. 3. ESTUDIO DE FACTIBILIDAD

Para el desarrollo TarNet analizamos la Factibilidad Técnica, Operacional y la Económica, permitan la realización y ejecución del proyecto.

Factibilidad Técnica

La Factibilidad Técnica permite analizar la conveniencia o no del Proyecto, en el aspecto de:

Si contamos con un Proyecto que supere en beneficios para la institución, que el sistema propio de RADIUS.

Esto es posible con TarNet, ya que permitirá brindar mejores facilidades, tanto en reportes, ingresos, consultas, sobre todo brindara un mejor panorama para la administración de los usuarios.

Factibilidad Operacional

TarNet permitirá completa y eficiente administración de los rubros, que cada uno de los usuarios deberá asumir.

La administración de TarNet, la podrá realizar, cualquier persona que tenga ligeros conocimientos, tanto en los planes de conexión de la Empresa como en la forma de ingresar los datos.

Por este motivo, la administración y uso de TarNet la podrán realizar personas, que tengan o se les proporcione una ligera charla, sobre el uso y funcionamiento de TarNet.

Factibilidad Económica

El aspecto económico del proyecto es muy inferior al costo real el Sistema con fines comerciales.

8. 2. 4. DISEÑO DEL SISTEMA

TarNet un sistema que permitirá manipular datos desde un navegador Web o browser como cliente, y como servidor de base de datos actuara el servidor de Web Apache con una extensión llamada PHP.

TarNet estará compuesto por cinco elementos principales como:

- LINUX como sistema operativo abierto.
- Apache como servidor Web.
- PHP como modulo de aplicación de Apache para acceder a la base de datos.
- MySQL como base de datos.
- Una interfaz Web a MySQL.

Todos los elementos del sistema se pueden obtener sin ningún tipo de costo por lo que el montaje inicial de TarNet no conlleva ninguna inversión. A excepción de MySQL, de la que hay que comprar licencias en caso de que se quiera vender sistemas que la incluyan, todos los demás elementos tienen licencia libre.

INTRODUCCIÓN AL SISTEMA

TarNet tiene la siguiente arquitectura, **Figura 8.1**

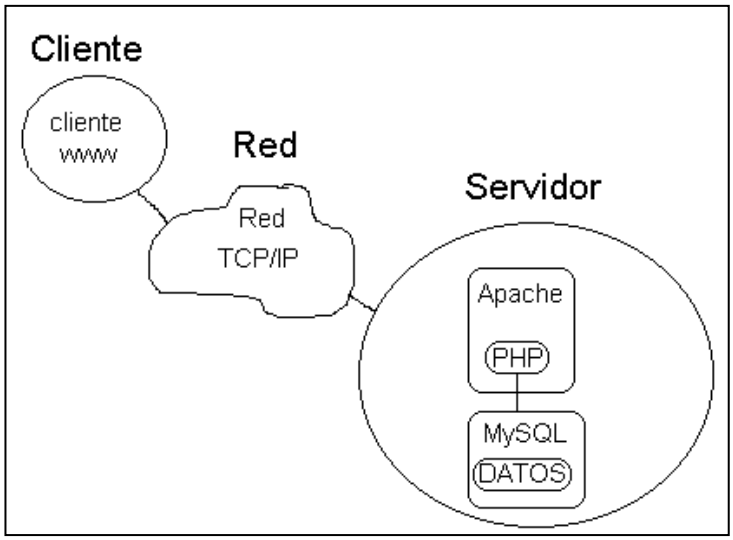


Figura 8.1 Arquitectura de TarNet

TarNet permite que el usuario interactué con la base de datos, a través de los siguientes pasos:

- El cliente carga una página WEB con un formulario, ingresa los datos y los envía al servidor.

- A través de la red TCP/IP los datos llegan al servidor, y son enviados a un programa PHP.

- El servidor detecta que los datos se envían a una pagina PHP, por lo que informa al modulo de PHP del programa a ejecutar y le pasa los datos del cliente.

- El modulo de PHP ejecuta el programa, el cual accederá a MySQL.

- MySQL procesa la petición del programa PHP y le envía de vuelta los resultados.

- El modulo PHP recibe los resultados y a través del servidor Apache, envía una pagina WEB con los resultados al cliente.

- El cliente recibe la pagina WEB resultado de sus peticiones, a través de la red TCP/IP, interna.

8. 2. 5. DESARROLLO DEL SISTEMA

Introducción

Realizado el análisis de factibilidad, determinación de los requerimientos, el diseño de su arquitectura general, se procedido al desarrollo de TarNet (Tarifación de Internet)

El desarrollo de TarNet tuvo facetas bien definidas, como:

- Instalación y configuración de los equipos (Servidor y Cliente), al nivel de Hardware.

- Instalación y configuración de LINUX Software base.

- Instalación y configuración de Software de desarrollo, MySQL, PHP, APACHE.

- Verificación de la presencia de un browser en el cliente y servidor.

Diagramas explicativos de Tarnet

La estructura, el funcionamiento y disponibilidad para cada usuario de Tarnet se explica a través de los siguientes diagramas:

Diagrama de Casos de Uso

Un Diagrama de Casos de Uso es un diagrama que muestra un conjunto de casos y sus relaciones. Normalmente contiene: Casos de uso, Actores, Relaciones de Dependencia.

Los diagramas de caso de uso se emplean para modelar la vista de casos de uso estática de un sistema. Esta vista cubre principalmente los servicios visibles externamente que proporciona el sistema.

Para la construcción del diagrama de casos de uso (ver **Figura 8.2**) se identificaron:

Dos actores, cinco cosos de uso, dos relaciones de extensión y dos relaciones de inclusión.

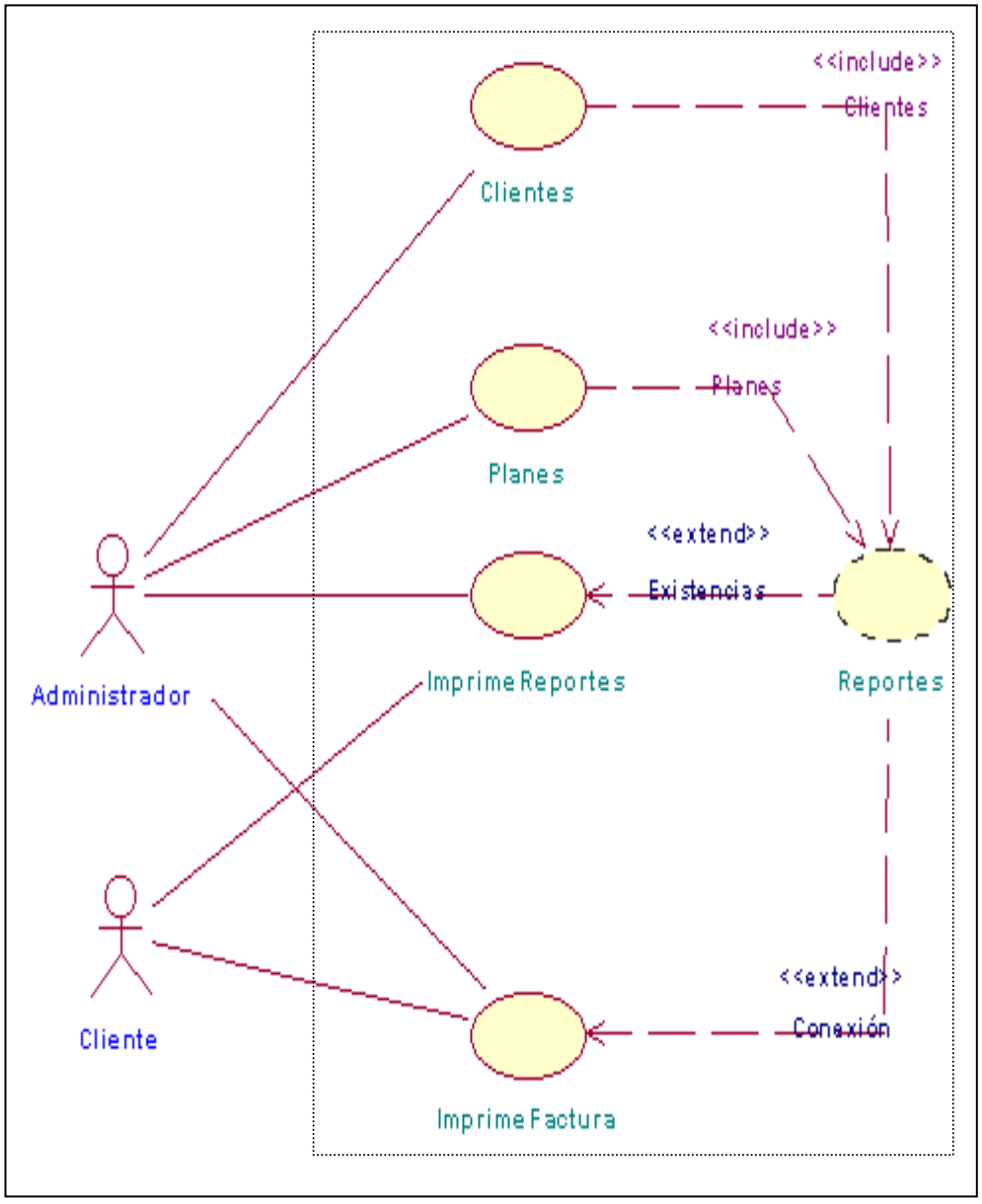


Figura 8.2 Diagrama de Casos de Uso

La descripción de los actores y caos de uso se detalla a continuación:

ACTOR	CASO DE USO	RELACIÓN
Administrador	Clientes	Primaria
Administrador	Planes	Primaria
Administrador	Imprime Reportes	Primaria
Administrador	Reportes	Inclusión (Clientes/Reportes)
Administrador	Reportes	Inclusión (Planes/Reportes)
Cliente	ImprimeReportes	Primaria
Cliente	ImprimeFactura	Primaria
Cliente	Reportes	Extensión (Reportes/ImprimeReporte)
Cliente	Reportes	Extensión (Reportes/ImprimeFactura)

Tabla 8.1 Descripción Casos de Uso

Diagrama de Actividades

Un Diagrama de Actividades es fundamentalmente un diagrama de flujo de control entre actividades.

Los Diagramas de Actividades se utiliza para modelar aspectos dinámicos de un sistema, esto implica modelar los pasos secuénciales de un proceso computacional. Las actividades producen finalmente alguna acción , que producen un cambio en el estado del sistema o la devolución de un valor. Las acciones incluyen llamadas a otras operaciones.

Para la construcción del Diagrama de Actividades (ver **Figura 8.3**) se identificaron:

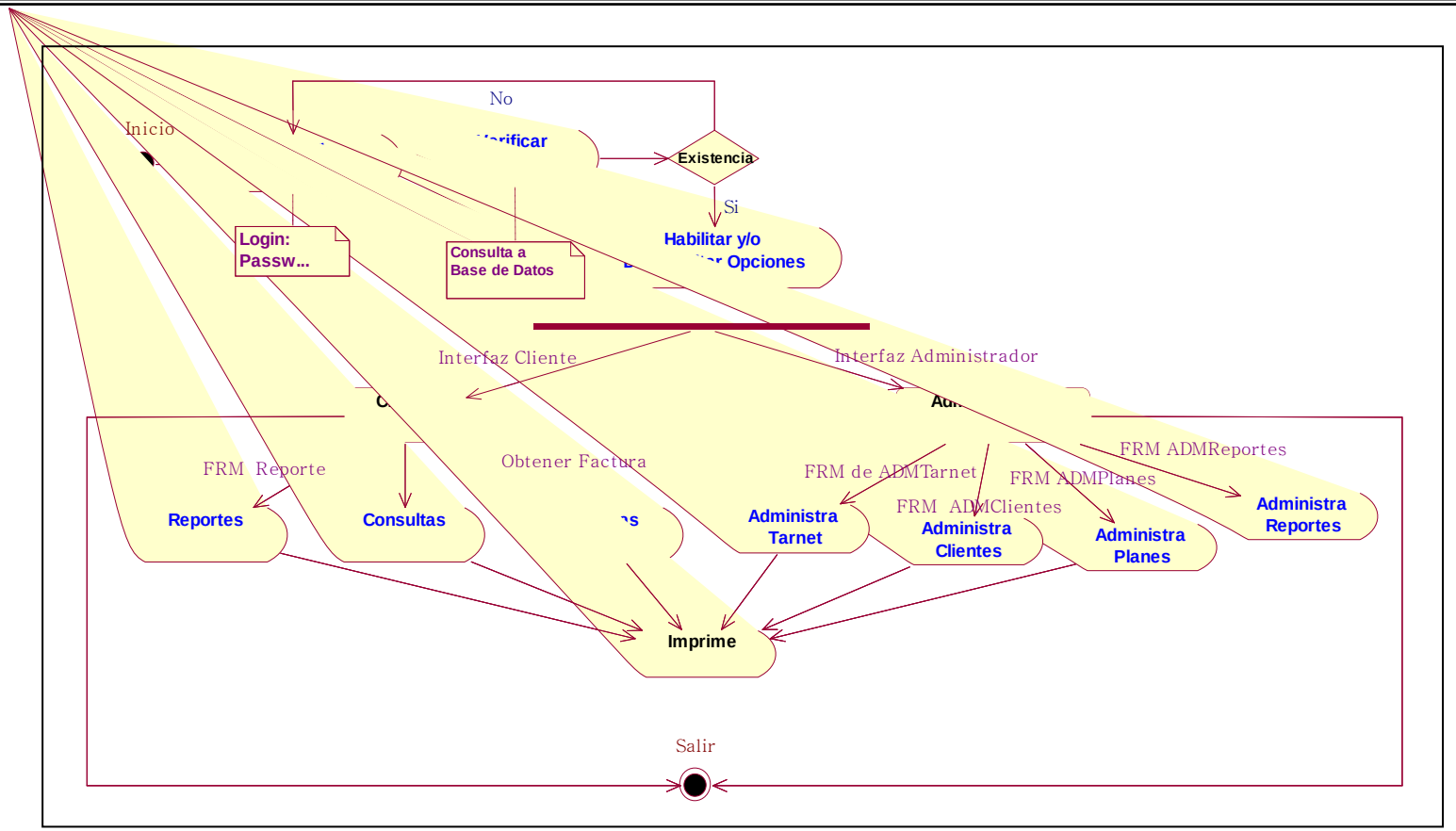


Figura 8.3 Diagrama de Actividades

Diagrama de Clases

Un Diagrama de Clases es un diagrama que muestra un conjunto de Interfaces, colaboraciones y sus relaciones. Gráficamente, es una colección de nodos y arcos

Los Diagramas de Clases se utilizan para modelar la vista de diseño estática de un sistema. Principalmente, esto incluye modelar el vocabulario del sistema, modelar las colaboraciones o modelar esquemas.

Los Diagramas de Clase son importantes no solo para visualizar, especificar y documentar modelos estructurales, sino también para construir sistemas ejecutables.

Los Diagramas de Clases contienen normalmente los siguientes elementos: Clases, Interfaces, Colaboraciones, Relaciones de Dependencia, etc.

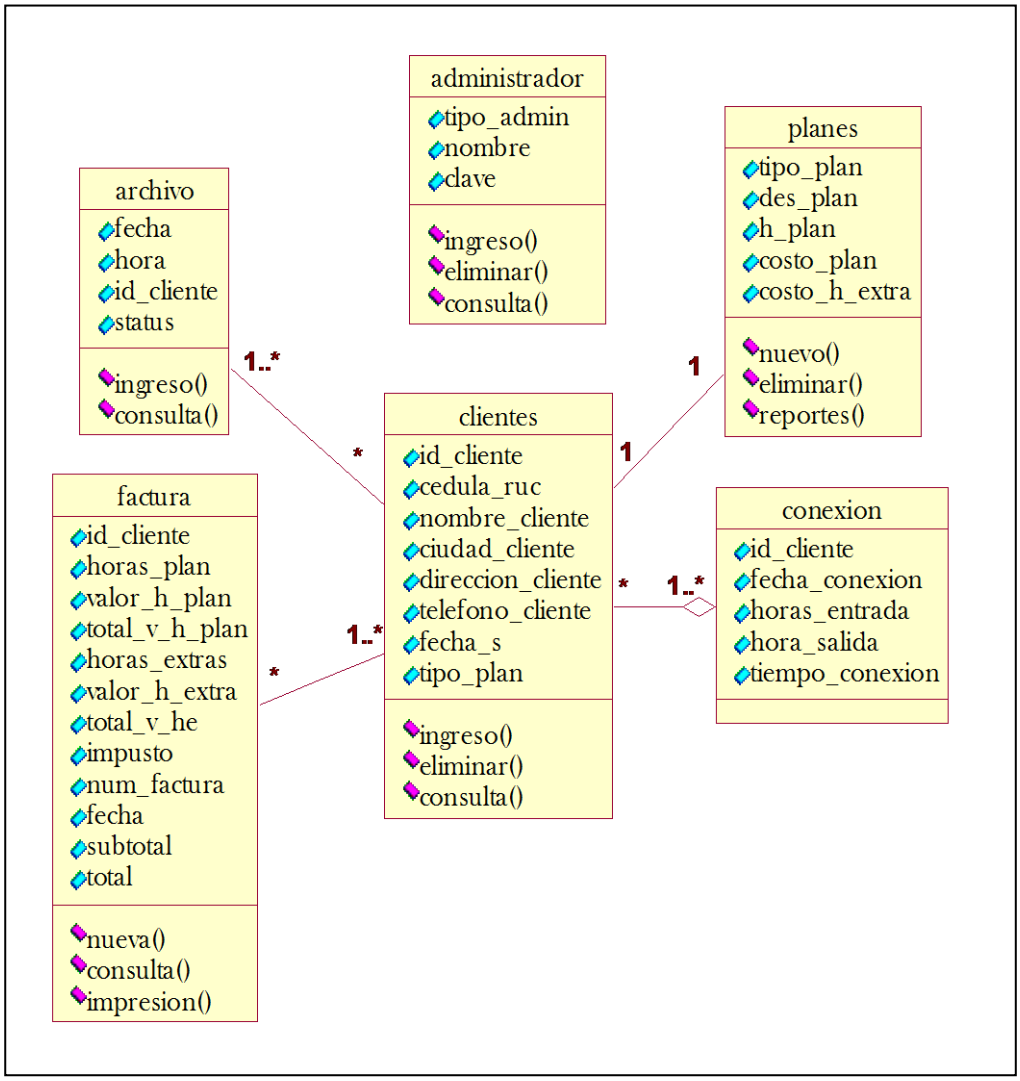
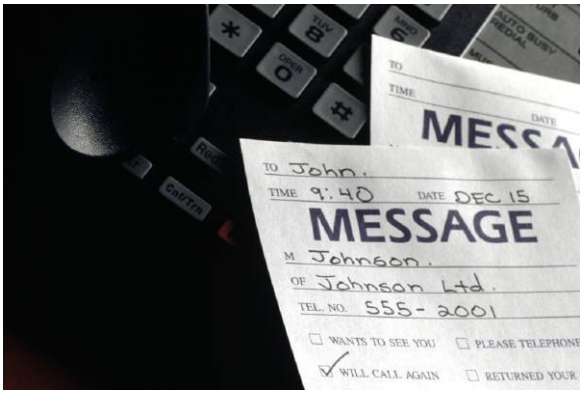


Figura 8.4 Diagrama de Actividades

La Figura 8.4 muestra las clases de TarNet a nivel suficiente detallado para construir una base de datos física.

En las seis clases contienen sus atributos y operaciones para manipular sus partes, estas operaciones se incluyen para mantener la integridad de los datos.

CAP. IX



CONCLUSIONES Y RECOMENDACIONES

VERIFICACIÓN DE LA HIPÓTESIS

CONCLUSIONES

RECOMENDACIONES

BIBLIOGRAFÍA

ANEXOS

9. CONCLUSIONES Y RECOMENDACIONES

9. 1. VERIFICACIÓN DE LA HIPÓTESIS

La hipótesis planteada en el Anteproyecto

> **"El estudio del comportamiento y evaluación del tiempo, en el que los usuarios acceden a los servicios de un ISP, permitirá la creación de un Software de Tarifación, otorgando flexibilidad al proceso de facturación y control, con alta confiabilidad a menor costo, que solucione los problemas actuales de este tipo de Empresas".**

Consideramos que de acuerdo a la investigación realizada y el Software, desarrollado para el efecto, demuestran la Verificación de Hipótesis.

A continuación un análisis valorativo del Sistema de Tarifación de Usuarios RAS en un proveedor de Servicios de Internet bajo Plataformas Linux (**TARNET**).

VARIABLES INDEPENDIENTES

1. Comportamiento de acceso

2. Tiempo de acceso

VARIABLES DEPENDIENTES

1. Creación de Software

ALTERNATIVA 1

EL COMPORTAMIENTO DE ACCESO FRENTE A LA CREACIÓN DEL SOFTWARE

SOFTWARE		
COMPORTAMIENTO DE ACCESO	**Nº USUARIOS**	**%**
HORAS PICO	35000	70
HORAS NO PICO	15000	30
TOTAL	50000	100

Tabla 9.1 Comprobación Alternativa 1

Diagrama

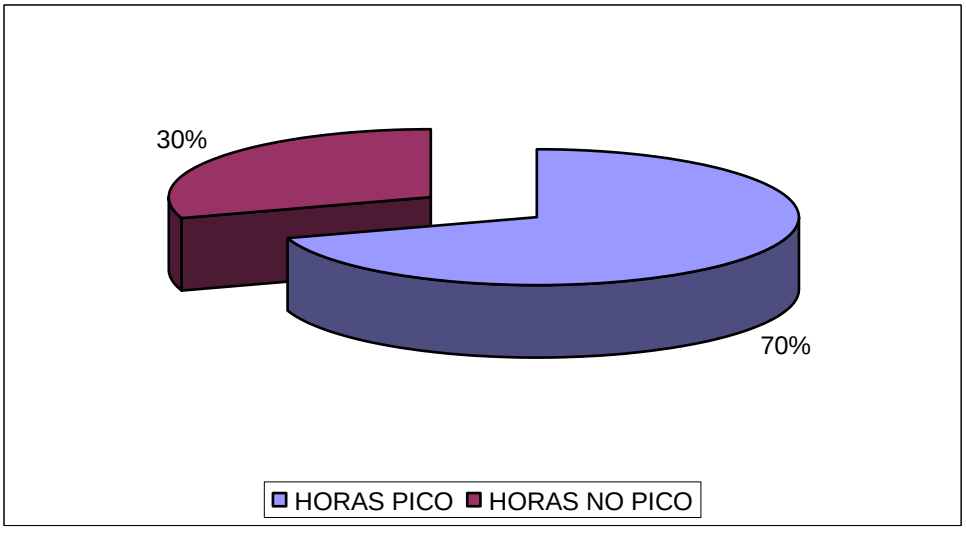


Figura 9.1 Comprobación Alternativa 1

Análisis

De los 50000 usuarios que acceden a los servicios del ISP, el 70% acceden en horas pico y el 30% en horas no pico; lo que indica la conveniencia de la creación del Software.

ALTERNATIVA 2

LOS TIEMPOS DE ACCESO FRENTE A LA CREACIÓN DEL SOFTWARE

SOFTWARE		
EL TIEMPO DE ACCESO	**Nº USUARIOS**	**%**
SI INFLUYE	45000	90
NO INFLUYE	5000	10
TOTAL	50000	100

Tabla 9.2 Comprobación Alternativa 2

Diagrama

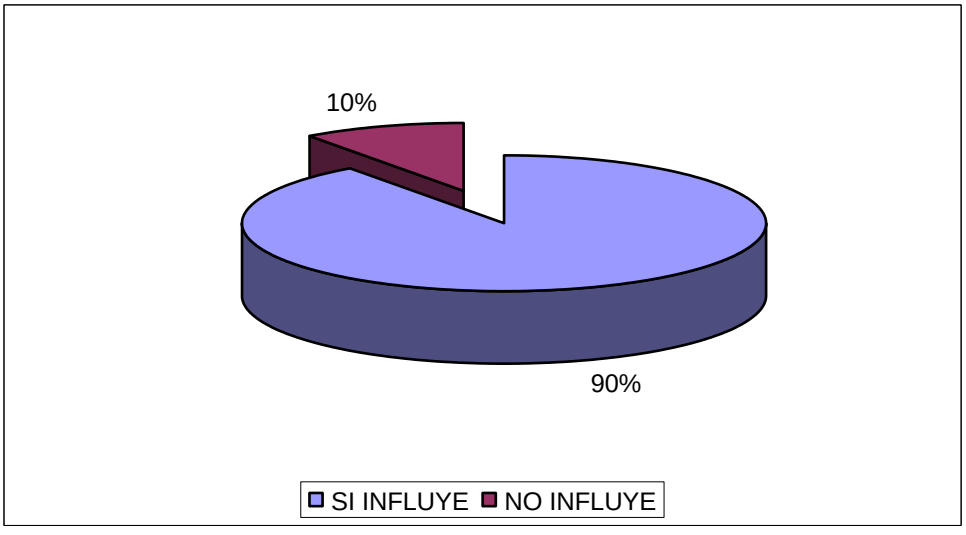


Figura 9.2 Comprobación Alternativa 2

Análisis

De los 50000 usuarios que acceden a los servicios del ISP en relación a los tiempos de conexión, el 90% influye la flexibilidad y rendimiento del Software de tarifación.

Resultados

El Software de Tarifación presta los siguientes servicios:

- Registro de Usuarios a ser miembros de los servicios de un ISP
- Registro de Planes Tarifarios de acuerdo a las necesidades y comodidades de los usuarios
- Asignación o modificación de datos y planes a los usuarios nuevos o registrados por parte del Administrador del ISP
- Registro de Tarifas y cálculo de valores tarifarios de los usuarios basándose en sus tiempos de acceso y plan suscrito
- Búsqueda de los usuarios que accedieron a los servicios del ISP
- Agrupamiento dinámico de los tiempos de acceso
- Bloquear o suspender el servicio a los usuarios que exceden los planes tarifarios suscritos

- Visualizar información de los tiempos de acceso

- Eliminación de usuarios del registro del ISP

9. 2. CONCLUSIONES

- Linux es un Sistema Operativo que ha ganado confianza y mercado en las empresas prestadoras de servicios de Internet.

- Linux, posee excelentes herramientas de desarrollo (Kylix, PHP, C++, KDeveloper, etc.) y avanzados motores de Bases de Datos (MySQL, Postgres, Oracle, Informix, etc.).

- RADIUS un protocolo estándar de seguridad para accesos remotos, su interfuncionamiento con Redes IP, permite un eficiente control de usuarios del ISP.

- La utilización y manejo de Elementos Activos en los ISP es fundamental para la prestación de servicios del Internet.

- TarNet presta la flexibilidad y rendimiento en el control de acceso de Usuarios a un ISP

- El control del tiempo de conexión es fundamental en TarNet.

- La tecnología que poseen los ISPs permite brindar un mejor servicio a los clientes.

- La documentación que facilitan las empresas públicas y privadas, constituye un aporte fundamental para la investigación y obtención de nuevas alternativas.

9. 3. RECOMENDACIONES

- Capacitar al responsable de la Administración de Usuarios en un ISP, sobre el manejo de TarNet

- Obtener informes cuando no sean horas pico, por mayor rapidez.

- Masificar el uso del sistema operativo Linux, como software base en los Proveedores de Servicios de Internet.

- Utilizar el estándar RADIUS, aprovechando configuraciones y compatibilidades con los Sistemas Operativos del mercado.

- Elaborar un cronograma de monitoreo para Elementos Activos del Proveedores de Servicios.

- Aplicar, normar, reglas estándares actuales en la configuración de Elementos Activos.

- Todo ISP tendrá que estar a la vanguardia de la tendencia tecnológica.

- Fomentar los convenios Interinstitucionales, con el la finalidad de facilitar la obtención de la información necesaria.

9. 4. BIBLIOGRAFÍA

- TANEMBAUM, Andrew S. (1997). Redes de Computadoras. México: Editorial Prentice Hall Hispanoamericana S.A..
- COMER, Douglas. (1997). Redes de Computadoras, Internet e Interredes. España: Editorial Prentice Hall Hispanoamericana S.A.
- JONES, A., OHLUND J. (1999). Network Programming for Microsoft Windows. Madrid: Microsoft Press.
- TIMKY (1995). Aprendiendo TCP/IP en 14 Días. México: Parker.Editorial Prentice Hall Hispanoamericana S.A.
- TACKETT, J., BURNETT, S. (1998). Linux. Madrid: Editorial Prentice Hall Hispanoamericana S.A., 4ta Edición.
- CARLING, M., DEGLER, S., JONES D. (2000). Administración de Sistemas Linux. Madrid: Editorial Prentice Hall Hispanoamericana S.A.
- TYSON, Greer (1998). Así son las Intranets. Madrid: Editorial Mc GrawHill Hispanoamericana S. A.
- BOOCH, G., RUMBAUGH, J., JACOBSON, I. (1999). El Lenguaje Unificado de Modelado. Madrid: EMCMXCIX S.A.
- BLACK, Uyless. (1989). Redes de Computadoras. Madrid: EMA Editorial.
- SHELDON, Tom (1995). Enciclpedia LANTIMES de Redes (Traducido por M. Isabel ARROYO Y DE DOMPABLO). México: McGraw-Hill, Inc. (Original publicado en 1994.)
- DUBRIS, Paúl (2001, Primera Edición). MySQL (Traducido por KME, Sistemas, S.L.). Madrid: Prentice Hall. (Original publicado en 2001.)
- Anónimo (2000). Administración de Sistemas Linux. Madrid, España: The Coriolis Group, LLC.

INTERNET

http://www.genuity.com/services/access/dialink/index_sp.htm

http://www.gio.es/abonados/información/internet

http://200.44.120.106/volumenes/internetbib/curso/cap2

http://www.rediris.es/ftp/docs/network/rfc/.

http://www.worldbank.org/worldlinks/spanish/training/MODULOS_html/MOD_2

/ redes.html

http://memeber.tripod.com/a_pizano/html/cap2.html

http://www.nerja.net/ tcp-ip/Tutorial de Internet,arquitec-Internet-archivos.htm

http://alojamiento24h.com/conexión/page4.html

9. 5. GLOSARIO

10 BASE 2 Especificación IEEE 802.3, similar a Ethernet, mediante el uso de cable coaxial, soporta una capacidad de transferencia de hasta 10 Mbps. La distancia limite de este tipo de cableado es de hasta 185 mts por segmento.

10 BASE T Especificación IEEE 802.3, hace uso del cable twisted-pair o par trenzado, soporta una capacidad de transferencia de 10 Mbps.

100 BASE T Especificación IEEE 802.3, hace uso del cable twisted-pair o par trenzado reforzado, soporta una capacidad de transferencia de 100 Mbps.

ABM Modo asíncrono balanceado. Siendo el HDLC un protocolo derivado, que soportan modos de comunicación orientado de puntos, punto a punto, las comunicaciones entre dos estaciones, donde una estación pueden iniciar la transmisión.

ADAPTADOR DE RED Tarjeta de interfase de red, dispositivo que colocado sobre una ranura ISA, EISA o PCI. Permita la comunicación entre la PC o equipo computacional y la Red.

ADMINISTRACIÓN DE DATOS Función dentro de una organización encargada de la administración de los datos, mediante el análisis, clasificación y conservación de los datos y las relaciones entre los mismos; la coordinación para el desarrollo de modelos y diccionario de datos, combinado con el volumen de transacciones, representan la materia prima para el diseño de Base de Datos.

ADSL Línea de Abonados Digital Asimétrica

AM Amplitud Modulada, técnica de modulación de la conversión de la información sobre una amplitud de la onda.

AMERICAN NATIONAL STANDARD INSTITUTE (ANSI)	Instituto Nacional de Estándares de los Estados Unidos
AMPLITUD	Valor máximo análogo a una onda de forma digital
APACHE	Servidor Web
APLICACIÓN	Programa de computadora orientado a automatizar alguna actividad
APPI	Estándar abierto de arquitectura IP para redes SNA, bajo el entorno de redes punto a punto.
APPN	Redes punto a punto. Facilidades de operación de las Redes SNA de IBM, que provee de distribución de procesos basado en Unidades Lógicas LU 6.2.
AR	Indicador de acceso.
ARPA	Advanced Research Proyect Agency.
ARPANET	Primera Red Científica y Académica. La primera red de conmutación de paquetes. Ofrece servicios datagrama en los cuales se envían los paquetes a lo larga de varias rutas a través de una malla de conexión.
ARPANET	Constituye una Red Informática organizado por el Departamento de Estado de EE.UU., que sirvió de base para la implantación de INTERNET.
AS	Sistema autónomo, un conjunto de redes bajo una administración común que comparte una común estrategia de desarrollo.
ASCII	Código estándar de Americano (EE.UU.) para el intercambio de información, bajo la representación de caracteres de 8 bits.
ATDM	Multiplexor de División de Tiempo Asíncrono. Método de seding información que parece TDM normal, excepto que las ranuras de tiempo se destinan como preassigned transmisores específicos.

ATM	(Asynchronous Transfer Mode) Modo de transferencia asíncrono. Técnica de conmutación por paquetes de alta velocidad, adecuada para redes de área metropolitana (MAN), transmisión de banda ancha y redes digitales de servicios integrados (RDSI).
AUI	Attachment Unit Interface. Son los elementos (ejemplo un cable y un MAU) que conectan un dispositivo a la red.
BACKBONE NETWORK	Espina dorsal de una red de comunicaciones. Es el cableado principal que une la red Base con las redes departamentales.
BASE DE DATOS	Conjunto de datos organizados entre los cuales existe una correlación y que están almacenados con criterios independientes de los programas que los utilizan. La filosofía de las bases de datos es la de almacenar grandes cantidades de datos de una manera no redundante y que permita las posibles consultas de acuerdo a los derechos de acceso.
BITNET	**B**ecause **I**t's **T**ime **Net**work. Una red académica de bajo costo, baja velocidad que consistía primariamente de Mainframes IBM y líneas de comunicación de 9600 bps
BNC CONNECTOR	Conector estándar usado para conectar cables coaxiales (10Base2- Norma IEEE 802.3).
BRI	Interfase de programación básica
BROWSER	Navegador WEB.
CABLE	Medio de transmisión de cable o fibra óptica, dentro de una cubierta protectora
CABLE COAXIAL	Cable de alta capacidad utilizado en comunicaciones y vídeo. Contiene un alambre aislado, sólido o de filamentos, que esta rodeado por un forro metálico sólido o trenzado (tipo malla), bajo una cubierta exterior de material plástico.

CCITT	**C**onsultive **C**ommittee for **I**nternational **T**elephony and **T**elegraphy (Comité Consultivo para Telefonía y Telegrafía Internacionales)
CD	**C**arrier **D**etect. Señal que indica cuando un dispositivo esta activo. Se le denomina así también a la señal generada por un MODEM indicando que una llamada esta ingresando. Se usa también para indicar un **C**ompact **D**isc.
CELULAR RADIO	Una tecnología que usa la transmisión por ondas radiales para acceder a la red de la compañía de teléfonos.
CHAP	Autentificación criptográfica o no criptográfica
CLIENTE	Estación de trabajo o computador personal en un ambiente de Cliente / servidor.
CLIENTE / SERVIDOR	Arquitectura donde el cliente es la maquina solicitante (computador personal o estación de trabajo) y el servidor es la máquina proveedora. El cliente suministra la interfaz del usuario y realiza una o la mayor parte del procesamiento de la aplicación. El servidor mantiene las bases de datos y procesa las solicitudes del cliente para extraer o actualizar los datos de la base correspondiente. El servidor además controla la integridad y seguridad de la aplicación.
CM/P	Control de Programa para Microcomputadores
ComOS	Sistema Operativo del RAS
COMUNICACIONES	Transferencia electrónica de información de un lugar a otro. Las comunicaciones de datos se refieren a transmisiones digitales, y las **telecomunicaciones** se refieren a todas las formas de transmisión, que incluyen voz y vídeo analógicos y digitales.
CONCENTRADOR	Dispositivo que une varios canales de comunicación en uno solo. Se le suele denominar también HUB.

CSLIP	Compressed SLIP
CSMA / CD	**C**arrier **S**ense **M**ultiple **A**ccess / **C**ollision **D**etection.
DARPA	Defense Advanced Research Projects Agency
DARPA	**D**efense **A**dvanced **R**esearch **P**rojects **A**gency. Agencia Gubernamental de los Estados Unidos para proyectos de desarrollo y experimentación con **Internet**. Anteriormente se denominaba ARPA (Advanced Research Projects Agency).
DATAGRAMA	Agrupación de datos con información de encabezamiento que contiene las direcciones fuente y destino, información de la corrección de errores, numero de secuencias y otra información. Tienen un tamaño limitado.
DECnet	ES un grupo de productos de Comunicaciones, desarrollado y soportado por la firma Digital Equipment Corporatión. DECnet Phase V esta ampliamente basada en los protocolos OSI.
DEMODULACION	Proceso de retornar una señal modulada a su forma original. Los módems realizan la demodulación tomando una señal analógica y retornándola a su forma (digital) original.
DHCP	Protocolo de configuración dinámica de ordenadores
DIAL-UP	Conexión vía telefónica
DNS	Servidores de Nombre de Dominio
EDI	**E**lectronic **D**ata **I**nterchange - Intercambio de Datos Electrónicos. Comunicación electrónica de transacciones entre organizaciones, como pedidos, confirmaciones, facturas, etc.
EIA	**E**lectronic **I**ndustries **A**ssociation. Asociación de Industrias Electrónicas. Es un grupo de industriales dedicados a la electrónica que realiza especificaciones de estándares de transmisión

eléctrica.

EISA **E**xtended Industry Standard Architecture. Arquitectura estándar industrial extendida.

ENVIO DE PAQUETES Proceso realizado por un nodo de red cuando envía paquetes al siguiente nodo o al encaminador apropiado de la red.

ESTUDIO DE FACTIBILIDAD Análisis de un proyecto, que determina la posibilidad de ser realizado en forma efectiva. Los aspectos operacionales (funcionamiento), económicos (costo/beneficio) y técnicos (posible ejecución); son partes del estudio. Los resultados de un estudio de factibilidad proveen datos para una decisión de iniciar el proyecto.

ETHERNET Es una especificación de una red de área local de banda base inventada por la Corporación XEROX y desarrollada en conjunto por Xerox, Intel y DEC (Digital Equipment Corporation). Las redes Ethernet operan a 10Mbps usando CSMA / CD (Sensor de portadora de accesos múltiples / Detección de colisiones) y corren sobre cable coaxial. Ethernet es similar a la serie de estándares IEEE 802.3.

FDDI **F**iber **D**istributed **D**ata **I**nterface. Interfaz de distribución de datos de fibra óptica. Conjunto de Normas de ANSI (American National Standards Institute) para redes de área local de alta velocidad que utiliza fibra óptica y transmite a 100 Mbps hasta 2 Km. Usa una arquitectura de doble anillo para proveer redundancia. Las especificaciones del FDDI se aplican a las capas 1 y 2 del modelo OSI.

FILTRO IP Forma de clasificar y seleccionar IP de forma que solo se acepten IPs de un tipo especifico.

FILTRODO DE PAQUETES	Forma de clasificar y seleccionar paquetes de forma que solo se transmitan los paquetes de un tipo especifico o con una dirección concreta.
FRAME	Marco, Cuadro. En Comunicaciones, un agrupamiento de bits que constituyen un bloque elemental de datos para su transmisión mediante ciertos protocolos.
FRAME RELAY	Relay de Cuadro o Trama. Protocolo de conmutación de paquetes de alta velocidad que proporciona una transmisión más rápida que el protocolo X.25. Es más adecuado para la transferencia de datos y de imágenes que para la voz.
FRONT END	Es un nodo o programa de software que hace un pedido de servicio a un Back End (proveedor de servicios).
FTP	File Transfer Protocol. Es una aplicación usando el protocolo IP (Internet Protocol) para transferir archivos entre nodos de una red.
FTTH	Fibre To The Home
GNOME	Entorno de Desarrollo Gráfico de LINUX
GRE	Generic Routing Encapsulation
GUI	Interfaz Gráfica
HOST	Ordenador conectado a Internet. Ordenador en general.
HUB	Dispositivo que sirve como centro de una red de topología estrella. Los hubs pueden ser **activos** (cuando repiten la señal enviada a través de ellos) o **pasivos** (cuando no lo repiten, sino que solamente reparten la señal enviada a través de ellos)
IAS	Servicio de Interconexión Abierto
IEEE	**I**nstitute of **E**lectrical and **E**lectronic **E**ngineers. Organización de profesionales Eléctricos y Electrónicos que define los estándares de redes.
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange

INFOMAIL	Servicio Público de Mensajería Multimedia en Red
INTERCONECTIVIDAD	Véase Interoperatividad
INTERCONEXION DE REDES	Véase Redes
INTERNET	Malla mundial de computadoras y redes de computadoras interconectadas, es una única gran red de comunicaciones extendida por todo el mundo. Termino usado para referirse a la red más grande del mundo, que conecta miles de redes con alcance mundial. Esta creando una cultura que basándose en la simplicidad, investigación y estandarización basada en usos de la vida real, esta cambiando la forma de ver y hacer muchas de las tareas actuales. Mucha de la tecnología de punta en redes esta proviniendo de la comunidad Internet. Internet es una evolución de ARPANET, algunas veces llamada DARPA Internet.
INTERNETWORKING	Termino general usado para referirse a la industria que se ha desarrollado alrededor del problema de interconectar y hacer trabajar en forma conjunta diferentes tipos de redes. El término puede referirse a productos, procedimientos y tecnologías.
INTEROPERABILIDAD	Es la habilidad de equipos de cómputo de diferentes proveedores de intercomunicarse entre ellos, dentro de una red.
INTEROPERATIVIDAD	Es la capacidad de que diferentes sistemas de computadoras, redes, sistemas operativos y aplicaciones trabajen juntos.
IP	**I**nternet **P**rotocol. Es nivel de protocolo de redes que contiene información de direccionamiento y alguna información de control que los paquetes de datos sean adecuadamente encaminados.
IPng	Next Generation Internet Protocol
IPSEC	Protocolo de Seguridad IP
IPv6	Internet Protocol Version 6

IPX	**I**nternetwork **P**acket **E**xchange. Es un nivel (nivel 3) de protocolo de redes Novell que es similar al protocolo XNS (Xerox Network Systems) y al IP, y que es usado en las redes que usan software de Novell.
IRC	Internet Relay Chat
ISA	**I**ndustry **S**tandard **Ar**chitecture. Arquitectura Industrial estándar. Se refiere a la arquitectura original del Bus para PC de 16 bits.
ISDN	Servicios integrados de Red Digital
ISO	**I**nternational Standards Organization. Organización con sede en Ginebra que impulsa los estándares técnicos que incluyen el OSI (Open Systems Interconnect) para las comunicaciones a nivel mundial.
ISO 9000	Es un juego de estándares internacionales de administración de la calidad definida por ISO (International Standards Organization). Estos estándares, que no pertenecen a un país, industria o producto especifico, permite a las compañías que lo acreditan, poder afirmar que cuentan con procesos para mantener un sistema de calidad eficiente.
ISP	Proveedor de Servicio de Internet
KDE	Entorno de Desarrollo de LINUX
KERNEL	Núcleo del Sistema Operativo
L2F	Layer 2 Forwarding
LAC	Concentrador de Acceso
LAN	**L**ocal **A**rea **N**etwork. Red de área local. Red de comunicaciones que sirve a usuarios dentro de un área geográfica limitada.
LAN MANAGER	Sistema Operativo para redes de área local de Microsoft, que corre como una aplicación bajo OS/2 en un servidor y soporta las estaciones de trabajo en DOS, OS/2 y UNIX.
LCP	Link Control Protocol

LNS	L2TP Server Network
LPCD	Línea Privada de Comunicación de Datos
MAC	Control de Acceso al Medio. Es un recipiente de los controladores.
MAN	**M**etropolitan **A**rea **N**etwork. Red de Area Metropolitana. Red de comunicaciones que cubre un área geográfica como una ciudad.
MODEM	**MO**dulator - **DEM**odulator. Dispositivo que adapta una terminal o computador personal a una línea telefónica. Convierte las pulsaciones digitales del computador en audio-frecuencias y vuelve a convertir éstas en pulsaciones en el lado receptor.
MySQL	Base de Datos con publicaciones tanto para Windows como para Linux, bajo Licencia o sin Licencia.
NAME SERVER	Es un servicio que se provee en la red para la conversión de los nombres de una red (usuarios, computadoras, impresoras o servicios) en direcciones de la red.
NCP	Network Control Protocols. Es el software de control que se ejecuta en el procesador frontal. Una aplicación que actúa fundamentalmente como un sistema operativo de entrada/salida. Gestiona todos los datos que llegan de y salen a una red.
NOS	Network Operating System
OPEN SOURCE	Fuente Abierta
OSI	International Organization for Standarization
PAP	Protocolo de Autentificación de Contraseña
PAQUETE	Ver Trama.
PASARELA	Un computador u otro dispositivo que actúa como traductor entre dos sistemas que no utilizan los mismos protocolos de comunicación.
PASARELA LAN	Proporciona un trayecto para los datos que fluyen de una LAN a otra a través de una LAN intermedia.

PBX	Central de Ramificación Privado
PDU	Unidad de Datos del Protocolo
PILA DE PROTOCOLOS	Define como los fabricantes pueden crear productos que trabajen con los productos de otros fabricantes.
PILA DE PROTOCOLOS OSI	Define la pila de protocolos para promover la interoperatividad a nivel mundial.
PING	Protocolo que se usa en el entorno del Protocolo de control de transmisión para probar si un nodo o dispositivo remoto se comunica en redes de área local o redes de área extensa.
PLATAFORMA	Un entorno de Sistema Operativo. Un sistema de computadora basado en un procesador especifico.
PMVision	Software Para el Ingreso de Comando en el RAS
PORTMASTER	Equipo de Acceso Remoto
PPP	Protocolo Punto Punto
PPTP	Protocolo de Tunel Punto Punto
PRI	Interfase de programación primaria
PROCESAMIENTO AUTOMATICO DE DATOS	Se define como la actividad de captura, almacenamiento, actualización, transformación, generación y recuperación de datos por medios computacionales.
PROGRAMA LIBRE	Libre de Licencia
PROGRAMACION	Se define como el proceso de creación de un programa de computadora, mediante la aplicación de procedimientos lógicos mediante los siguientes pasos:
PROTOCOLO	Reglas de Comunicación. Es un modo definido de comunicación con otro sistema. Especifica la sincronización de las señales y la estructura de datos comunicados.
PROTOCOLO IP	Protocolo de comunicación sin conexión que por si mismo proporciona un servicio de datagramas.
PROTOCOLO TCP	Protocolo de control de transmisión que establece una conexión duplex entre dos sistemas mediante la

	utilización de una interfaz de conectores.
PVC	Circuito Virtual Permanente
RACSA	Telepuerto
RADIUS	Remote Authentication Dial-In User Service. Protocolo de autentificación y registro de los usuarios a un sistema.
RAS	Servidor de Acceso Remoto
RDI	Red Digital Integrada
RED PRIVADA DE DATOS	Consiste en un equipo de conmutación y de comunicación que es propiedad de una organización interconectada mediante lineal de comunicaciones alquiladas o propias.
RED PUBLICA DE DATOS	Se ocupan las compañías de telecomunicaciones, sea o no de valor añadido.
REDES	Sistema de comunicaciones de datos que enlaza dos o más computadoras y dispositivos periféricos.
RENDIMIENTO	Constituye una medida de la velocidad de transferencia de datos para una computadora o un sistema de comunicación de datos.
SA	Asociación de Seguridad
SDSL	Línea de Abonados Digital Simétrica
SEGMENTO DE RED	Es un cable lineal terminado por los dos extremos. Las señales transmitidas por un segmento se escuchan en todas las estaciones que estén conectadas a el.
SEGURIDAD	Medidas de resguardo contra el acceso no autorizado a los datos. Los programas y datos se pueden asegurar entregando números de identificación y contraseñas a los usuarios autorizados de una computadora.

SERVICIO INFORMATICO	Conjunto de actividades (planeamiento, análisis, diseño, programación, operación, entrada de datos, autoedición, bases de datos, etc.) asociadas al manejo automatizado de la información que satisfacen las necesidades de los usuarios de éste recurso.
SISTEMA DE INFORMACION	Se denomina Sistema de Información al conjunto de procedimientos manuales y/o automatizados que están orientados a proporcionar información para la toma de decisiones.
SISTEMA EN LINEA (ON-LINE)	Se refiere a un sistema operativo con terminales, sin implicar su modo de operación.
SLIP	Serial Line IP
SMTP	Simple Mail Transfer Protocol
SO	Sistema Operativo
TDT	TV Digital Terrestre
USUARIO	Cualquier persona que utiliza una computadora. Por lo general se refiere a las personas que no pertenecen al personal técnico y que proporcionan entradas y reciben salidas de la computadora.
VPN	Redes Privadas virtuales
VSAT	Very Small Apertura Terminal
WAN	Red de Area Extendida. Es una red con proporciones potencialmente globales. Si se emplean facilidades públicas, una WAN involucra compañías de telecomunicaciones para el intercambio local.
WWW	World Wide Web
xDSL	Tecnología para la transmisión de datos a alta velocidad.

9. 6. ANEXOS

Los anexos se encuentran en el CD adjunto.

9. 6. 1. ANTEPROYECTO DE TESIS

9. 6. 2. MANUAL DE USUARIO (TARNET)

9. 6. 3. MANUAL PHP

9. 6. 4. MANUAL HTML

9. 6. 5. MANUAL MYSQL

9. 7. ÍNDICE GENERAL

CAP. I

1. 1. REALIDAD ACTUAL DE LOS SERVICIOS DE INTERCONECTIVIDAD. ..... - 4 -

1. 1. 1. Orígenes De La Interconectividad ..... - 4 -

1. 1. 2. Conceptos De Interconectividad ..... - 5 -

1. 1. 3. Problemas De La Interconectividad ..... - 5 -

1. 1. 4. Actualidad De Los Servicios De Interconectividad ..... - 6 -

1. 1. 5. Futuro De La Interconectividad ..... - 8 -

1. 2. COMPORTAMIENTO DE LOS PROVEEDORES DE SERVICIOS DE INTERNET ..... - 13 -

1. 2. 1. Isp Y La Arquitectura De Internet ..... - 13 -

1. 2. 2. Isp En Los Negocios ..... - 15 -

1. 2. 3. Isp Y Aplicaciones Empresariales En Internet ..... - 16 -

CAP. II

2. 1. CONCEPTOS Y TERMINOLOGIA. ..... - 23 -

2. 1. 1. Estaciones De Trabajo Y/O Clientes ..... - 24 -

2. 1. 2. Servidores ..... - 24 -

2. 1. 3. Tarjetas De Interfaz De Red ..... - 24 -

2. 1. 4. Equipos De Conectividad ..... - 25 -

2. 2. FUNCIONES DE LOS ELEMENTOS ACTIVOS ..... - 30 -

2. 2. 1. Introducción ..... - 30 -

2. 2. 2. Modem ..... - 30 -

2. 2. 3. Router ..... - 30 -

2. 2. 4. Switch ..... - 32 -

2. 2. 5. Pbx ..... - 33 -

2. 2. 6. Pull De Modems ..... - 34 -

2. 2. 7. Portmaster (Acceso Remoto) ..... - 35 -

2. 3. TECNOLOGÍAS DE TRANSMISIÓN PARA ACCEDER A UN ISP ..... - 35 -

2. 3. 1. Introducción ..... - 35 -

2. 3. 2. Tipos De Acceso A Internet ..... - 36 -

2. 4. COMO ACCEDE UN USUARIO A UN ISP ..... - 42 -

2. 4. 1. ¿Qué Tipos De Planes Existen? ..... - 43 -

2. 4. 2. ¿Cómo Es Que Mi Computador Recibe Información Desde La Red Mundial Internet? ..... - 44 -

2. 4. 3. Pero… ¿Qué Información Se Transfiere? ..... - 44 -

CAP. III

3. 1. DEFINICIONES ..... - 47 -

3. 1. 1. Introducción ..... - 47 -

3. 1. 2. Protocolo ..... - 48 -

3. 1. 3. Características ..... - 51 -

3. 1. 4. Funciones ..... - 53 -

3. 2. PROTOCOLOS TCP/IP (IPV4 VS IPV6) ..... - 56 -

3. 2. 1. Introducción ..... - 57 -

3. 2. 2. ¿Qué Es El Ipv6? ..... - 57 -

3. 2. 3. Diferencias De Ipv6(Ipng) Vs Ipv4(Tcp/Ip) ..... - 57 -

3. 3. PROTOCOLOS EN LA TARIFACIÓN ..... - 61 -

3. 3. 1. Protocolo Ppp ..... - 65 -

3. 3. 2. Protocolo De Interfaz De Línea Serie (Slip) ..... - 71 -

3. 3. 3. Protocolo Tunneling Nivel 2 (L2tp) ..... - 73 -

3. 3. 4. Protocolo De Control De Enlace (Lcp) ..... - 76 -

3. 3. 5. Point-To-Point Tunneling Protocol (Pptp) ..... - 81 -

3. 3. 6. Protocolo De Seguridad Ip (Ipsec) ..... - 88 -

3. 3. 7. Protocolo Chap ..... - 95 -

3. 3. 8. Protocolo Pap ..... - 97 -

3. 4. NOTA ..... - 98 -

CAP. IV

4. 1. INTRODUCCIÓN ..... - 101 -

4. 2. HERRAMIENTAS Y OPERABILIDAD ..... - 102 -

4. 2. 1. Gestión De Autentificación De Usuarios ..... - 102 -

4. 2. 2. Gestión De Configuraciones ..... - 104 -

4. 2. 3. Gestión De Rendimiento ..... - 108 -

4. 2. 4. Gestión De Estadísticas ..... - 109 -

4. 2. 5. Gestión De Seguridades ..... - 109 -

4. 2. 6. Gestión De Velocidades ..... - 115 -

4. 2. 7. Gestión De Paridades ..... - 116 -

4. 2. 8. Gestión De Direccionamiento Dinámico (Dhcp) ..... - 119 -

CAP. V

5. 1. INTRODUCCIÓN ..... - 121 -

5. 1. 1. Clasificación De Sistemas Operativos ..... - 121 -

5. 2. CARACTERÍSTICAS ..... - 125 -

5. 3. FACILIDADES ..... - 130 -

5. 3. 1. Linux ..... - 130 -

5. 3. 2. Windows ..... - 131 -

5. 4. VENTAJAS / DESVENTAJAS ..... - 132 -

5. 4. 1. Linux ..... - 133 -

5. 4. 2. Windows ..... - 133 -

CAP. VI

6. 1. INTRODUCCIÓN ..... - 137 -

6. 2. CARACTERÍSTICAS ..... - 137 -

6. 3. LENGUAJES DE PROGRAMACIÓN VISUAL ..... - 138 -

6. 3. 1. C++ (Kdevelop) ..... - 138 -

6. 3. 2. Delphi (Kylix) ..... - 138 -

6. 3. 3. Php (Kdevelop) ..... - 140 -

6. 4. BASES DE DATOS EN LINUX ..... - 142 -

6. 4. 1. Mysql Como Motor De Base Se Datos ..... - 142 -

CAP. VII

7. 1. INTRODUCCIÓN ..... - 145 -

7. 2. ESTUDIO DE RADIUS ..... - 145 -

7. 2. 1. Características ..... - 145 -

7. 3. VENTAJAS Y DESVENTAJAS ..... - 148 -

7. 4. SOPORTE ..... - 151 -

7. 4. 1. Funciones De Radius ..... - 151 -

7. 4. 2. Arquitectura Radius En Una Red Ip (Isp) ..... - 155 -

7. 4. 3. Requisitos De Servidores ..... - 158 -

7. 5. VERSIONES ..... - 166 -

7. 5. 1. Instalación Del Servidor Radius ..... - 167 -

CAP. VIII

8. 1. INTRODUCCIÓN ..... - 172 -

8. 2. INVESTIGACIÓN PRELIMINAR ..... - 172 -

8. 2. 1. Como Funciona ..... - 172 -

8. 2. 2. Determinación De Los Requerimientos ..... - 176 -

8. 2. 3. Estudio De Factibilidad ..... - 177 -

8. 2. 4. Diseño Del Sistema ..... - 178 -

8. 2. 5. Desarrollo Del Sistema ..... - 181 -

CAP. IX

9. 1. VERIFICACIÓN DE LA HIPÓTESIS ..... - 190 -

9. 2. CONCLUSIONES ..... - 195 -

9. 3. RECOMENDACIONES ..... - 196 -

9. 4. BIBLIOGRAFÍA ..... - 197 -

9. 5. GLOSARIO ..... - 199 -

9. 6. ANEXOS ..... - 212 -

9. 6. 1. Anteproyecto De Tesis ..... - 212 -

9. 6. 2. Manual De Usuario (Tarnet) ..... - 212 -

9. 6. 3. Manual Php ..... - 212 -

9. 6. 4. Manual Html ..... - 212 -

9. 6. 5. Manual Mysql ..... - 212 -

9. 7. ÍNDICE GENERAL ..... - 213 -

9. 8. INDICE DE FIGURAS ..... - 220 -

9. 9. INDICE DE TABLAS ..... - 223 -

9. 8. INDICE DE FIGURAS

Cap. I

FIGURA 1.1 USUARIOS CONECTADOS A INTERNET EN ECUADOR ..... - 2 -

FIGURA 1.2 DATOS DEL NÚMERO DE USUARIOS EN EL MUNDO DE INTERNET ..... - 3 -

FIGURA 1.3 ARQUITECTURA RACSA ..... - 9 -

FIGURA 1.4 ARQUITECTURA INTERNET ..... - 14 -

Cap. II

FIGURA 2.1 HARDWARE DE CONECTIVIDAD ..... - 23 -

FIGURA. 2.1 CONJUNTO DE EQUIPOS DE INTERCONECTIVIDAD ..... - 26 -

FIGURA. 2.2 TIPOS DE CONEXIÓN A INTERNET ..... - 37 -

FIGURA 2.3 ACCESO A UN ISP ..... - 43 -

FIGURA. 2.4 INTERCONEXIÓN DE ISPS ..... - 45 -

Cap. III

FIGURA 3.1. ARQUITECTURA PROTOCOLOS DE COMUNICACIÓN ..... - 48 -

FIGURA 3.2 ENCAPSULADO ..... - 54 -

FIGURA 3.3. FORMATO DE LA CABECERA DE IPV6 ..... - 59 -

FIGURA 3.4 PROTOCOLOS EN LA TARIFACIÓN ..... - 64 -

FIGURA 3.5. FORMATO DE TRAMA DEL PROTOCOLO PUNTO A PUNTO. ..... - 67 -

FIGURA 3.6. PILA DE PROTOCOLOS PUNTO A PUNTO. ..... - 68 -

FIGURA 3.7. CONEXIONES SLIP. ..... - 73 -

FIGURA 3.8 FORMATO DE UN PAQUETE ..... - 78 -

FIGURA 3.9 FORMATO DE UN DATAGRAMA ..... - 84 -

FIGURA 3.10. ENCAPSULACIÓN PPTP ..... - 85 -

FIGURA 3.11. REGISTRO DE SOLICITUDES Y RESPUESTAS ..... - 86 -

FIGURA 3.12. PROTECCIÓN DE TRANSFERENCIA DE DATOS. ..... - 89 -

FIGURA 3.13. COMPROBACIÓN DE PAQUETES. ..... - 91 -

FIGURA 3.14. ASEGURAMIENTO DE COMUNICACIONES ..... - 93 -

FIGURA 3.15. PROTECCIÓN DE INFORMACIÓN ENTRE DIVERSOS ..... - 94 -

FIGURA 3.16. CHALLENGE HANDSHAKE DE PPP. ..... - 96 -

Cap. VII

FIGURA 7.1 ESQUEMA DE FUNCIONES DE RADIUS ..... - 152 -

FIGURA 7.2 ARQUITECTURA DE SERVIDOR RADIUS ..... - 156 -

Cap. VIII

FIGURA 8.1 ARQUITECTURA DE TARNET ..... - 180 -

FIGURA 8.2 DIAGRAMA DE CASOS DE USO ..... - 183 -

FIGURA 8.3 DIAGRAMA DE ACTIVIDADES ..... - 186 -

Cap. IX

FIGURA 9.1 COMPROBACIÓN ALTERNATIVA 1 ..... - 191 -

FIGURA 9.2 COMPROBACIÓN ALTERNATIVA 2 ..... - 192 -

9. 9. INDICE DE TABLAS

Cap. II

TABLA 2.1 NOMENCLATURA DE EQUIPOS DE INTERCONECTIVIDAD. ..... - 27 -

Cap. IV

TABLA 4.1 OPCIONES DE UN FILTRO ..... - 113 -

TABLA 4.2 OPCIONES DE PARIDAD ..... - 118 -

Cap. V

TABLA 5.1 COMPARACIÓN DE PLATAFORMAS ..... - 130 -

Cap. VIII

TABLA 8.1 DETALLE DE ARCHIVO DETAIL..... - 175 -

TABLA 8.1 DESCRIPCIÓN CASOS DE USO..... - 184 -

Cap. IX

TABLA 9.1 COMPROBACIÓN ALTERNATIVA 1 ..... - 191 -

TABLA 9.2 COMPROBACIÓN ALTERNATIVA 2 ..... - 192 -