UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES E INFORMÁTICOS

Seminario de Graduación "Proyectos de Conectividad y Redes de Comunicación, Administración de Redes y Servicios, Seguridad Industrial, Normativas de Calidad y Automatización Robótica (Mecatrónica)"

TEMA

Aplicación de un software de tipo hotspot con autenticación LDAP para administrar el tiempo de acceso a Internet en la Biblioteca de la Facultad de Ingenierías en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato.

Proyecto de Investigación, presentado previo a la obtención del título de Ingeniero en Sistemas Computacionales e Informáticos.

AUTOR: ÁNGEL ROBERTO MAYORGA ZAMBRANO

TUTOR: ING. DAVID GUEVARA AULESTIA

AMBATO – ECUADOR

Septiembre 2009

APROBACIÓN DEL TUTOR

En mi calidad de tutor del trabajo de investigación sobre el tema: **Aplicación de un software de tipo hotspot con autenticación LDAP para administrar el tiempo de acceso a Internet en la Biblioteca de la Facultad de Ingenierías en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato**, de Ángel Roberto Mayorga Zambrano, estudiante de la Carrera de Ingeniería en Sistemas Computacionales e Informáticos, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, considero que el informe investigativo reúne los requisitos suficientes para que continúe con los trámites y consiguiente aprobación de conformidad con el Artículo 45 del Capítulo III Seminarios, del Reglamento de Graduación de Pregrado de la Universidad Técnica de Ambato.

Ambato, septiembre 14 de 2009

EL TUTOR

_____

Ing. David Guevara Aulestia

AUTORÍA

El presente trabajo de investigación titulado: **Aplicación de un software de tipo hotspot con autenticación LDAP para administrar el tiempo de acceso a Internet en la Biblioteca de la Facultad de Ingenierías en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato**. Es absolutamente original, auténtico y personal, en tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, septiembre 14 de 2008

_____

Ángel Roberto Mayorga Zambrano
C.C.: 1711245587

ÍNDICE GENERAL DE CONTENIDOS

ÍNDICE DE GRÁFICOS

ÍNDICE DE FIGURAS

RESUMEN EJECUTIVO

Se presenta a consideración los resultados de la investigación cuyo propósito principal fue elaborar la propuesta de aplicación de un software de tipo hotspot con autenticación LDAP para administrar el tiempo de acceso a Internet en la Biblioteca de la Facultad de Ingenierías en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato.

En este trabajo se investigó la variable independiente: software de tipo hotspot con autenticación LDAP, y la dependiente: administración de tiempo de acceso a internet.

La técnica de recolección de datos fue la observación directa. Los resultados de la aplicación de los instrumentos fueron analizados cuantitativamente y porcentualmente y se los representa mediante gráficos.

Del análisis de los resultados se obtuvieron las conclusiones del trabajo de investigación. Se propuso la aplicación de una solución software que permita administrar el tiempo de acceso a internet en la Biblioteca de la FISEI-UTA.

La propuesta está constituida por una metodología de aplicación que contiene 4 objetivos sobre los cuales se desarrolló los contenidos permitiendo el análisis de los tiempos de ingreso y salida del servicio de internet de la Biblioteca de la Facultad.

CAPÍTULO 1
EL PROBLEMA

1 EL PROBLEMA

1.1 TEMA

Aplicación de un software de tipo hotspot con autenticación LDAP para administrar el tiempo de acceso a Internet en la Biblioteca de la Facultad de Ingenierías en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato.

1.2 PLANTEAMIENTO DEL PROBLEMA

1.2.1 CONTEXTUALIZACIÓN

Básicamente, Internet es una interconexión de redes informáticas que permite a las computadoras conectadas comunicarse directamente. El término suele referirse a una interconexión en particular, de carácter mundial y abierto al público, que conecta redes informáticas de organismos oficiales, educativos y empresariales, ésta referencia se suele identificar al encontrarse con mayúscula.

Administrar el acceso a Internet de forma eficiente para fomentar su aprovechamiento con fines didácticos o científicos, constituye una prioridad en la "Sociedad de la Información", en la cual la creación, distribución y manipulación de la información, principalmente a través de las TIC's, constituyen parte importante de las actividades culturales y económicas. Un Hotspot es una de las maneras más popularizadas de ofrecer y acceder al servicio de Internet, generalmente en aeropuertos, bibliotecas, cafeterías, hoteles, y otros sitios públicos, a través de una conexión WIFI. Sin embargo el software destinado a controlar este servicio se ha ido extendiendo a entornos que comprenden también conexiones alámbricas para ofrecer una mayor flexibilidad a los administradores.

Si bien en muchos países la utilización del Internet en la educación es incentivada al punto de ser un servicio gratuito, en el Ecuador, pese a los recientes decrementos en su costo, gran parte de las instituciones educativas se ven obligadas a hacer que los estudiantes deban cubrir sus consumos.

Los métodos utilizados en el Ecuador para determinar el tiempo que una persona utiliza Internet, y el costo que implica el mismo, en lugares públicos han evolucionado lentamente; podemos visualizar dos perspectivas: pos pago (como en cibercafés) y prepago (como en bibliotecas). Bajo la primera de ellas se puede decir que inicialmente se realizaba de forma completamente manual, anotando la

hora de ingreso y salida, calculando los minutos, y revisando en una tabla de precios; actualmente se utilizan programas que realizan estas tareas de forma semiautomática ya que debe existir al menos persona a cargo del "desbloqueo" del equipo que va a ser utilizado. En el caso de la segunda perspectiva nos el acceso se ha venido controlando a través de tarjetas de prepago (similares a las utilizadas en restaurantes por los comensales), es decir, piezas de cartulina en las que deben ser tachados o picados ciertos indicadores de consumo que no permiten realizar un seguimiento exacto.

Por otro lado en los establecimientos en los cuales se ofrece acceso inalámbrico a Internet (centros comerciales, convenciones, hoteles, y aeropuertos) el control es prácticamente nulo ya que dicho acceso es gratuito, requiriendo cuando mucho alguna clase de registro o configuración específica, razón por la cual no se ha popularizado el concepto de Hotspot.

En la Biblioteca de la Facultad de Ingenierías en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato (FISEI–UTA) el personal se encarga tanto de las tareas propias de su cargo como préstamo y recepción de libros y demás tareas específicas, como de la de recepción de carnets y tarjetas de Internet de los alumnos y control del tiempo utilizado, lo cual ocasiona situaciones conflictivas tanto a los estudiantes como a las personas que se encuentran a cargo de este servicio.

Aunque simultáneamente se ofrece conexión inalámbrica a quienes poseen un computador portátil, el costo de estos equipos aún no permite que se pueda convertir en una solución a la gran demanda de información proveniente del ciberespacio por parte del alumnado.

1.2.2 ANÁLISIS CRÍTICO

Se ha considerado que la forma actual de controlar el tiempo de acceso a Internet en la Biblioteca de la FISEI–UTA resulta inadecuado debido a varias razones entre las cuales podemos contemplar que:

- el registro de los estudiantes que desean hacer uso del servicio es manual;
- la medición del tiempo no se realiza de forma automática, lo cual conlleva aproximaciones que pueden beneficiar o perjudicar tanto al estudiante como a la Universidad, es decir, el estudiante pagó por un tiempo de uso y espera utilizarlo por completo, y a su vez la Universidad necesita llevar un control estricto y exacto de los minutos de acceso;

- parte del personal de Biblioteca no está adecuadamente capacitado, sus conocimientos no están orientados a la administración de redes de computadores o de servicios computacionales;
- existe desatención de las autoridades, principalmente porque al problema no se le presta la importancia que se merece.

Como consecuencias de la situación planteada se puede afirmar que existe:

- desperdicio de tiempo para acceder al servicio ya que en horas pico hay gran cantidad de estudiantes pugnando por usar un computador y solamente un bibliotecario para atenderlos a todos;
- desperdicio de tiempo del personal al encargarse de diferentes tareas, en similares horas pico pueden encontrarse alumnos que requieren uno o varios libros para realizar consultas o investigaciones, y al mismo tiempo los alumnos que desean utilizar los computadores;
- inconformidad de los usuarios (en este caso los estudiantes);
- posibilidad de que se presenten preferencias a personas específicas, potencialmente basadas en afinidad entre el personal y el estudiantado; riesgo de que, en determinadas circunstancias, se omitiera el "tachado" de las tarjetas.

1.2.3 PROGNOSIS

En la eventualidad de no tomar medidas correctivas al respecto de la situación se puede desembocar en: pérdida de usuarios que no se sientan satisfechos con el servicio, que inclusive pudieran convertirse en reclamos puesto que están en su derecho de exigir algo por lo que han pagado; pérdidas económicas, partiendo del hecho de que según la nueva constitución la educación superior es gratuita y ninguna universidad puede exigir la adquisición de un servicio por parte de los alumnos; malestar en el personal, al verse involucrado en temas para los cuales no se encuentran plenamente capacitados; pérdida de prestigio puesto que la FISEI debería ser una muestra de eficiencia, automatización y sistematización de todas las tareas.

Por lo tanto, se hace necesaria la aplicación de un software de tipo hotspot apoyándose en la confiabilidad y seguridad de una autenticación LDAP (*Lightweight Directory Access Protocol*, o Protocolo Ligero de Acceso a Directorios) para administrar el tiempo de acceso a Internet en la Biblioteca de la FISEI–UTA de forma eficiente y equitativa.

1.2.4 FORMULACIÓN DEL PROBLEMA

¿Cuál es la forma más adecuada de aplicar un software de tipo hotspot con autenticación LDAP para administrar de tiempo de acceso a Internet en la Biblioteca de la Facultad de Ingenierías en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato?

1.2.5 INTERROGANTES

1.2.5.1 ¿Qué características tiene el uso de Internet en la Biblioteca de la FISEI–UTA?

1.2.5.2 ¿Qué herramienta software de tipo hotspot es la más apropiada para ser aplicada?

1.2.5.3 ¿Qué implementación de LDAP es la más adecuada para el caso?

1.2.5.4 ¿Qué características deben cumplir los equipos clientes y el servidor para utilizar el software de tipo hotspot y la implementación LDAP a aplicarse?

1.2.5.5 ¿Qué ventajas ofrece la aplicación de un software de tipo hotspot con autenticación LDAP a la administración de tiempo de acceso a Internet en la Biblioteca de la FISEI–UTA?

1.2.5.6 ¿Cómo se realizaría la configuración del software de tipo hotspot y de la implementación de LDAP para cumplir la función requerida?

1.2.6 DELIMITACIÓN DEL OBJETO DE INVESTIGACIÓN

La presente investigación está orientada a la aplicación de un software de tipo hotspot con autenticación LDAP para administrar el tiempo de acceso a Internet en la Biblioteca de la Facultad de Ingenierías en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato, con un período de duración de 5 meses iniciándose en el mes de noviembre de 2008 y extendiéndose hasta el 30 de marzo de 2009; como población se trabajará con el personal de la Biblioteca.

1.3 JUSTIFICACIÓN

La presente investigación referente al servicio de Internet ofrecido en la Biblioteca de la FISEI–UTA, busca corregir y mejorar la administración del tiempo de acceso a Internet por parte de los estudiantes.

El mejoramiento y automatización de la administración del tiempo de acceso a Internet en la Biblioteca de la FISEI–UTA son muy importantes porque a permiten incrementar la eficiencia y calidad de dicho servicio, colocando a la Facultad a la vanguardia de la administración de servicios de Internet.

Los beneficiarios del proyecto de investigación serán los estudiantes de la FISEI y la Universidad Técnica de Ambato porque, adicionalmente la experiencia adquirida puede ser empleada para extender dichas ventajas a las bibliotecas de las otras facultades de la Universidad Técnica de Ambato.

Este es un proyecto factible de realizarse por se dispone de los conocimientos necesarios durante la carreras , de las experiencias vividas por los estudiantes, así como del personal especializado para el asesoramiento del trabajo y la información necesaria proporcionada por la Facultad de Ingeniería en Sistemas Electrónica e Industrial.

1.4 OBJETIVOS

1.4.1 GENERAL

Diseñar la aplicación de un software de tipo hotspot con autenticación LDAP para administrar el tiempo de acceso a Internet en la Biblioteca de la Facultad de Ingenierías en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato.

1.4.2 ESPECÍFICOS

1.4.2.1 Determinar las características del uso de Internet en la Biblioteca de la FISEI–UTA.

1.4.2.2 Definir la herramienta software de tipo hotspot más apropiada para ser aplicada.

1.4.2.3 Establecer la implementación de LDAP más adecuada para el caso.

1.4.2.4 Describir las características que deben cumplir los equipos clientes y servidor para utilizar el software de tipo hotspot y la implementación LDAP que se aplicarán.

1.4.2.5 Especificar las ventajas que ofrece la aplicación de un software de tipo hotspot con autenticación LDAP a la administración de tiempo de acceso a Internet en la Biblioteca de la FISEI–UTA.

1.4.2.6 Explicar el procedimiento de configuración del software de tipo hotspot y de la implementación de LDAP para cumplir la función requerida.

CAPÍTULO 2
MARCO TEÓRICO

2 MARCO TEÓRICO

2.1 ANTECEDENTES INVESTIGATIVOS

Una vez revisados los archivos de la Facultad de Ingenierías en Sistemas, Electrónica e Industrial se detecta que aún no existen trabajos similares de investigación en la Biblioteca de dicha entidad.

Sin embargo en los archivos del Centro de Posgrados existe un trabajo sobre el tema "Autenticación de redes inalámbricas usando software libre" realizado por el Ing. David Guevara Aulestia cuyas conclusiones se refieren a que con la utilización de herramientas de software libre se puede ofrecer un servicio de acceso a redes inalámbricas seguro y confiable, inclusive por niveles superiores al ofrecido por software propietario de alto costo, las cuales serán tomadas en cuenta para el presente trabajo investigativo.

2.2 FUNDAMENTACIÓN LEGAL

Universidad Técnica de Ambato

La Universidad Técnica de Ambato se crea mediante Ley Nº 69-05 del 18 de abril de 1969, como una comunidad de profesores, estudiantes y trabajadores.

Facultad de Ingenierías en Sistemas, Electrónica e Industrial

Resolución Nº 347-91-CU-P, 14 de agosto de 1991:

Consejo Universitario en sesión ordinaria efectuada el día martes 13 de agosto de 1991, visto el Acuerdo Nº 090-CAU-UTA con fecha 12 de agosto de 1991, resolvió:

- De conformidad con el Artículo 15, Literal b) del Estatuto Universitario Vigente, se crea la carrera de Licenciatura en Informática y Computación en base al proyecto elaborado por Administración Central.
- La Escuela de Informática y Computación funcionará transitoriamente adscrita a Administración Central, bajo la modalidad de Semestres Discontinuos, a partir de la fecha de resolución.

Resolución Nº 386-92-CU-P, 4 de agosto de 1992:

Consejo Universitario en sesión ordinaria del día martes 4 de agosto de 1992, visto el Acuerdo Nº 098-CAU-UTA con fecha 4 de agosto de 1992, resolvió:

- Aprobar el Proyecto de la Carrera de Ingeniería de Sistemas preparado por la comisión presidida por el Ing. Washington Medina, Director de la Escuela de Informática y Computación, con la asesoría del Dr. José Antonio Días Batista, Decano de la Facultad de Ingeniería Industrial del ISPJAE.
- Los organismos de gobierno de la nueva facultad se estructurarán en el plazo de un año. Mientras tanto funcionará como hasta la fecha con el Director de Escuela encargado.
- En el plazo de 60 días, una comisión especial designada por el Señor Rector redactará la correspondiente reglamentación, para someter a la aprobación del H. Consejo Universitario.
- Para el año de 1993 se hará constar el presupuesto de la nueva facultad.

Resolución Nº 804-98-CU-P, 20 de octubre de 1998:

Consejo Universitario en sesión ordinaria efectuada el día martes 20 de octubre de 1998, visto el Acuerdo CAU-P-205-98 con fecha 13 de octubre de 1998, resolvió:

- Aprobar el Proyecto de Reestructuración Académica de la Facultad de Ingeniería en Sistemas, de conformidad con el documento adjunto.

Resolución Nº 837-2002-CU-P, 11 de junio de 2002:

Consejo Universitario en sesión ordinario del día martes 11 de junio de 2002, visto el oficio CAP-P-239-2002 con fecha 3 de junio de 2002, resolvió:

- Aprobar los mapas curriculares reformados de la Facultad de Ingeniería en Sistemas de las carreras de Ingeniería en Sistemas Computacionales e Informáticos, Ingeniería Electrónica y Comunicaciones; e Ingeniería Industrial en Procesos de Automatización; de conformidad con los cuadros adjuntos.

Resolución Nº 0006-CU-P-2007, 3 de enero de 2007:

El Honorable Consejo Universitario de la Universidad Técnica de Ambato en sesión ordinaria efectuada el miércoles 3 de enero de 2007, visto el Acuerdo CAU-P-583-2006 con fecha 18 de diciembre de 2006, resolvió:

- Aprobar el Proyecto de Reforma Curricular de las Carreras de Ingeniería en Sistemas Computacionales e Informáticos, Ingeniería Electrónica y Comunicaciones, Ingeniería Industrial en Procesos de Automatización de la Facultad de Ingeniería en Sistemas, con vigencia a partir del Ciclo Académico marzo-agosto 2007, planteado a través de la Optimización del tiempo de duración de las Carreras con la eliminación del Décimo Primer Semestre del Pensum Intermedio, del Décimo Semestre del Pensum nuevo, y la reubicación de los Seminarios de Desarrollo de los Perfiles de Proyectos de Graduación y Emprendimiento, sin afectar al Perfil Profesional aprobado; Reforma Curricular que tiene el visto bueno del Centro de Desarrollo de la Docencia (CEDED).

2.3 CATEGORÍAS FUNDAMENTALES

Internet

Internet es un conjunto descentralizado de redes de comunicación interconectadas, que utilizan la familia de protocolos TCP/IP, garantizando que las redes físicas heterogéneas que la componen funcionen como una red lógica única, de alcance mundial. Sus orígenes se remontan a 1969, cuando se estableció la primera conexión de computadoras, conocida como ARPANET, entre tres universidades de California y una de Utah en Estados Unidos.

Uno de los servicios que más éxito ha tenido en Internet ha sido la World Wide Web (WWW o "la web"), hasta tal punto que es habitual la confusión entre ambos términos. La WWW es un conjunto de protocolos que permite, de forma sencilla, la consulta remota de archivos de hipertexto. Ésta se desarrollo posteriormente (1990) y utiliza Internet como medio de transmisión.

Existen, por tanto, muchos otros servicios y protocolos en Internet, aparte de la Web: el envío de correo electrónico (SMTP), la transmisión de archivos (FTP y P2P), las conversaciones en línea (IRC), la mensajería instantánea, la transmisión de contenido y comunicación multimedia (telefonía VoIP, televisión IPTV), los

boletines electrónicos (NNTP), el acceso remoto a otras máquinas (SSH y Telnet), juegos en línea, etc.

Estructura de Internet

Internet no es una red centralizada está regida por un solo organismo. Su estructura se parece a una tela de araña en la cual unas redes se conectan a otras.

No obstante hay una serie de organizaciones responsables de la adjudicación y el desarrollo de los protocolos necesarios para que Internet evolucione, por ejemplo:

- Internet Engineering Task Force (IETF) se encarga de redactar los protocolos usados en Internet.
- Corporación de Internet para los Nombres y los Números Asignados (ICANN) es la autoridad que coordina la asignación de identificadores únicos en Internet, incluyendo nombres de dominio, direcciones IP, etc.

Las direcciones en Internet

En Internet se emplean varios formatos para identificar máquinas, usuarios o recursos en general.

- Se emplean direcciones numéricas para identificar máquinas: las direcciones IP. Se representan por cuatro números, de 0 a 255, separados por puntos. Un servidor puede identificarse, por ejemplo, con la dirección IP 66.230.200.100. Como es más sencillo recordar un nombre, las direcciones se "traducen" a nombres. Los trozos "traducidos" se denominan nombres de dominio. El servicio encargado de la traducción es el DNS.
- Para identificar a usuarios de correo electrónico se emplean las *direcciones de correo electrónico*, que tienen el siguiente formato: usuario@servidor_de_correo.dominio.
- Para identificar recursos en Internet se emplean direcciones URL (*Uniform Resource Locator*, Localizador Uniforme de Recursos). Una dirección URL tiene la forma: *http://nombre_de_empresa.dominio/abc.htm*, siendo "http://" el protocolo, "nombre_de_empresa.dominio" el dominio (que es trasladado a una dirección IP por el servicio DNS), y "abc.htm" la localización del recurso al que se accede.

El flujo de información en Internet

La arquitectura cliente-servidor

El procedimiento empleado para intercambiar información en Internet sigue el modelo cliente-servidor.

- Los servidores son computadoras donde se almacenan datos.
- El cliente es la computadora que realiza la petición al servidor para que éste le muestre alguno de los recursos almacenados.

Los paquetes de información

En Internet la información se transmite en pequeños trozos llamados "paquetes". Lo importante es la reconstrucción en el destino del mensaje emitido, no el camino seguido por los paquetes que lo componen.

Si se destruye un nodo de la red, los paquetes encontrarán caminos alternativos. Este procedimiento no es el más eficiente, pero resiste las averías de una parte de la red.

Protocolo TCP/IP

Para intercambiar información entre computadores es necesario desarrollar técnicas que regulen la transmisión de paquetes.

Dicho conjunto de normas se denomina protocolo. Hacia 1973 aparecieron los protocolos TCP e IP, utilizados ahora para controlar el flujo de datos en Internet.

- El protocolo TCP (y también el UDP), se encarga de fragmentar el mensaje emitido en paquetes. En el destino, se encarga de reorganizar los paquetes para formar de nuevo el mensaje, y entregarlo a la aplicación correspondiente.
- El protocolo IP enruta los paquetes. Esto hace posible que los distintos paquetes que forman un mensaje puedan viajar por caminos diferentes hasta llegar al destino.

Servicio de Nombres

Existe un servicio que se encarga de proporcionar la correspondencia entre una dirección IP y su nombre de dominio, y viceversa. Este servicio es el DNS (*Domain Name System*, Sistema de Nombres de Dominio).

Cada vez que se inicia una comunicación con un nombre de dominio, el ordenador realiza una petición a su servidor DNS para que le proporcione la IP asociada a ese nombre.

El sistema DNS es jerárquico. Cada subdominio de Internet suele tener su propio servidor DNS, responsable de los nombres bajo su dominio. A su vez, hay un servidor encargado de cada dominio (por ejemplo un nivel nacional [.ec]), y hay una serie de servidores raíz, que *conocen* toda la estructura DNS superior.

Conexión a Internet

RTC

La Red Telefónica Conmutada (RTC), también llamada Red Telefónica Básica, es la red original y habitual (analógica). Por ella circulan habitualmente las vibraciones de la voz, las cuales son traducidas en impulsos eléctricos que se transmiten a través de dos hilos de cobre. A este tipo de comunicación se denomina *analógica*. La señal del ordenador, que es digital, se convierte en analógica a través del modem y se transmite por la línea telefónica. Es la red de menor velocidad y calidad.

La conexión se establece mediante una llamada telefónica al número que le asigne su proveedor de Internet. Este proceso tiene una duración mínima de 20 segundos. Puesto que este tiempo es largo, se recomienda que la programación de desconexión automática no sea inferior a 2 minutos. Su costo es el de una llamada local, aunque también hay números especiales con tarifa propia.

Para acceder a la Red sólo necesitaremos una línea de teléfono y un módem, ya sea interno o externo. La conexión en la actualidad tiene una velocidad de 56 Kbps (Kilo bits por segundo), y se realiza directamente desde un PC o en los centros escolares a través de router o proxy.

RDSI

La Red Digital de Servicios Integrados (RDSI) envía la información codificada digitalmente, por ello necesita un adaptador de red, modem o tarjeta RDSI que adecúa la velocidad entre el PC y la línea. Para disponer de RDSI hay que hablar con un operador de telecomunicaciones para que instale esta conexión especial que, lógicamente, es más cara pero que permite una velocidad de conexión digital a 64 Kbps en ambos sentidos.

El aspecto de una tarjeta interna RDSI es muy parecido a un modem interno para RTC.

La RDSI integra multitud de servicios, tanto transmisión de voz, como datos, en un único acceso de usuario que permite la comunicación digital entre los terminales conectados a ella (teléfono, fax, ordenador, etc.).

Sus principales características son:

- Conectividad digital punto a punto.
- Conmutación de circuitos a 64Kbps.
- Uso de vías separadas para la señalización y para la transferencia de información (canal adicional a los canales de datos).

La conexión RDSI divide la línea telefónica en tres canales: dos B o portadores, por los que circula la información a la velocidad de 64Kbps, y un canal D, de 16Kbps, que sirve para gestionar la conexión. Se pueden utilizar los dos canales B de manera independiente (es posible hablar por teléfono por uno de ellos y navegar por Internet simultáneamente), o bien utilizarlos de manera conjunta, lo que proporciona una velocidad de transmisión de 128Kbps. Así pues, una conexión que utilice los dos canales (Ej.: videoconferencia) supondrá la realización de dos llamadas telefónicas.

DSL

Digital Subscriber Line (Línea de abonado digital). Es un término utilizado para referirse de forma global a todas las tecnologías que proveen una conexión digital sobre línea de abonado de la red telefónica básica o conmutada: ADSL, ADSL2, ADSL2+, SDSL, IDSL, HDSL, SHDSL, VDSL, y VDSL2.

Tienen en común que utilizan el par trenzado de hilos de cobre convencionales de las líneas telefónicas para la transmisión de datos a gran velocidad.

La diferencia entre ADSL y otras DSL es que la velocidad de bajada y la de subida no son simétricas, es decir, que normalmente permiten una velocidad de bajada mayor que la de subida.

Cable

Normalmente se utiliza cable coaxial que también es capaz de conseguir tasas elevadas de transmisión pero utilizando una tecnología completamente distinta. En lugar de establecer una conexión directa, o punto a punto, con el proveedor de acceso, se utilizan conexiones multipunto, en las cuales muchos usuarios comparten el mismo cable.

Las principales consecuencias del uso de esta tecnología son:

- Cada nodo (punto de conexión a la Red) puede dar servicio a entre 500 y 2000 usuarios.
- Para conseguir una calidad óptima de conexión la distancia entre el nodo y el usuario no puede superar los 500 metros.
- No se pueden utilizar los cables de las líneas telefónicas tradicionales para realizar la conexión, siendo necesario que el cable coaxial alcance físicamente el lugar desde el que se conecta el usuario.
- La conexión es compartida, por lo que a medida que aumenta el número de usuarios conectados al mismo nodo, se reduce la tasa de transferencia de cada uno de ellos.

Esta tecnología puede proporcionar una tasa de 30Mbps de bajada como máximo, pero los módems normalmente están fabricados con una capacidad de bajada de 10Mbps y 2Mbps de subida. De cualquier forma, los operadores de cable normalmente limitan las tasas máximas para cada usuario a niveles muy inferiores a estos, sobre todo en la dirección de subida.

Vía satélite

En los últimos años, cada vez más compañías están empleando este sistema de transmisión para distribuir contenidos de Internet o transferir ficheros entre distintas sucursales. De esta manera se puede aliviar la congestión existente en las redes terrestres tradicionales.

El sistema de conexión que generalmente se emplea es un híbrido de satélite y teléfono. Hay que tener instalada una antena parabólica digital, un acceso telefónico a Internet (utilizando un modem RTC, RDSI, ADSL o por cable), una

tarjeta receptora para PC, un software específico y una suscripción a un proveedor de satélite.

El cibernauta envía sus mensajes de correo electrónico y la petición de las páginas Web, que consume muy poco ancho de banda, mediante un modem tradicional, pero la recepción se produce por una parabólica, ya sean programas informáticos, videos o cualquier otro material que ocupe muchos megas. La velocidad de descarga a través del satélite puede situarse en casos óptimos en torno a 400Kbps.

Redes inalámbricas

Las redes inalámbricas o wireless son una tecnología normalizada por el IEEE que permite montar redes locales sin emplear ningún tipo de cableado, utilizando infrarrojos u ondas de radio a frecuencias des-normalizadas (de libre utilización).

Están compuestas por dos elementos:

- Punto de acceso:
    - Access Point (AP) o "transceiver", es la estación base que crea un área de cobertura donde los usuarios se pueden conectar. El AP cuenta con una o dos antenas y con una o varias puertas Ethernet.

- Dispositivos clientes:
    - Son elementos que cuentan con tarjeta de red inalámbrica. Estos proporcionan una interfaz entre el sistema operativo de red del cliente y las ondas, a través de una antena.

El usuario puede configurar el canal (se suelen utilizar las bandas de 2,4GHz y 5GHz) con el que se comunica con el punto de acceso por lo que podría cambiarlo en caso de interferencias.

La velocidad con el punto de acceso disminuye con la distancia.

Los sistemas inalámbricos de banda ancha se conocen cómo BWS (Broadband Wireless Systems) y uno de los más atractivos, son los sistemas LMDS.

LMDS

El LMDS (Local Multipoint Distribution System) es un sistema de comunicación de punto a multipunto que utiliza ondas radioeléctricas a altas frecuencias, en

torno a 28 ó 40GHz. Las señales que se transmiten pueden consistir en voz, datos, Internet y video.

Este sistema utiliza como medio de transmisión el aire para enlazar la red troncal de telecomunicaciones con el abonado. En este sentido, se configura un nuevo bucle de abonado, con gran ancho de banda, distinto al tradicional par de hilos de cobre que conecta cada terminal doméstico con la centralita más próxima.

Las bandas de frecuencias utilizadas ocupan un rango en torno a 2GHz, para las cuales la atenuación por agentes atmosféricos es mínima. Debido a las altas frecuencias y al amplio margen de operación es posible conseguir un gran ancho de banda de comunicaciones, con velocidades de acceso que pueden alcanzar los 8Mbps. El sistema opera en el espacio local mediante las estaciones base y las antenas receptoras usuarias, de forma bidireccional. Se necesita que haya visibilidad directa desde la estación base hasta el abonado, por lo cual pueden utilizarse repetidoras si el usuario está ubicado en zonas sin señal.

El LMDS ofrece las mismas posibilidades en cuanto a servicios, velocidad y calidad que el cable de fibra óptica, coaxial o el satélite. La ventaja principal respecto al cable consiste en que puede ofrecer servicio en zonas donde el cable nunca llegaría de forma rentable. Respecto al satélite, ofrece la ventaja de solucionar el problema de la gran potencia de emisión que se dispersa innecesariamente en cubrir amplias extensiones geográficas. Con LMDS la inversión se rentabiliza de manera muy rápida respecto a los sistemas anteriores. Además, los costos de reparación y mantenimiento de la red son bajos, ya que al ser la comunicación por el aire, la red física como tal no existe. Por tanto, este sistema se presenta como un serio competidor para los sistemas de banda ancha.

Hotspots

Brett Stewart en la conferencia NetWorld/InterOp realizada en San Francisco en 1993 propuso este concepto, aunque él no utilizó el término "Hotspot" sino que simplemente hacía referencia al "acceso público a redes inalámbricas".

Se dice que fue la firma Nokia, alrededor de cinco años después, la que se encargó de acuñar esta palabra y relacionarla al concepto mismo.

En la actualidad su proliferación es exponencial.

Un Hotspot es el acceso, generalmente en un lugar público (aeropuertos, bibliotecas, cafeterías, hoteles, etcétera), hacia Internet a través de una conexión WIFI, ya sea a través de uno o varios Access Points.

Los hotspots pueden encontrarse tanto en espacios interiores como en espacios exteriores.

Si consideramos que cada vez son más populares los PDAs (que actualmente casi todos incluyen WIFI) y los computadores portátiles (todos soportan WIFI), y el descenso en los costos de conexión a Internet, es innegable la corriente que vuelve a los hotspots algo imprescindible.

Ha llegado a ser indispensable en cualquier tipo de establecimiento que pretenda dar un alto nivel de calidad en los servicios que presta a sus clientes. Dicho nivel de calidad es claramente apreciable en hoteles, aeropuertos, y demás lugares frecuentados por turistas, en convenciones, ferias comerciales, exposiciones, o similares donde pueda existir gran afluencia de hombres de negocios.

Dado que el concepto de hotspot implica la facilidad de uso, el método más generalizado es el de redireccionar el explorador del cliente en su primer acceso a la red hacia una página que permita realizar el login (esto se conoce como portal cautivo, o captive portal). El nombre de usuario y la contraseña será proporcionado previamente por el administrador del hotspot. Esto hace que el cliente no tenga que realizar cambios en la configuración de su equipo.

Algunos de los sistemas de administración de hotspots exigen que se instale software adicional en los equipos cliente, lo cual sin lugar a duda es un punto en contra de gran importancia frente a aquellos que no lo necesitan; imaginemos a un viajero frecuente que tenga que instalar el software cliente para cada aeropuerto por el que pasa.

La característica de un hotspot que lo vuelve superior a los sistemas de conexión totalmente abierta es que se puede realizar control de las conexiones; con un conexión abierta podemos estar regalando acceso gratuito a Internet a cualquier persona que se encuentre dentro del área de cobertura, incluso es posible que esa persona utilice la conexión para realizar descargas ilegales con P2P, use aceleradores de navegación o gestores de descarga que provoquen que cuando uno de nuestros clientes desee conectarse se encuentre con un servicio absolutamente deficiente. El trabajar con el portal cautivo para hacer login, nos permite conocer en todo momento quién está conectado a nuestro hotspot, independientemente de que el servicio sea gratuito o pagado; y además podemos administrar el ancho de banda y el tiempo que se le permite navegar al cliente.

La configuración de un hotspot puede realizarse con diferentes herramientas independientes que al ser agrupadas nos ofrezcan el funcionamiento deseado, sin embargo existen programas que realizan muchas y en algunos casos todas las tareas, con gran cantidad de opciones y una significativa facilidad de configuración.

Cabe recalcar que se puede encontrar tanto programas gratuitos como pagados. Pero es una buena idea probar diferentes versiones de evaluación para determinar el mejor para cada caso.

Además para establecimientos que no desean enterarse de ninguna tarea de instalación, configuración o mantenimiento del servicio existen proveedores que se encargan de todo, obviamente con un costo que no siempre significará un ahorro hacia el establecimiento.

Una consideración importante a tener en cuenta si nuestro hotspot va a ser pagado, es que el costo debe estar dentro de lo que los usuarios estarían dispuestos a pagar por él. Para determinarlo se debe tener en cuenta:

- Que la velocidad de conexión es siempre inferior a la de una LAN cableada (más aún si consideramos la tecnología 10/100/1000Mbps incluída en casi la totalidad de mainboards actuales), factor que propondría un decremento en el costo.
- Que si la duración de la batería de los equipos portátiles es baja, posiblemente el cliente necesitará conectarse a alimentación, es decir, que consumirá tanto el Internet como energía eléctrica que innegablemente será marcada en nuestro medidor, este factor propondría un incremento en el costo.

Si el costo se encuentra muy por encima del de la conexión cableada podríamos encontrarnos en el caso de que un cliente aunque tenga un equipo portátil opte por utilizar la conexión habitual y luego transferir la información que considere necesaria a través de medios de almacenamiento. Y esto nos llevaría a que la inversión en el o los Access Point, y el software de administración no pueda ser recuperado.

Actualmente en Ambato casi todos los cibercafés ofrecen sus servicios a US$ 0,02 por minuto, es decir, US$ 1,20 por cada hora. Lo cual nos permite tener una referencia.

En el caso de que el servicio vaya a ser gratuito debe tenerse muy en cuenta los costos de instalación, configuración y mantenimiento del hotspot, ya que si bien

el establecimiento que va a ofrecerlo como un plus hacia sus clientes no querrá que estos costos sean excesivamente altos.

Tipos

Se puede realizar dos clasificaciones de los hotspots, una dependiendo del costo, y otra dependiendo de quién lo ofrece.

Por costo:

En general, los programas utilizados para administrar un hotspot poseen gran variedad de opciones en este sentido, adicionalmente algunos permiten combinar políticas de cobro, con lo que se puede realizar un control completamente personalizado, que se ajuste a nuestras necesidades.

- *Gratuito*
  Es decir, que el cliente no tiene que pagar (al menos directamente) para utilizar el servicio. Es muy común en centros comerciales, restaurantes, universidades, bibliotecas, aeropuertos, etc. Sin embargo hay que considerar que aunque servicio sea gratuito no tiene por qué ser ilimitado:

  - En cafeterías y restaurantes podríamos realizar control por tiempos de manera que no ocurra que una persona pida un café a las 8 de la mañana y permanezca en el establecimiento hasta las 6 de la tarde.

  - También podríamos diferenciar el ancho de banda asignado dependiendo del tipo de consumo que realiza el cliente, por ejemplo en aeropuertos, clientes de primera clase con relación al resto de pasajeros, o tomando en cuenta las millas acumuladas, etc.

- *Pagado*
  En este caso se pueden manejar diferentes formas de administrarlo, la mayoría de ellas basadas en el prepago:

  - Una conexión gratuita con velocidad muy baja, en que no se permita la descarga de archivos, pero que ofrezca la posibilidad de obtener mayor velocidad y eliminar restricciones al pagar por el servicio.

  - Conexión en la que se cuentan los minutos y al finalizar se cancela por el uso; este es un modelo al cual la gente ya se ha acostumbrado dado que es el que se utiliza en los cibercafés.

  - Una opción que está en auge es la de los hotspots municipales o metropolitanos, en los cuales son los gobiernos locales los que se encargan de la infraestructura WIFI, y podrían vender acceso

prepagado al servicio. Imaginemos sentarnos en la banca de un parque, sacar nuestro equipo con WIFI (laptop, PDA, celular, etc.) y empezar a navegar con nuestra clave que hemos adquirido en el quiosco de periódicos; o que por suerte nuestra casa se encuentre dentro del área de cobertura del hotspot municipal de manera que podemos acceder a Internet con sólo encender nuestro equipo. Tan sólo en el año 2006 se presentaron más de 800 proyectos de este tipo en los Estados Unidos.

Por ofertante:

Aquí nos referimos a la perspectiva de la administración del hotspot, ya que no será lo mismo una universidad, cibercafé, Biblioteca, donde seguramente existirán personas encargadas de llevar a cavo esta tarea, que un restaurante, cafetería, donde la existencia de estas personas supondría un gasto en algunos casos innecesario.

- *Servicio ofrecido*
  Es decir, el servicio de acceso a Internet es el principal. La administración y la instalación misma del hotspot pueden ser llevadas a cabo por personal de la institución o establecimiento que lo ofrece, dado que el personal está al tanto de la tecnología y resulta una tarea no muy complicada. Es el caso que hemos mencionado de los cibercafés, universidades, bibliotecas, etc.

- *Servicio añadido*
  En este caso, el servicio es simplemente algo opcional que el establecimiento pone a disposición de sus clientes. Un ejemplo muy claro es una cafetería en donde el hotspot se debe tomar como cualquier otro producto: la cafetería adquiere gaseosas a su proveedor y las entrega al cliente que lo requiere, de la misma manera existen proveedores de hotspot de forma que el establecimiento simplemente entregue tarjetas con el nombre de usuario y contraseña que ha de usar el cliente para conectarse. Los meseros, o el cajero no necesitan tener conocimientos de la forma central en que está trabajando el hotspot.

Conceptos relacionados

Hotspot falso

También se le conoce como "hotspot envenenado". Es en realidad un hotspot típico, pero que ha sido configurado con fines malintencionados: interceptar datos que viajan a través de dicho Access Point, como contraseñas, tarjetas de crédito, cuentas bancarias, etc. Para luego llevar a cabo estafas con dichos datos.

Honeypot

Si nos damos cuenta el hotspot falso es un ataque realizado desde el hotspot; pero qué ocurre cuando el ataque es desde el cliente. En ese caso se puede crear un honeypot que es en realidad una trampa para detectar y contrarrestar el uso malintencionado de los sistemas de información. Consiste en un equipo aparentemente desprotegido que parecería contener información importante o recursos valiosos para los atacantes, pero que en realidad está siendo monitorizado.

Software de tipo hotspot con autenticación LDAP

En la actualidad existe gran número de herramientas software que permiten configurar y brindar el servicio de Hotspot, algunas de ellas soportan autenticación LDAP.

Autenticación LDAP

LDAP (*Lightweight Directory Access Protocol*, Protocolo Ligero de Acceso a Directorios) es un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red. LDAP también es considerado una base de datos (aunque su sistema de almacenamiento puede ser diferente) a la que se le pueden realizar consultas.

Habitualmente, se almacena la información de login (usuario y contraseña) y es utilizado para autentificarse aunque es posible almacenar otra información (datos de contacto del usuario, ubicación de diversos recursos de la red, permisos, certificados, etc.).

En conclusión, LDAP es un protocolo de acceso unificado a un conjunto de información sobre una red.

Implementaciones

Existen diversas implementaciones y aplicaciones reales del protocolo LDAP.

Active Directory

Active Directory es el nombre utilizado por Microsoft (desde Windows 2000) como almacén centralizado de información de uno de sus dominios de administración.

Un Servicio de Directorio es un depósito estructurado de la información de los diversos objetos que contiene el Active Directory, en este caso podrían ser impresoras, usuarios, equipos, etc.

Bajo este nombre se encuentra realmente un esquema (definición de los campos que pueden ser consultados) LDAP versión 3, lo cual permite integrar otros sistemas que soporten el protocolo. En este LDAP se almacena información de usuarios, recursos de la red, políticas de seguridad, configuración, asignación de permisos, etc.

Novell Directory Services

También conocido como eDirectory es la implementación de Novell utilizada para manejar el acceso a recursos en diferentes servidores y computadoras de una red. Básicamente está compuesto por una base de datos jerárquica y orientada a objetos, que representa cada servidor, computadora, impresora, servicio, persona, etc., entre los cuales se crean permisos para el control de acceso, por medio de herencia. La ventaja de esta implementación es que corre en diversas plataformas, por lo que puede adaptarse fácilmente a entornos que utilicen más de un sistema operativo.

iPlanet

Basado en la antigua implementación de Netscape, iPlanet se desarrolló cuando AOL adquirió Netscape Communications Corporation y luego conjuntamente con Sun Microsystems comercializaron software para servidores, entre ellos el iPlanet Directory Server, su implementación de LDAP.

OpenLDAP

Se trata de una implementación libre del protocolo que soporta múltiples esquemas por lo que puede utilizarse para conectarse a cualquier otro LDAP.

Tiene su propia licencia, la *OpenLDAP Public License*. Al ser un protocolo independiente de la plataforma, varias distribuciones Linux y BSD lo incluyen, al igual que AIX, HP-UX, Mac OS X, Solaris, Windows (2000/XP) y z/OS.

Red Hat Directory Server

Directory Server es un servicio basado en LDAP que centraliza configuración de aplicaciones, perfiles de usuarios, información de grupos, políticas, así como información de control de acceso dentro de un sistema operativo independiente de la plataforma.

Forma un repositorio central para la infraestructura de manejo de identidad, Red Hat Directory Server simplifica el manejo de usuarios, eliminando la redundancia de datos y automatizando su mantenimiento.

Apache Directory Server

Apache Directory Server (ApacheDS), es un servidor de directorio completamente escrito Java por Alex Karasulu y disponible bajo la licencia de Apache Software, es compatible con LDAP versión 3 certificado por el Open Group, soporta otros protocolos de red tales como Kerberos y NTP, además provee Procedimientos Almacenados, triggers y vistas; características que están presentes en las Bases de Datos Relacionales pero que no estaban presentes en el mundo de LDAP.

Redes de computadoras

Una red de computadoras es dos o más computadoras enlazadas para el intercambio de datos. El software de una red permite compartir periféricos tales como modem, fax, CD-ROM, sistema de almacenamiento masivo, correo electrónico, manejo de proyectos en grupo, compartir aplicaciones, obtener recursos comunes, entre otros.

La conexión física entre los computadores puede efectuarse por un alambre de cobre, fibra óptica, cableado UTP, satélites de comunicación, microondas, entre otros.

Arquitectura Lógica

Maestro/Esclavo

Similar a una relación de alumno y maestro. Características:

- Control y administración central.
- Procesamiento central de información.
- Poleo de estaciones.

Punto a punto

Similar al concepto de grupo de trabajo. Características:

- Administración distribuida.
- Procesamiento independiente de información.
- Medio de transmisión compartido.

Modelo cliente-servidor

Similar a una transacción de cajero automático. Características:

- Red de administrador central.
- Flujo controlado de la información.
- Procesamiento independiente de la información.
- Medio de transmisión compartido.

Topologías de red más comunes

Topología jerárquica

También conocida como configuración de árbol. Se refiere a un arreglo de red en el que las estaciones están unidas a un bus en común.

Topología de bus

También se denomina bus lineal. Todas las estaciones se conectan directamente a un único canal físico (cable) de comunicación (bus). Según los sentidos posibles de transmisión, el bus puede ser unidireccional (principalmente buses de fibra

óptica), los extremos del canal (cable) no están interconectados sino simplemente finalizados con un terminador de 50 ohmios, el terminador elimina automáticamente la señal de los extremos, es posible unir varios segmentos de buses en una configuración "multi-bus" siendo necesario utilizar repetidores de señal en el caso de grandes distancias.

El procedimiento de comunicación utilizado en los buses bidireccionales es el de difusión ("Broadcast").

Topología en estrella

Una configuración de cables para redes LAN, que normalmente se utilizan un dispositivo central, a través del cual pasa toda la comunicación.

Topología en anillo

Es una configuración de los cables en una red, en la cual los equipos se distribuyen alrededor de un anillo formado por el medio de transmisión, por ejemplo, Token Ring. El medio de comunicación de una red en anillo forma un bucle cerrado en el que se integran todas las estaciones de la red, mediante un pequeño repetidor que interrumpe el canal (nodo activo de regeneración de la señal), de modo que cada una de las estaciones mantiene la conexión con las otras adyacentes.

Topología en malla

Esta estructura de red es típica de las WAN, pero también se puede utilizar en algunas aplicaciones de LAN, tiene ventajas frente a problemas de embotellamiento y averías debido a su multiplicidad de caminos o rutas, y a la posibilidad de orientar el tráfico por trayectorias alternativas, los nodos están conectados cada uno con todos los demás. Su desventaja radica en que es cara y compleja su implementación.

Medios físicos

La capa física maneja directamente los medios de transmisión. Estos pueden ser, por ejemplo, cables de cobre, fibra óptica, cable coaxial, enlaces satelitales, enlaces de microondas, etc.

Par trenzado de cobre

Es el medio de transmisión más antiguo y el más utilizado actualmente. Consiste en un par de alambres de cobre aislados y trenzados con el propósito de cancelar el flujo magnético inducido por la corriente que fluye sobre ellos y reducir de esta forma la interferencia eléctrica. El sistema telefónico común que utilizamos se basa en este medio de transmisión, y a través de él se pueden tener comunicaciones análogas y digitales.

Cable coaxial

Es un cable también de cobre, pero con un mejor blindaje. Además, posee un dieléctrico entre el blindaje o tierra y el conductor por donde viaja la señal. La respuesta en alta frecuencia de este tipo de cable es muy superior, permitiendo el transporte de más información a distancias más largas. Por ejemplo, se pueden lograr velocidades de hasta 2Gbps en 1 Km de distancia.

Fibra óptica

La fibra óptica ha sido una de las tecnologías que ha traído mayores beneficios en cuanto a medios de transmisión se refiere, ya que no es un conductor eléctrico, sino un material por el que se propaga la luz.

Siendo aparentemente un cable, contiene fibras en su interior por las cuales se pueden enviar señales de luz en forma independiente. Es muy utilizada actualmente para troncales telefónicas o de datos, así como para los cables interoceánicos, tales como Americas-1 y el TCS-1. Es totalmente inmune al ruido electromagnético y las pérdidas son muy bajas en largas distancias.

Enlaces de radio, microondas y satélites

Otro medio muy utilizado, y de igual importancia, es el que usa las ondas de radio (RF) dentro del espectro electromagnético. La comunicación puede darse, por ejemplo, con microondas, donde a altas frecuencias (superiores a 500Mhz) se establecen enlaces muy confiables entre dos puntos gracias a la alta directividad que se puede lograr con los patrones de radiación en las antenas. De esta forma se pueden tener comunicaciones a grandes distancias, o donde haya línea visual, y hacerlo de forma directa, sin repartir la información de manera omnidireccional. Este mismo principio se aplica en esencia a los enlaces de satélites, en donde se recurre a una frecuencia más alta y se usa el satélite como repetidor para devolver el mensaje a otro punto de la tierra, evitando los problemas presentados por obstáculos como las montañas, por ejemplo. En este caso, existe un elemento

en contra que es el retardo, y que está dado por las grandes distancias que debe recorrer la señal para llegar a su destino.

Tipos de redes

Redes LAN

Local Area Network. Son redes de propiedad privada que funcionan dentro de una oficina, edificio o terreno hasta unos cuantos kilómetros, generalmente son usadas para conectar computadores personales y estaciones de trabajo en una compañía y su objetivo es compartir recursos e intercambiar información.

Las redes LAN generalmente usan una tecnología de transmisión que consiste en un cable sencillo, al cual se encuentran conectados todos los computadores, la velocidad tradicional de las redes de área local oscila entre 10 y 100Mbps.

Redes MAN

Metropolitan Area Network. Es básicamente una versión más grande que las redes de área local con una tecnología similar. Una red MAN puede manejar voz y datos e incluso podría estar relacionada con la red de televisión local por cable. Este estándar define un protocolo de gran velocidad, en donde los computadores conectados comparten un bus doble de fibra óptica utilizando el método de acceso llamado bus de cola distribuido.

El distinguir las redes MAN en una categoría especial indica que se ha adoptado un estándar especial denominado DQDB, que consiste en dos cables ópticos unidireccionales, donde están conectados todos los computadores.

Redes WAN

Wide Area Network. Es una red de gran alcance con un sistema de comunicaciones que interconecta redes geográficamente remotas, utilizando servicios proporcionados por las empresas de servicio público como comunicaciones vía telefónica o en ocasiones instalados por una misma organización. Una red que se extiende por un área geográfica extensa mantiene computadores con el propósito de efectuar aplicaciones, a estos se les denomina HOSTS. Los HOSTS se encuentran conectados a subredes de comunicaciones, cuya función es conducir mensajes de un host a otro, a diferencia del sistema telefónico que conduce la voz, los hosts conducen datos utilizando la misma vía (red telefónica).

Una red WAN también tiene la posibilidad de comunicarse mediante un sistema de satélite o radio, utilizando antenas las cuales efectúan la transmisión y recepción.

Redes inalámbricas

Las redes inalámbricas se basan en el principio de conectar una antena a un circuito eléctrico en donde las ondas electromagnéticas se difunden para captarse en un receptor a cierta distancia.

La instalación de redes inalámbricas es relativamente fácil, pero presentan algunas desventajas como su velocidad de transmisión y recepción que puede alcanzar de 1 a 2 Mbps, lo cual es mucho más lento que las redes LAN y redes WAN.

Administración de redes y servicios

La Administración de Redes es un conjunto de técnicas tendientes a mantener una red operativa, eficiente, segura, constantemente monitoreada y con una planeación adecuada y propiamente documentada.

Sus objetivos son:

- Mejorar la continuidad en la operación de la red con mecanismos adecuados de control y monitoreo, de resolución de problemas y de suministro de recursos.
- Hacer uso eficiente de la red y utilizar mejor los recursos, como por ejemplo, el ancho de banda.
- Reducir costos por medio del control de gastos y de mejores mecanismos de cobro.
- Hacer la red más segura, protegiéndola contra el acceso no autorizado, haciendo imposible que personas ajenas puedan entender la información que circula en ella.
- Controlar cambios y actualizaciones en la red de modo que ocasionen las menos interrupciones posibles, en el servicio a los usuarios.

La administración de la red se vuelve más importante y difícil si se considera que las redes actuales comprendan lo siguiente:

- Mezclas de diversas señales, como voz, datos, imagen y gráficas.

- Interconexión de varios tipos de redes, como WAN, LAN y MAN.
- El uso de múltiples medios de comunicación, como par trenzado, cable coaxial, fibra óptica, satélite, láser, infrarrojo y microondas.
- Diversos protocolos de comunicación, incluyendo TCP/IP, SPX/IPX, SNA, OSI.
- El empleo de muchos sistemas operativos, como DOS, NetWare, Windows NT, UNIX, OS/2.
- Diversas arquitecturas de red, incluyendo Ethernet 10baseT, Fast Ethernet, Token Ring, FDDI, 100vg-Any LAN y Fiber channel.
- Varios métodos de compresión, códigos de línea, etc.

El sistema de administración de red opera bajo los siguientes pasos básicos:

1. Colección de información acerca del estado de la red y componentes del sistema. La información recolectada de los recursos debe incluir: eventos, atributos y acciones operativas.
2. Transformación de la información para presentarla en formatos apropiados para el entendimiento del administrador.
3. Transportación de la información del equipo monitoreado al centro de control.
4. Almacenamiento de los datos coleccionados en el centro de control.
5. Análisis de parámetros para obtener conclusiones que permitan deducir rápidamente lo que pasa en la red.
6. Actuación para generar acciones rápidas y automáticas en respuesta a una falla mayor.

La característica fundamental de un sistema de administración de red moderno es la de ser un sistema abierto, capaz de manejar varios protocolos y lidiar con varias arquitecturas de red, es decir: soporte para los protocolos de red más importantes.

Administración de tiempo de acceso a Internet

En cualquier establecimiento que proporciona servicios de Internet es necesario administrar dichos servicios estableciendo restricciones o limitaciones, que pueden ser: ancho de banda, sitios permitidos, protocolos y puertos abiertos, y tiempo de acceso (sea considerado como tiempo máximo de sesión o tiempo límite de uso).

Todas estas restricciones no siempre son bien recibidas por parte del usuario pero pretenden asegurar la equidad y calidad entre ellos (ancho de banda), los

contenidos visualizados (sitios permitidos), evitar saturaciones y sobrecargas de tráfico en la red (protocolos y puertos), y exactitud en el cobro de la utilización del servicio (tiempo de acceso).

Para estas tareas existen muchas técnicas, todas guardando estrecha relación con la Administración de Redes y Servicios, por lo cual se hace plenamente evidente que está en manos del administrador establecer la o las más apropiadas para su entorno.

PPP

Point-to-Point Protocol (Protocolo punto a punto). Es un protocolo de nivel de enlace estandarizado en el documento RFC 1661. Por tanto, se trata de un protocolo asociado a la pila TCP/IP de uso en Internet.

El protocolo PPP permite establecer una comunicación a nivel de enlace entre dos computadoras. Generalmente, se utiliza para establecer la conexión a Internet de un particular con su proveedor de acceso a través de un módem telefónico. Ocasionalmente también es utilizado sobre conexiones de banda ancha, como PPPoE o PPPoA.

Además del simple transporte de datos, PPP facilita dos funciones importantes:

- *Autenticación.*
  Generalmente mediante una clave de acceso.

- *Asignación dinámica de IP.*
  Los proveedores de acceso cuentan con un número limitado de direcciones IP y cuentan con más clientes que direcciones. Naturalmente, no todos los clientes se conectan al mismo tiempo. Así, es posible asignar una dirección IP a cada cliente en el momento en que se conectan al proveedor. La dirección IP se conserva hasta que termina la conexión por PPP. Posteriormente, puede ser asignada a otro cliente.

PPP también tiene otros usos, por ejemplo, se utiliza para establecer la comunicación entre un módem ADSL y la pasarela ATM del operador de telecomunicaciones. También se ha venido utilizando para conectar a trabajadores desplazados (con laptops) con sus oficinas a través de un centro de acceso remoto de su empresa. Aunque esta aplicación se está abandonando a favor de las redes privadas virtuales, que son más seguras.

Funcionamiento

PPP consta de las siguientes fases:

1. *Establecimiento de conexión.*
   Durante esta fase, una computadora contacta con la otra y negocian los parámetros relativos al enlace como el método de autenticación que se va a utilizar, el tamaño de los datagramas, números mágicos para usar durante la autenticación, etc., usando el protocolo LCP.

2. *Autenticación.*
   No es obligatorio. Existen dos protocolos de autenticación. El más básico e inseguro es PAP, aunque no se recomienda dado que manda el nombre de usuario y la contraseña en claro. Un método más avanzado y preferido por muchos ISP es CHAP, en el cual la contraseña se manda cifrada.

3. *Configuración de red.*
   En esta fase se negocian parámetros dependientes del protocolo de red que se esté usando. PPP puede llevar muchos protocolos de red al mismo tiempo y es necesario configurar individualmente cada uno de estos protocolos. Para configurar un protocolo de red se usa el protocolo NCP correspondiente. Por ejemplo, si la red es IP, se usa el protocolo IPCP para asignar la dirección IP del cliente y sus servidores DNS.

4. *Transmisión.*
   Durante esta fase se manda y recibe la información de red. LCP se encarga de comprobar que la línea está activa durante períodos de inactividad. PPP no proporciona cifrado de datos.

5. *Terminación.*
   La conexión puede ser finalizada en cualquier momento y por cualquier motivo.

PPP tiene todas las propiedades de un protocolo de nivel de enlace:

- Garantía de recepción.
- Recepción ordenada.

PPPoE

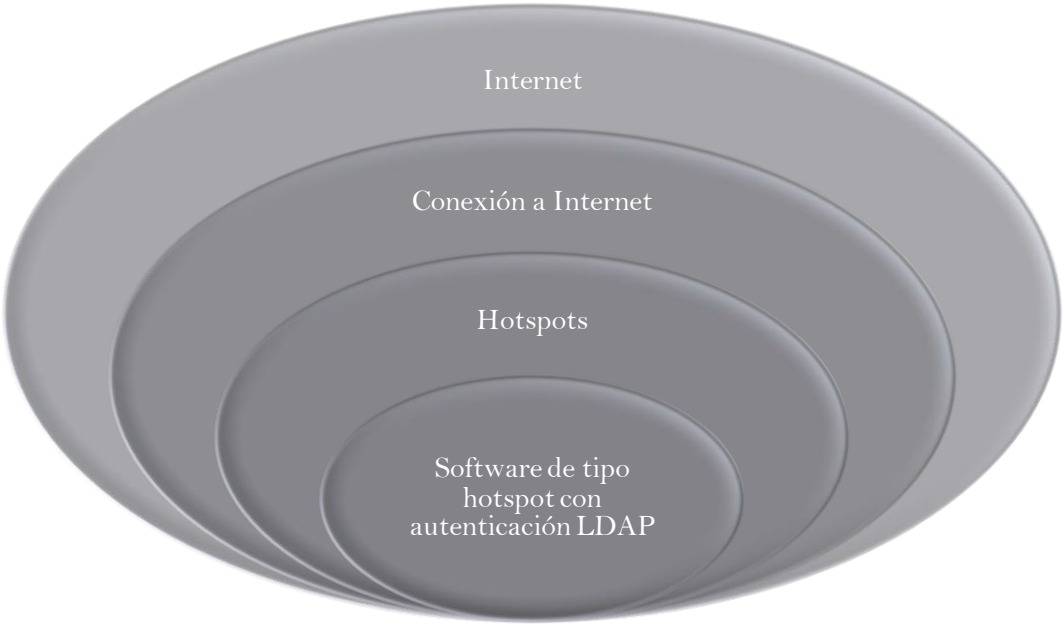
Point-to-Point Protocol over Ethernet. Es un protocolo de red para la encapsulación PPP sobre una capa de Ethernet. Es utilizada mayormente para

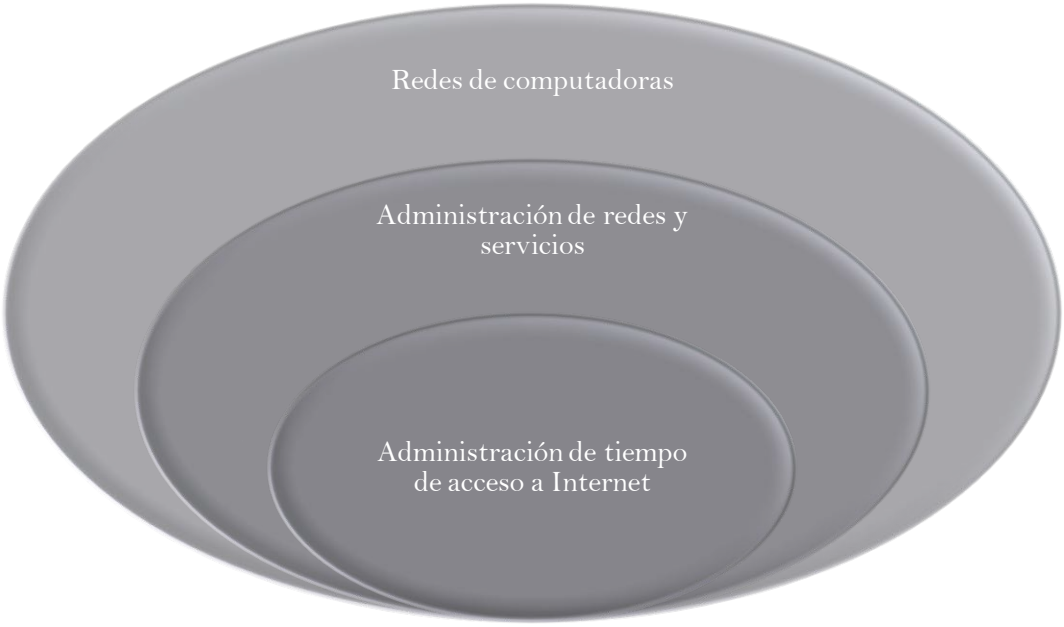
proveer conexión de banda ancha mediante servicios de cable módem y xDSL. Este ofrece las ventajas del protocolo PPP como son la autenticación, cifrado y compresión.

En esencia, es un protocolo túnel, que permite implementar una capa IP sobre una conexión entre dos puertos Ethernet, pero con las características de software del protocolo PPP, por lo que es utilizado para virtualmente "marcar" a otra máquina dentro de la red Ethernet, logrando una conexión "serial" con ella, con la que se pueden transferir paquetes IP, basado en las características del protocolo PPP.

Esto permite utilizar software tradicional basado en PPP para manejar una conexión que no puede usarse en líneas seriales pero con paquetes orientados a redes locales como Ethernet para proveer una conexión clásica con autenticación para cuentas de acceso a Internet. Además, las direcciones IP en el otro lado de la conexión sólo se asignan cuando la conexión PPPoE es abierta, por lo que admite la reutilización de direcciones IP (direccionamiento dinámico).

PPPoE fue desarrollado por UUNET, Redback y RouterWare. El protocolo está publicado en RFC 2516.





2.4 HIPÓTESIS

La aplicación de un software de tipo hotspot con autenticación LDAP mejoraría la eficiencia en la administración de tiempo de acceso a Internet en la Biblioteca de la Facultad de Ingenierías en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato.

2.5 SEÑALAMIENTO DE VARIABLES

2.5.1 VARIABLE INDEPENDIENTE

Software de tipo hotspot con autenticación LDAP.

2.5.2 VARIABLE DEPENDIENTE

Administración de tiempo de acceso a Internet.

CAPÍTULO *3*
METODOLOGÍA

3 METODOLOGÍA

3.1 MODALIDAD BÁSICA DE LA INVESTIGACIÓN

El presente trabajo se basa en la investigación bibliográfica–documental puesto que permite obtener antecedentes de casos similares, que sirve como sustento en la elaboración de la metodología de la propuesta. Adicionalmente, emplea investigación de campo debido a que permite efectuar recolección directa de datos.

3.2 NIVEL O TIPO DE INVESTIGACIÓN

La investigación se enmarca dentro del tipo básico. Y considera la modalidad exploratorio-descriptiva.

Es exploratorio porque será necesario realizar el estudio desde la Biblioteca de la Facultad, para poder establecer el origen del problema y considerar las circunstancias reales bajo las cuales se planteará la posible solución.

Es descriptivo porque se compararán distintas opciones antes de proponer la solución.

3.3 POBLACIÓN Y MUESTRA

3.3.1 POBLACIÓN

La población a considerarse en la presente investigación es la totalidad de estudiantes de la Facultad de Ingenierías en Sistemas, Electrónica e Industrial, que numéricamente se aproxima a los 860 alumnos.

3.3.2 MUESTRA

La muestra comprenderá al promedio de estudiantes de la Facultad que diariamente hacen uso de Internet en la Biblioteca de la misma, que numéricamente son 200 alumnos.

Para calcular la proporción de alumnos sobre los cuales se aplicará la observación directa, se divide el tamaño de la muestra entre el de la población: 200/860=0,23, lo que quiere decir que se está observando al 23% de la población.

Ahora se calcula cuántos individuos son representados por cada uno de los elementos de la muestra, realizando la división contraria: 860/200=4,3, lo que querría decir que cada uno de los elementos de la muestra representa a 4 alumnos de la Facultad.

3.4 OPERACIONALIZACIÓN DE VARIABLES

3.4.1 VARIABLE INDEPENDIENTE

Software de tipo hotspot con autenticación LDAP.

CONCEPTUALIZACIÓN	CATEGORÍAS	INDICADORES	ÍTEMS BÁSICOS	TÉCNICAS / INSTRUMENTOS
Software de tipo hotspot con autenticación LDAP se conceptúa como: Software que provee portal cautivo para realizar autenticación LDAP (Active Directory mediante Internet Authentication Service, IAS)	Portal cautivo	Página web con campos para ingreso de nombre de usuario y contraseña.	¿Qué interacción existe entre el usuario y el portal cautivo?	Redireccionamiento del sitio al que se pretende acceder en el explorador de Internet
	Autenticación	Ventana pop-up para permanencia y salida del sistema. Página web con reporte de error y opción de regresar a la página anterior.	¿Qué respuesta presenta el sistema ante la autenticación?	Registro del suceso en el log de IAS

3.4.2 VARIABLE DEPENDIENTE

Administración de tiempo de acceso a Internet.

CONCEPTUALIZACIÓN	CATEGORÍAS	INDICADORES	ÍTEMS BÁSICOS	TÉCNICAS / INSTRUMENTOS
Administración de tiempo de acceso a Internet se conceptúa como: medición del consumo de tiempo de uso de Internet	Administración	Control de tiempos de ingreso y de salida del usuario al servicio	¿Cuál es el proceso de administración del uso de Internet?	Registro de observación directa en la Biblioteca de la FISEI–UTA

3.5 PLAN DE RECOLECCIÓN DE INFORMACIÓN

Nº	Preguntas	Respuestas
1	¿Dónde?	En la Biblioteca de la FISEI–UTA
2	¿Sobre qué?	Sobre los tiempos de ingreso y salida de los usuarios de Internet
3	¿Por qué?	Porque es posible mejorar la administración del uso de Internet
4	¿Para qué?	Para incrementar la eficiencia a través de la reducción de tiempos
5	¿Quién?	El investigador y personal de apoyo
6	¿A quiénes?	A los usuarios del servicio de Internet
7	¿Cuándo?	Lunes, 16 de marzo de 2009
8	¿Cuántas veces?	Una vez
9	¿Cómo?	Registrando mediciones de los tiempo de entrada y salida
10	¿Con qué?	Con un registro de observación diseñado para el efecto

3.6 PLAN DE PROCESAMIENTO DE LA INFORMACIÓN

1. Los datos que se recolectaron fueron sometidos a una revisión, selección y posterior ordenamiento.
2. Los registros de observación se procesaron y fueron tabulados.
3. Los resultados de la tabulación fueron expresados estadísticamente por medio de gráficos.
4. Se realizó el análisis e interpretación de los datos.
5. El análisis se realizó en base a los objetivos.
6. La interpretación se realizó en base al marco teórico.

CAPÍTULO 4
ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

4 ANÁLISIS E INTERPRESTACIÓN DE RESULTADOS

4.1 ANÁLISIS DE RESULTADOS

4.1.1 VALORES DE LA OBSERVACIÓN DIRECTA

El "Tiempo de ingreso" hace referencia al lapso que comprende los siguientes eventos:

- El alumno se acerca al bibliotecario y solicita el servicio.
- El bibliotecario recepta el carnet de Internet y la Cédula del alumno.
- El alumno camina hasta el computador que va a utilizar.
- El alumno abre el explorador de Internet y empieza a navegar.

El "Tiempo de salida" hace referencia al lapso que comprende los siguientes eventos:

- El alumno cierra el explorador de Internet y desocupa el computador.
- El alumno se acerca al bibliotecario y solicita sus documentos.
- El bibliotecario compara la hora de ingreso y la hora de salida, realiza una resta, y tacha el carnet de Internet con la aproximación en minutos más cercana a un múltiplo de 5.
- El alumno recibe sus papeles y se retira.

Nº de observación	*Tiempo de ingreso (segundos)*	*Tiempo de salida (segundos)*
1	21	30
2	36	23
3	14	30
4	18	20
5	18	21
6	15	36
7	14	22
8	15	28
9	33	34
10	19	25
11	25	28
12	30	27
13	25	20
14	23	29
15	30	37
16	22	36
17	25	29
18	17	29
19	23	33
20	23	38
21	15	26
22	22	41
23	27	23
24	21	32
25	16	20
26	24	30
27	35	42
28	28	43
29	19	36
30	17	37
31	27	43
32	19	43
33	26	43
34	19	24
35	33	25
36	36	39
37	15	24
38	23	24
39	16	36
40	24	38
41	33	26
42	31	21
43	24	35
44	19	20
45	23	24
46	16	30
47	20	41
48	26	26
49	19	26
50	35	40
51	25	31
52	20	23
53	15	22
54	28	29
55	17	36
56	19	25
57	34	35
58	24	43
59	30	34
60	25	30
61	31	32
62	22	31
63	32	41
64	35	31
65	16	31
66	37	23
67	34	20
68	30	43
69	21	32
70	26	33
71	26	21
72	34	33
73	28	25
74	14	34
75	24	42
76	27	35
77	34	26
78	25	22
79	31	37
80	28	42
81	30	37
82	35	30

83	22	20
84	18	27
85	35	42
86	17	42
87	22	28
88	18	28
89	23	43
90	36	24
91	34	40
92	27	21
93	22	31
94	25	27
95	21	23
96	24	25
97	16	24
98	16	31
99	35	20
100	16	33
101	33	30
102	16	30
103	17	26
104	20	41
105	18	40
106	21	27
107	14	36
108	17	43
109	34	31
110	36	20
111	19	30
112	21	22
113	19	34
114	36	41
115	35	33
116	27	21
117	18	25
118	16	24
119	29	27
120	33	24
121	22	25
122	22	38
123	32	32
124	18	23

125	34	38
126	24	25
127	14	42
128	27	21
129	29	33
130	24	43
131	27	40
132	33	41
133	20	36
134	20	20
135	19	31
136	16	22
137	16	23
138	37	38
139	15	22
140	23	34
141	18	38
142	14	41
143	35	37
144	20	27
145	31	20
146	17	35
147	15	27
148	26	32
149	22	38
150	36	25
151	37	42
152	27	26
153	26	26
154	37	39
155	28	37
156	22	40
157	21	27
158	22	29
159	14	33
160	23	23
161	16	21
162	16	43
163	26	20
164	25	41
165	20	32
166	37	24

167	18	39
168	34	33
169	16	26
170	22	39
171	24	23
172	24	27
173	32	35
174	35	32
175	35	41
176	22	40
177	19	38
178	27	27
179	17	33
180	36	37
181	37	20
182	27	43
183	30	22
184	36	32

185	21	38
186	22	22
187	35	23
188	26	33
189	31	33
190	35	42
191	23	43
192	24	21
193	23	34
194	20	42
195	14	28
196	19	33
197	26	25
198	14	40
199	29	37
200	28	31
Sumatoria	4901	6238
Promedio	**24,505**	**31,19**

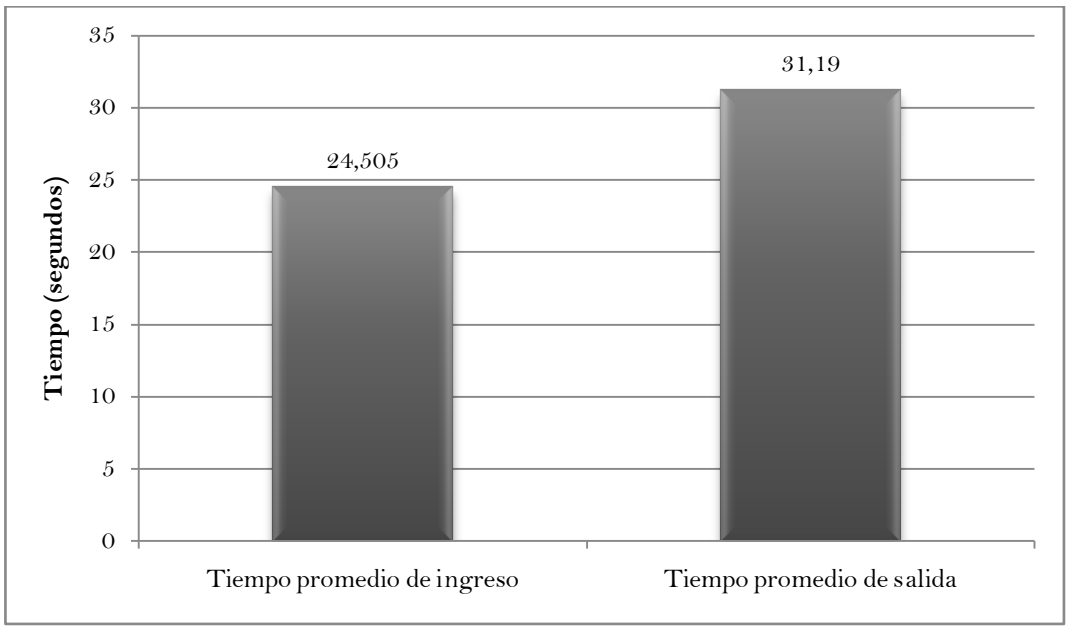


Gráfico 1. Resultados observación directa

4.1.2 VALORES CIENTÍFICAMENTE DEMOSTRABLES

Tomando los factores:

- Tiempo de procesador de percepción visual $T_{visual} = 230\ mseg$.
- Tiempo de procesador cognoscitivo $T_{cognoscitivo} = 70\ mseg$.
- Tiempo de procesador motriz $T_{motriz} = 70\ mseg$.

El "Tiempo de ingreso" hace referencia a la digitación del número de Cédula de Ciudadanía tanto en el campo de nombre de usuario como en el de contraseña y la pulsación del botón Continuar:

$$T_{ingreso} = T_{visual} + campos * dígitos * (T_{cognoscitivo} + T_{motriz})$$

$$T_{ingreso} = 0{,}23\ seg + 2 * 10 * (0{,}07\ seg + 0{,}07\ seg)$$

$$T_{ingreso} = 3{,}03\ seg$$

El "Tiempo de salida" hace referencia a la llamada a la ventana de Logout, la pulsación del botón de salida, y el cierre de dicha ventana.

$$T_{salida} = T_{vis\_1} + T_{mot\_1} + T_{mot\_2} + T_{vis\_1} + T_{mot\_3} + T_{vis\_3} + T_{mot\_4} + T_{mot\_5}$$

$$T_{salida} = (0{,}23 + 0{,}07 + 0{,}07 + 0{,}23 + 0{,}07 + 0{,}23 + 0{,}07 + 0{,}07)\ seg$$

$$T_{salida} = 1{,}04\ seg$$

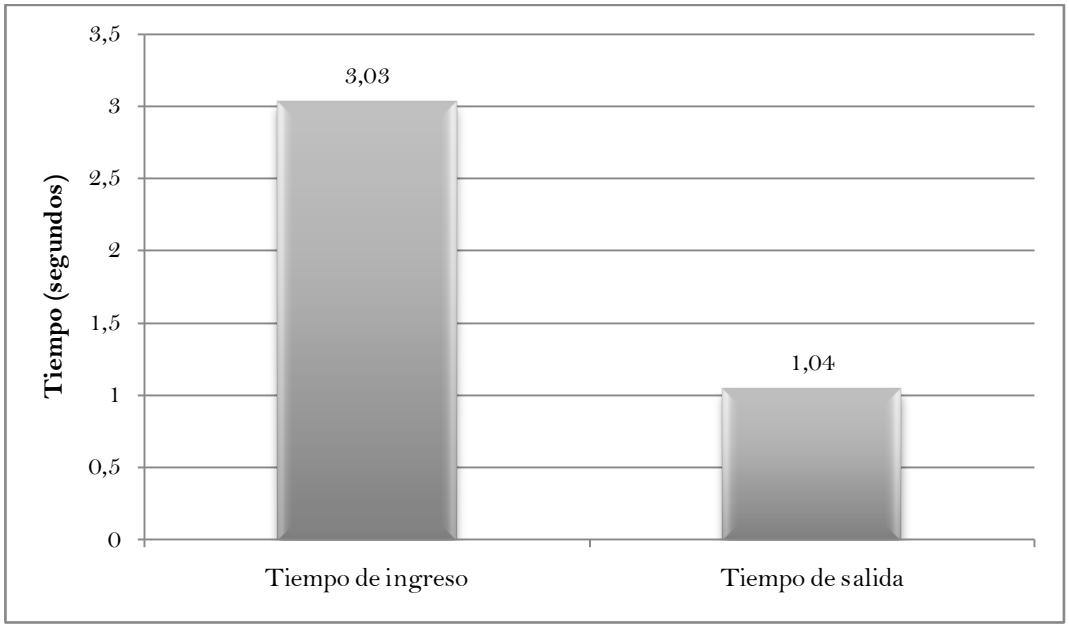


Gráfico 2. Resultados científicamente demostrables

4.2 INTERPRETACIÓN DE RESULTADOS

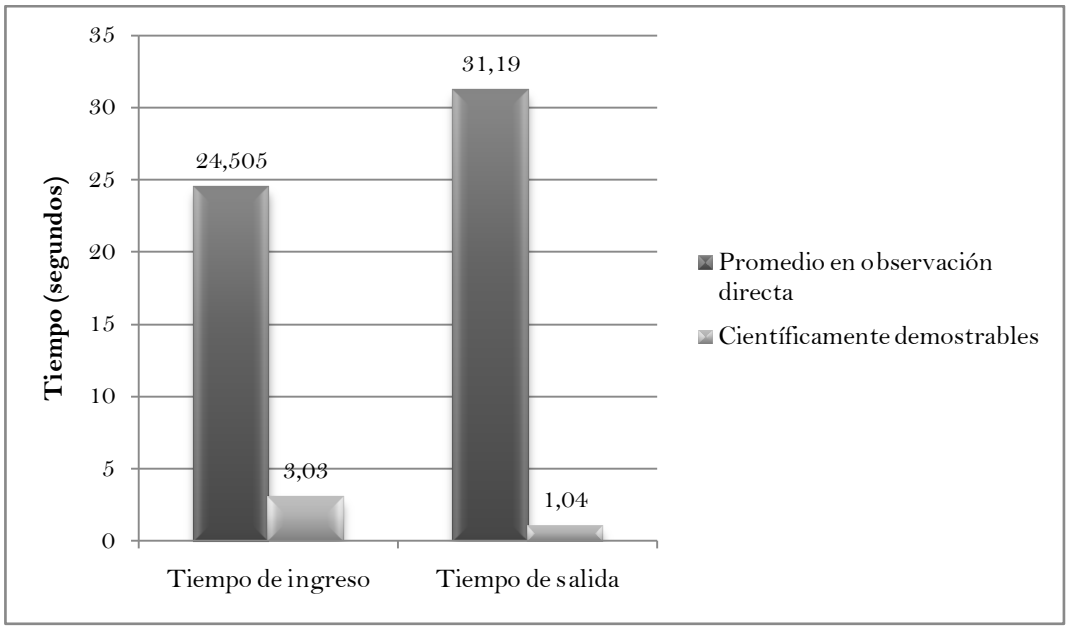


Gráfico 3. Comparación de resultados entre observación directa y valores científicamente demostrables

Como se aprecia en el Gráfico 3, el resultado promedio de los tiempos de ingreso en la observación directa (200 observaciones) corresponde a 24,505 segundos,

mientras sus equivalentes científicamente demostrables presentan un valor de 3,03 segundos, siendo significativamente menor.

El gráfico también permite valorar que del promedio de los tiempos de salida en la observación directa, correspondiente a 31,19 segundos, se produce una disminución aún más importante pues sus semejantes científicamente demostrables muestran un valor de 1,04 segundos.

4.3 VERIFICACIÓN DE HIPÓTESIS

La aplicación de un software de tipo hotspot con autenticación LDAP mejora la eficiencia en la administración de tiempo de acceso a Internet en la Biblioteca de la Facultad de Ingenierías en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato, esta afirmación se demuestra cuantitativamente porque: en el ingreso se produce una optimización del 87,63%, y en la salida de un 96,66%.

CAPÍTULO 5
CONCLUSIONES Y RECOMENDACIONES

5 CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- Se determinaron las características del uso de Internet en la Biblioteca de la FISEI–UTA gracias a la aplicación de la observación directa y la determinación de los tiempos convencionales de ingreso y salida del servicio.

- Se definió que pfSense es la herramienta software más apropiada que permiten establecer una solución de tipo hotspot (portal cautivo) para ser aplicada.

- Se estableció que IAS (Internet Authentication Service) provee la posibilidad de realizar autenticación contra Active Directory (implementación de LDAP) por lo que es la más adecuada para el caso.

- Cada uno de los equipos clientes de la solución software debe permitir que la dirección IP sea asignada mediante DHCP, y tener un navegador de Internet. El equipo ruteador deberá tener al menos 128MB de memoria RAM, procesador tipo Pentium superior a 100MHz, disco duro con capacidad de 1GB y dos tarjetas de red (NIC). El computador que trabajará como servidor deberá tener 512MB de memoria RAM como mínimo, sistema operativo Microsoft Windows 2003 Server, y espacio en disco suficiente para la base de datos de Microsoft SQL Server 2005 Express generada por el log de IAS.

- La ventaja que ofrece la aplicación de un software de tipo hotspot con autenticación LDAP en la administración de tiempo de acceso a Internet en la Biblioteca de la FISEI–UTA, es la optimización de los tiempos de ingreso y salida del servicio, que se traducen en 87,63% y 96,66% respectivamente.

- El procedimiento de configuración del software de tipo hotspot y de la implementación de LDAP para cumplir la función requerida se especifica en el siguiente capítulo como parte de la propuesta.

- Es posible realizar administración de redes y servicios utilizando únicamente software libre y software en versiones express (gratuito), y aprovechando máquinas aparentemente obsoletas pero que pueden tener una segunda vida útil en tareas específicas, como es el caso del equipo ruteador.

5.2 RECOMENDACIONES

Dados los contundentes resultados de la investigación se exhorta a las autoridades de la FISEI se disponga, a quien corresponda, se aplique la solución propuesta a la mayor brevedad posible.

Se recomienda a las autoridades de la Facultad que por su intermedio se transfieran los resultados de la presente investigación a todas las bibliotecas existentes en la Universidad Técnica de Ambato con el fin de socializar y participar a ellas el beneficio que significará su aplicación.

Una opción para aumentar la "productividad" del sistema propuesto sería la de añadir un Access Point, de manera que los estudiantes con computadores portátiles también sean controlados por la misma solución software.

CAPÍTULO 6
PROPUESTA

6 PROPUESTA

6.1 DATOS INFORMATIVOS

Aplicación de un software de tipo hotspot con autenticación LDAP para administrar el tiempo de acceso a Internet en la Biblioteca de la Facultad de Ingenierías en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato.

6.2 ANTECEDENTES DE LA PROPUESTA

En la Biblioteca de la Facultad de Ingenierías en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato (FISEI–UTA) el personal se encarga tanto de las tareas propias de su cargo como préstamo y recepción de libros y demás tareas específicas, como de la de recepción de carnets y tarjetas de Internet de los alumnos y control del tiempo utilizado, lo cual ocasiona situaciones conflictivas tanto a los estudiantes como a las personas que se encuentran a cargo de este servicio.

Aunque simultáneamente se ofrece conexión inalámbrica a quienes poseen un computador portátil, el costo de estos equipos aún no permite que se pueda convertir en una solución a la gran demanda de información proveniente del ciberespacio por parte del alumnado.

La presente investigación, que involucra la administración del tiempo de acceso a Internet en la Biblioteca de la FISEI–UTA, mediante la aplicación de un software de tipo hotspot con autenticación LDAP, precisamente se realizó para brindar solución a los problemas antes descritos que se han venido presentando y que motivaron la realización de la misma.

El estudio se realizó en la Biblioteca de la FISEI–UTA (2008-2009), gracias al apoyo del personal de la Biblioteca, del área de Administración de Redes, y autoridades de la Facultad.

Finalizada la investigación se concluye que, efectivamente, la aplicación de un software de tipo hotspot con autenticación LDAP, mejora la eficiencia en la administración de tiempo de acceso a Internet en la Biblioteca de la Facultad de Ingenierías en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato, según lo indican los resultados provenientes del registro de observación directa versus los valores de tiempos científicamente demostrables en base a factores tales como: Tiempo de procesador de percepción visual, Tiempo de

procesador cognoscitivo, Tiempo de procesador motriz, y sobre todo la constatación de dichos factores en la ejecución de la solución software en condiciones de laboratorio.

6.3 JUSTIFICACIÓN

La propuesta se justifica en las siguientes consideraciones:

- Es necesario reducir los tiempos de ingreso y salida al servicio de Internet por parte de los alumnos para un mejor aprovechamiento del tiempo disponible para consultas y tareas académicas.
- Es importante que el uso del servicio sea controlado de manera precisa, eliminando aproximaciones que pueden resultar en conflictos entre la Facultad como proveedora de un servicio y el alumno como consumidor del mismo.
- Es oportuno aprovechar las herramientas tecnológicas disponibles para realizarlo, sobre todo aquellas que se pueden aplicar sin costos por licencias.

6.4 OBJETIVOS

6.4.1 GENERAL

Proponer una la solución software para mejorar la administración del tiempo de acceso a Internet en la Biblioteca de la Facultad de Ingenierías en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato, utilizando herramientas de software libre.

6.4.2 ESPECÍFICOS

6.4.2.1 Formular una guía de configuración de la solución software tipo hotspot con autenticación LDAP para la administración del tiempo de acceso a Internet en la Biblioteca de la Facultad de Ingenierías en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato.

6.4.2.2 Generar un manual de operación para el bibliotecario referente a la creación de usuarios en la solución software.

6.4.2.3 Generar una guía de uso para el alumno (usuario) referente al portal cautivo.

6.5 ANÁLISIS DE FACTIBILIDAD

6.5.1 ASPECTO FINANCIERO

Es factible desde el punto de vista financiero puesto que el costo es mínimo al utilizarse herramientas de software libre, y que el hardware necesario es posible encontrarlo en equipos aparentemente obsoletos pero que reúnen las características necesarias para cumplir con los requerimientos.

6.5.2 ASPECTO TÉCNICO

La propuesta puede ser ejecutada gracias a los conocimientos adquiridos durante el transcurso de la vida académica en la Institución y el apoyo del personal del área de Administración de Redes de la Facultad.

6.6 FUNDAMENTACIÓN

Software de tipo hotspot con autenticación LDAP

En la actualidad existe gran número de herramientas software que permiten configurar y brindar el servicio de Hotspot, algunas de ellas soportan autenticación LDAP.

Autenticación LDAP

LDAP (*Lightweight Directory Access Protocol*, Protocolo Ligero de Acceso a Directorios) es un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red. LDAP también es considerado una base de datos (aunque su sistema de almacenamiento puede ser diferente) a la que se le pueden realizar consultas.

Habitualmente, se almacena la información de login (usuario y contraseña) y es utilizado para autentificarse aunque es posible almacenar otra información (datos de contacto del usuario, ubicación de diversos recursos de la red, permisos, certificados, etc.).

En conclusión, LDAP es un protocolo de acceso unificado a un conjunto de información sobre una red.

Administración de tiempo de acceso a Internet

En cualquier establecimiento que proporciona servicios de Internet es necesario administrar dichos servicios estableciendo restricciones o limitaciones, que pueden ser: ancho de banda, sitios permitidos, protocolos y puertos abiertos, y tiempo de acceso (sea considerado como tiempo máximo de sesión o tiempo límite de uso).

Todas estas restricciones no siempre son bien recibidas por parte del usuario pero pretenden asegurar la equidad y calidad entre ellos (ancho de banda), los contenidos visualizados (sitios permitidos), evitar saturaciones y sobrecargas de tráfico en la red (protocolos y puertos), y exactitud en el cobro de la utilización del servicio (tiempo de acceso).

Para estas tareas existen muchas técnicas, todas guardando estrecha relación con la Administración de Redes y Servicios, por lo cual se hace plenamente evidente que está en manos del administrador establecer la o las más apropiadas para su entorno.

6.7 METODOLOGÍA

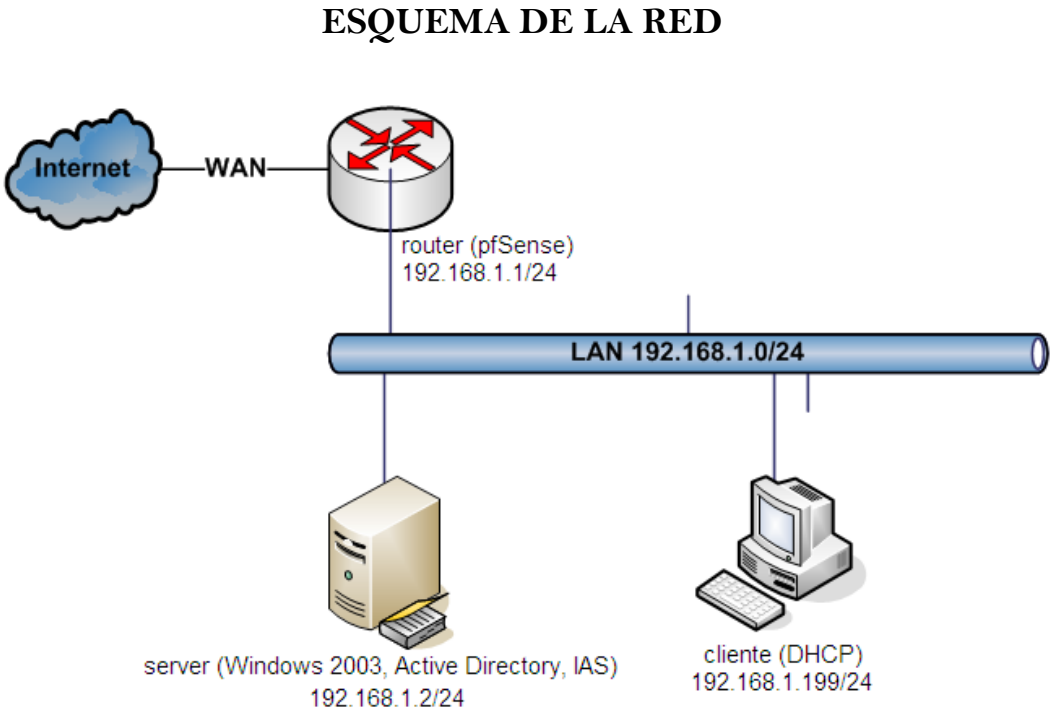


Figura 1. Esquema de la red

La Figura 1 permite visualizar las conexiones entre los equipos y la función de cada uno.

Equipo ROUTER

Este equipo no es un router como tal sino que se trata de un computador con dos tarjetas de red en el cual se instalará un sistema operativo FreeBSD modificado para realizar las funciones de firewall y router. Dicho sistema operativo es pfSense.

pfSense

pfSense es una distribución gratuita y open source de FreeBSD adaptada para su uso como cortafuegos y router. Además de ser una potente y flexible plataforma de cortafuegos y de enrutamiento, incluye una larga lista de características relacionadas y un sistema de paquetes que permite la adición de características adicionales.

Requisitos mínimos de hardware

- Procesador de 100MHz (Pentium).
- 128MB en RAM.
- Disco duro de 1GB.
- CD-ROM para instalación inicial.
- Dos tarjetas de red (NIC).

Equipo SERVER

Se trata de un computador funcionando con Microsoft Windows 2003 Server R2 que actuará como Controlador de Dominio con Active Directory y realizará la autenticación a través de IAS (Internet Authentication Service) y Microsoft SQL Server 2005 Express.

IAS (Internet Authentication Service)

IAS es la implementación de Microsoft de un servidor RADIUS con capacidades AAA (Authentication, Authorization and Accounting; *Autenticación, Autorización y Contabilización*), cuya autenticación se realiza contra los usuarios creados en Active Directory.

Requerimientos del sistema

- Microsoft .NET Framework 2.0.50727
- Microsoft SQL Server 2005 Express.
- 512MB en RAM.
- El espacio en disco de la base de datos depende del uso.
- Privilegios de administrador.

PROCESO DE CONFIGURACIÓN

En equipo ROUTER

Instalación de pfSense

Se arranca el computador con el LiveCD de pfSense, con las interfaces de red físicamente desconectadas. Cuando el programa de instalación pregunta si se desea crear VLANs se responde que no (Figura 2):

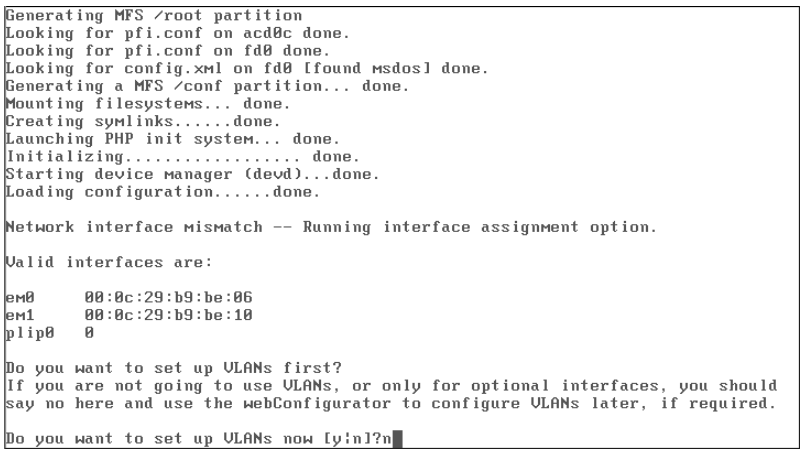


Figura 2. Instalación pfSense, creación de VLANs

Luego se observa una pantalla con las interfaces de red válidas (en este caso em0 y em1). Para asignar la interfaz que se utilizará en la conexión LAN se utiliza la opción 'a' para auto-detección (Figura 3), en este momento se conecta la interfaz de la red interna y pfSense detectará la activación de esta interfaz, se pulsa Enter para continuar.

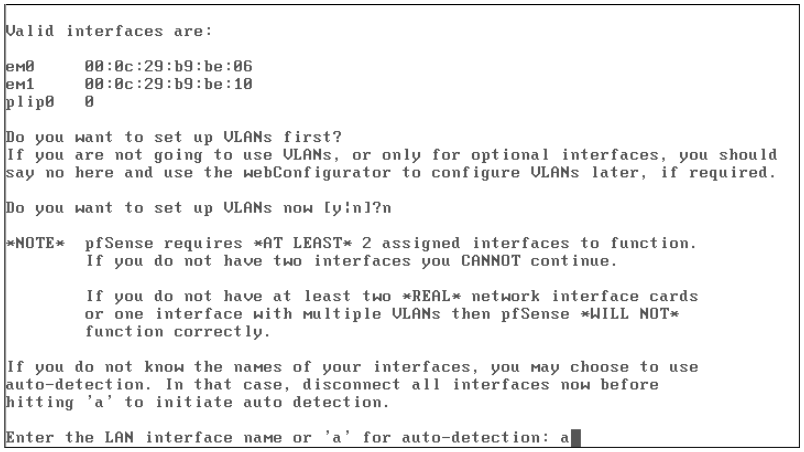


Figura 3. Instalación pfSense, asignación de interfaces por auto-detección

Para la interfaz WAN se realiza el mismo procedimiento con la conexión por la cual se tendrá salida hacia Internet. El programa de instalación preguntará por la asignación de una interfaz opcional, simplemente se pulsa Enter para continuar omitiendo este paso. Se presentará un pequeño resumen de la asignación de interfaces, se confirma con 'y' se da Enter para continuar (Figura 4):

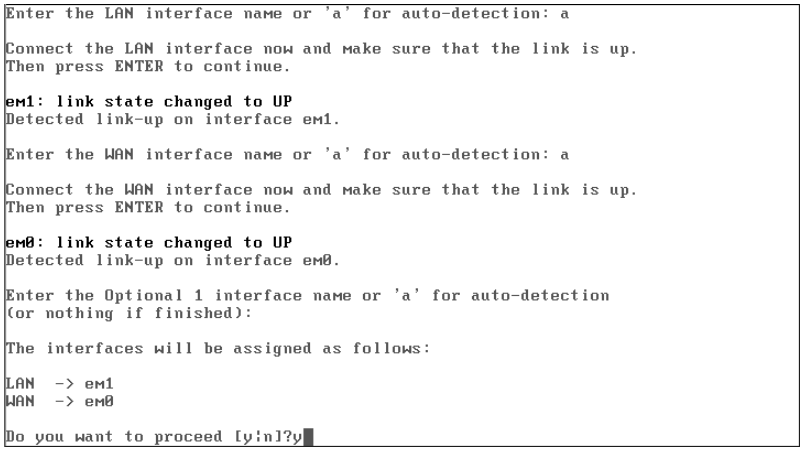


Figura 4. Instalación de pfSense, resumen de asignación de interfaces

Una vez realizado esto, pfSense completa su arranque con la configuración por defecto, es decir, la interfaz WAN busca un servidor DHCP que le asigne una dirección IP, mientras la interfaz LAN tiene la dirección IP estática 192.168.1.1/24, la cual puede ser utilizada para configurar pfSense desde otro equipo de la red a través del ambiente Web.

En el menú que se presenta, la opción 99 permite instalar pfSense en el disco duro del equipo (Figura 5):

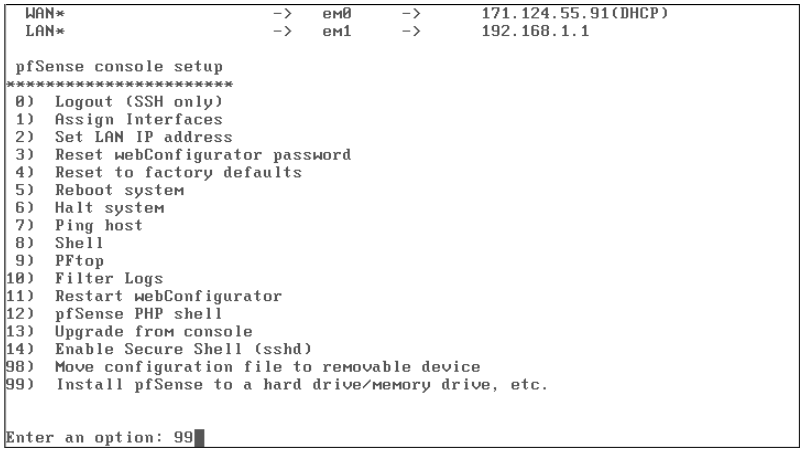


Figura 5. Instalación de pfSense, menú principal

En la primera pantalla que aparece para la instalación como tal, es posible realizar ajustes referentes a la consola, tales como la tipografía, el mapeado de la pantalla y la configuración (distribución) del teclado, se ajustará esta última y para ello se ingresa a la opción Change Keymap (Figura 6):

Figura 6. Instalación de pfSense, configuración del teclado de la consola

Se localiza y selecciona el teclado estándar en español (spanish.iso.kbd), se da Enter, se verifica que ahora junto a Change Keymap aparezca 'spanish.iso' en lugar de 'default' y se acepta esta configuración (Figura 7):

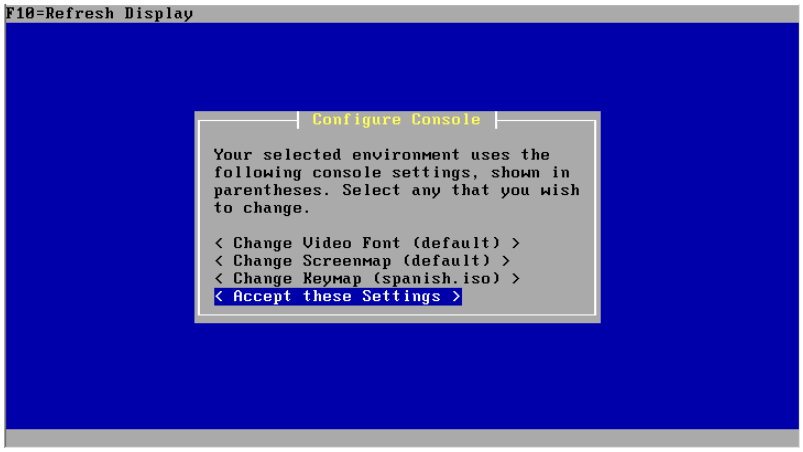


Figura 7. Instalación de pfSense, aceptar configuración de consola

A continuación se escoge la tarea Install pfSense. Aparece una pantalla para escoger el disco en el cual se instalará el sistema en caso de existir más de uno (Figura 8), simplemente se señala el disco y se pulsa Enter para continuar con el proceso de instalación:

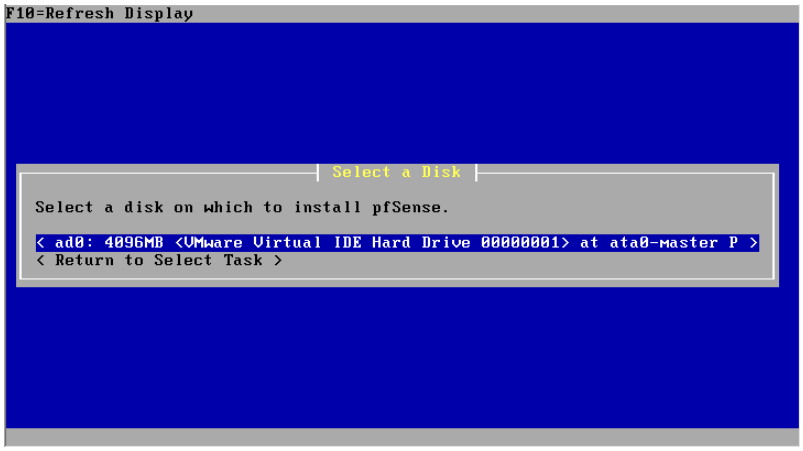


Figura 8. Instalación de pfSense, selección de disco destino

Ahora se muestran varias pantallas que hacen referencia al formateo del disco, la geometría del mismo, y la confirmación de continuar con el formato.

Luego el programa de instalación presenta la opción de crear particiones en caso de que se tenga planificado instalar múltiples sistemas operativos en el equipo (Figura 9), pero esta herramienta se encuentra en fase Beta por lo que su uso es considerado "Bajo su propio riesgo", además es preferible conseguir un disco duro de poca capacidad y destinarlo en su totalidad a pfSense, por tanto se omite este paso.

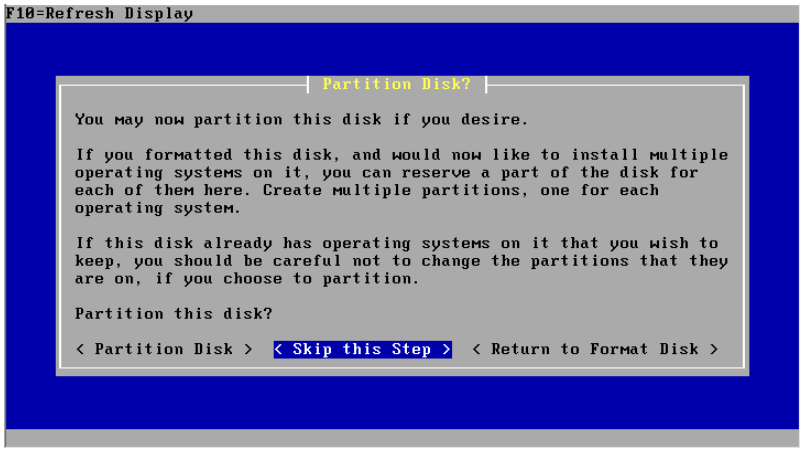


Figura 9. Instalación de pfSense, particionar el disco

Se confirma la partición (totalidad del disco) que utilizará pfSense, la misma que será formateada (Figura 10):

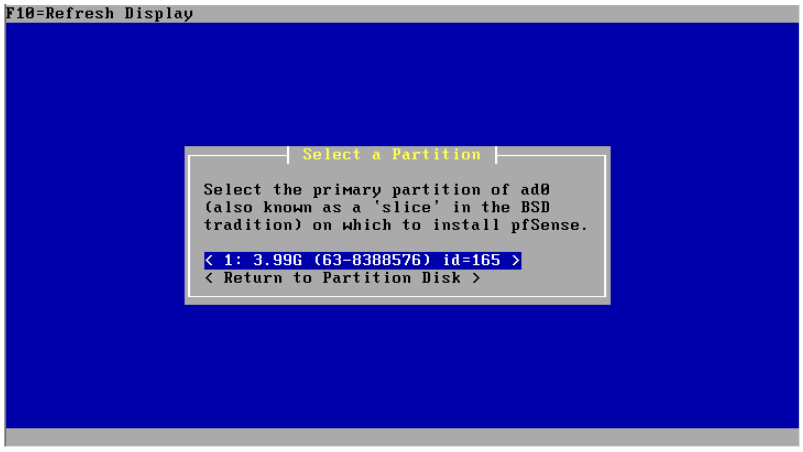


Figura 10. Instalación de pfSense, seleccionar la partición de pfSense

Aparecerá una pantalla para especificar las subparticiones necesarias, es recomendable aceptar la configuración propuesta y continuar, a menos que se tenga una buena comprensión de la estructura de directorios utilizada en sistemas Unix y se requiera alguna característica específica.

En seguida se tiene la posibilidad de especificar el tipo de kernel que mejor se ajuste a las características del equipo para que sea utilizado por el sistema (Figura 11):

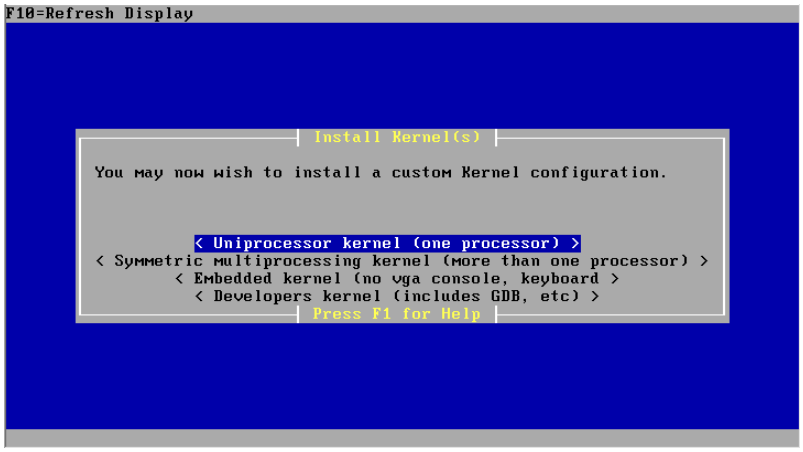


Figura 11. Instalación de pfSense, selección de kernel

El siguiente paso es instalar los Bootblocks, que actuarán como gestor de arranque para el sistema (Figura 12).

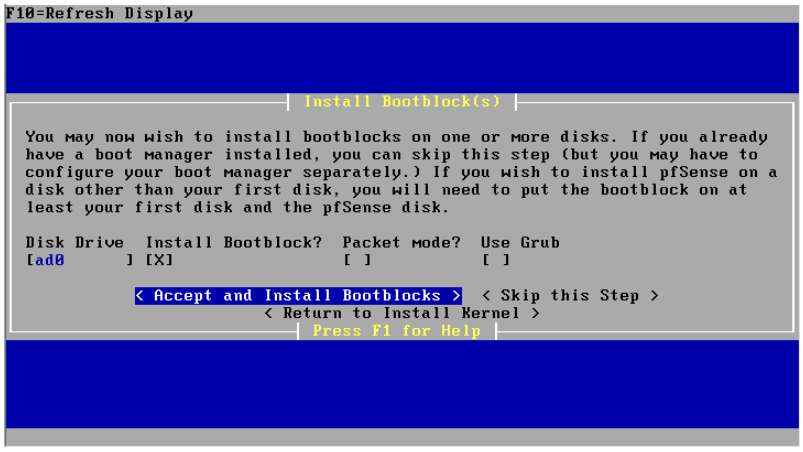


Figura 12. Instalación de pfSense, instalar bootblocks

Luego del mensaje que confirma que los bootblocks se instalaron correctamente aparecerá un diálogo para realizar el reinicio del sistema y la extracción del LiveCD.

Configuración inicial de pfSense

La configuración de pfSense se realiza desde un navegador web de una máquina de la red LAN. Para el ejemplo se utiliza Internet Explorer 6.

En la barra de navegación se escribe la dirección de la interfaz LAN de pfSense (192.168.1.1) y aparece una ventana pop-up para ingresar el usuario (admin) y la contraseña (pfsense) (Figura 13),

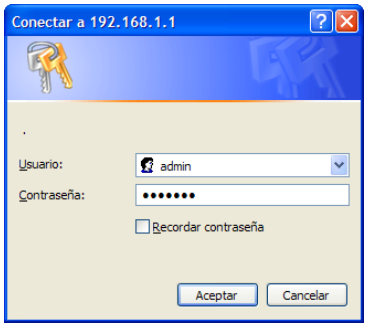


Figura 13. Configuración inicial de pfSense, ingresar usuario y contraseña

La primera vez que se ingresa entorno de configuración web de pfSense aparece un asistente de configuración (wizard) (Figura 14):

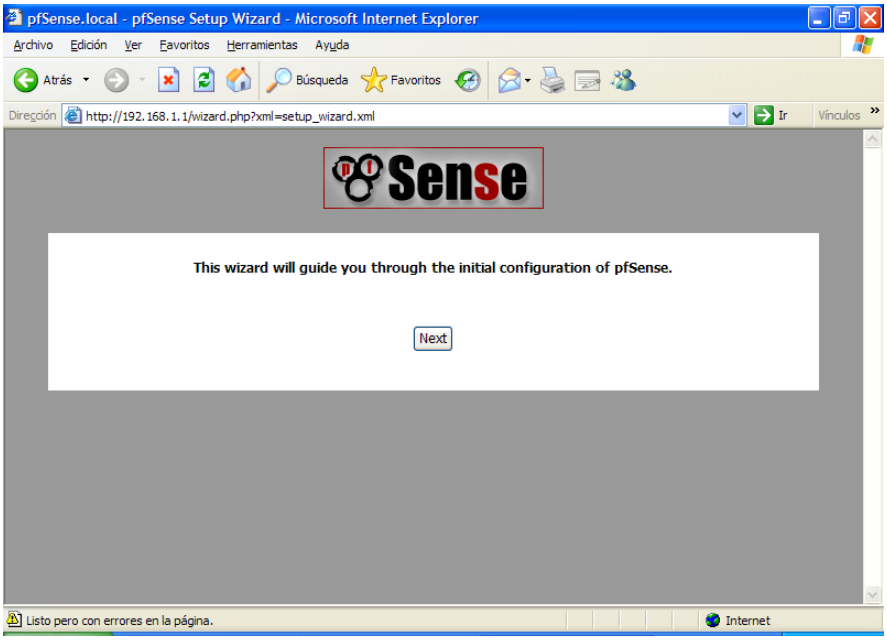


Figura 14. Pantalla de bienvenida al asistente de configuración inicial de pfSense

En la primera pantalla se indica el nombre con que se reconocerá el equipo en la red (en este caso 'router'), el dominio (en este caso 'biblioteca.fisei'), y la dirección del servidor DNS del dominio (Figura 15).

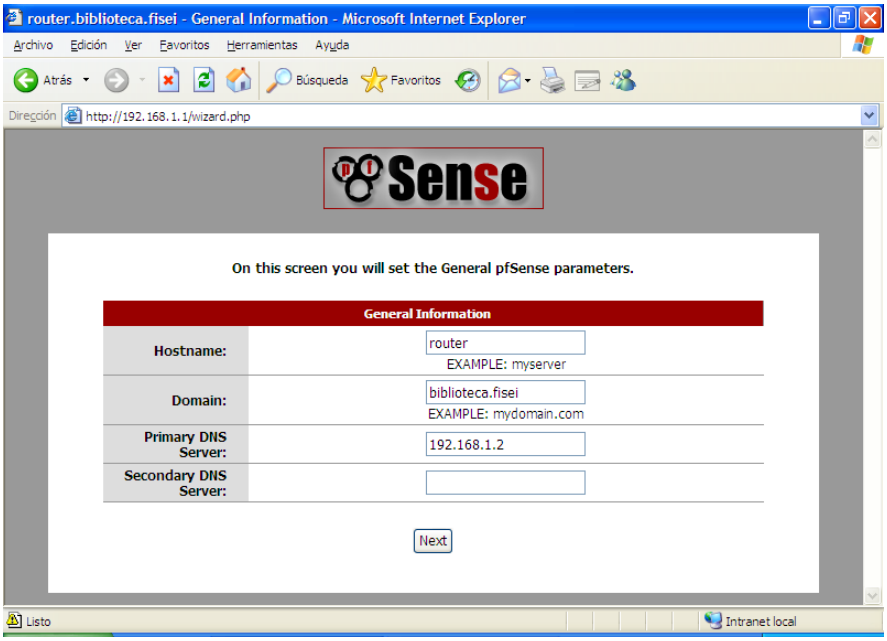


Figura 15. pfSense. Nombre de equipo, dominio y servidores DNS

En la segunda pantalla se especifica la zona horaria (Figura 16):

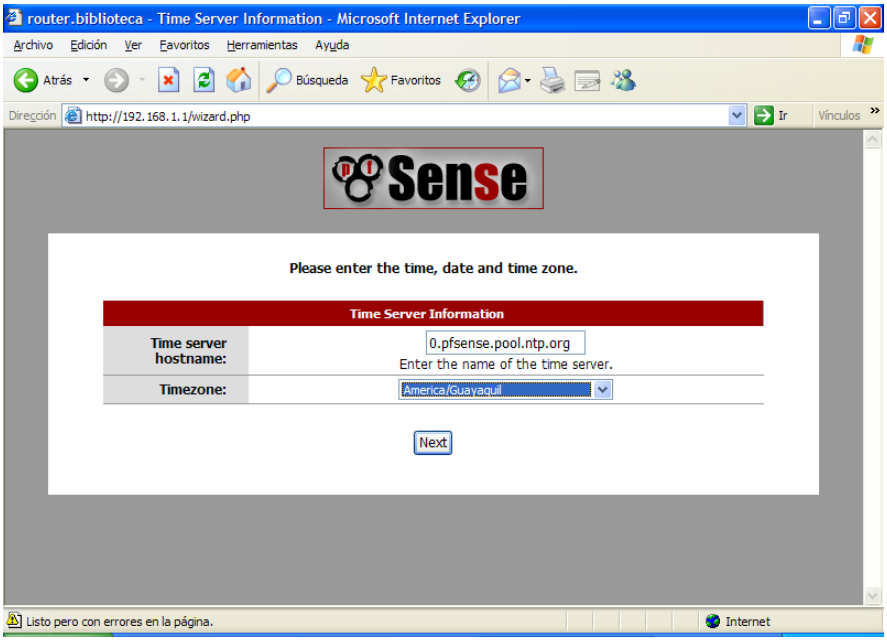


Figura 16. pfSense. Zona horaria

La tercera pantalla permite configurar la interfaz de conexión WAN, en la configuración de ejemplo se deja en DHCP (Figura 17), al final de la página se encuentra el botón para avanzar a la siguiente página.

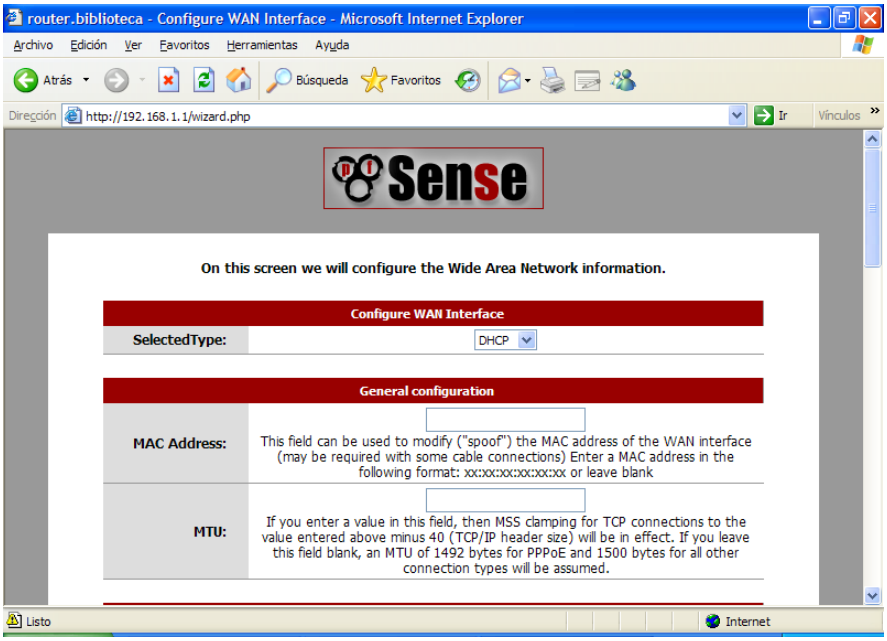


Figura 17. pfSense. Configuración de interfaz WAN

La cuarta pantalla permite configurar la interfaz de conexión LAN (Figura 18).

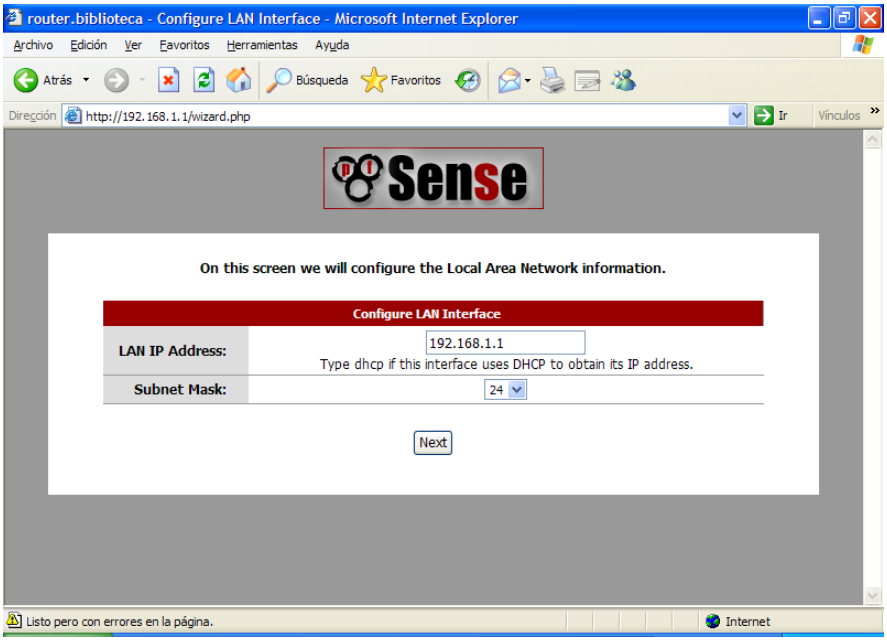


Figura 18. pfSense. Configuración de interfaz LAN

En la quinta pantalla se especifica una nueva contraseña para pfSense (Figura 19):

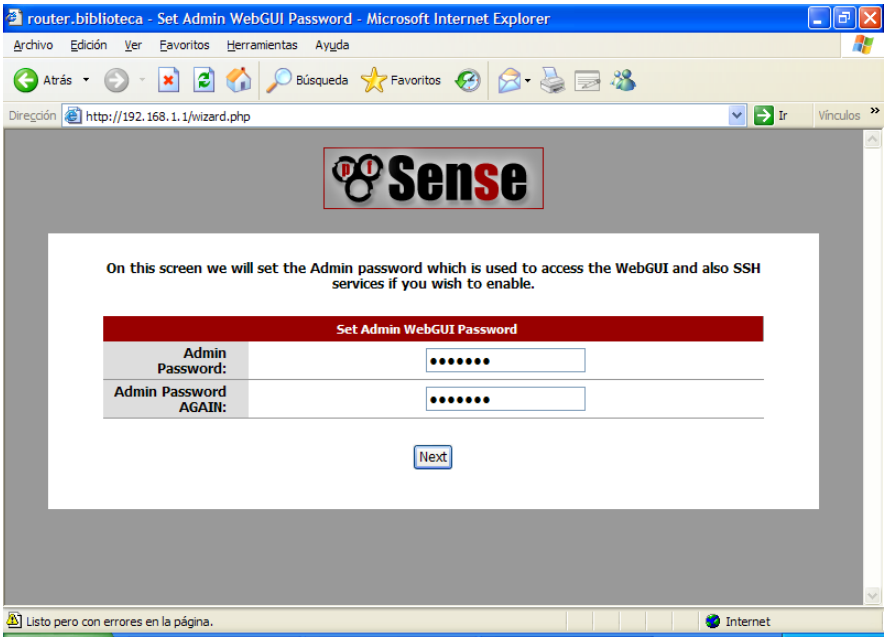


Figura 19. pfSense. Configuración de la contraseña de pfSense

La sexta pantalla sirve para recargar pfSense con la nueva configuración (Figura 20):

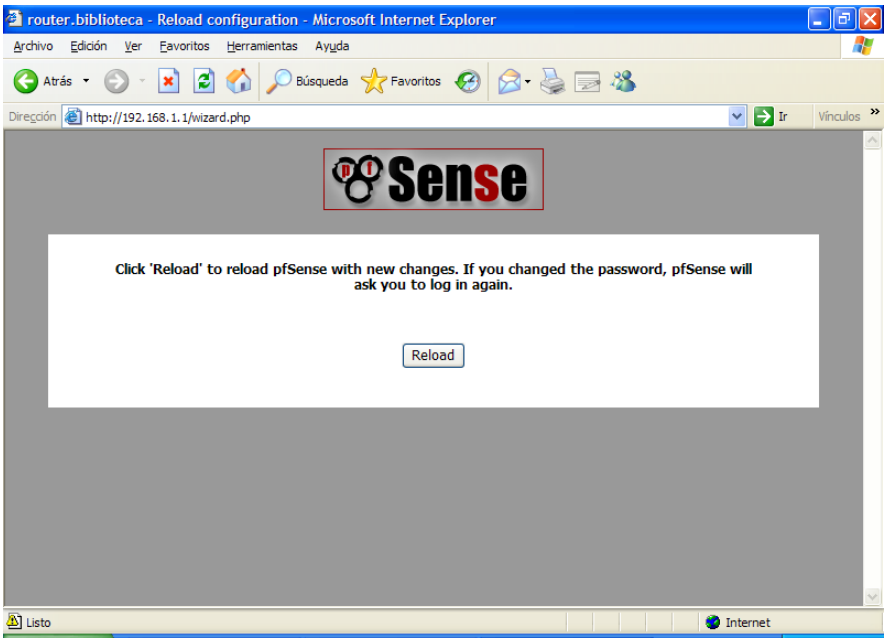


Figura 20. pfSense. Recargar la configuración

La última pantalla realiza una espera de 120 segundos para reingresar a la configuración de pfSense (Figura 21).

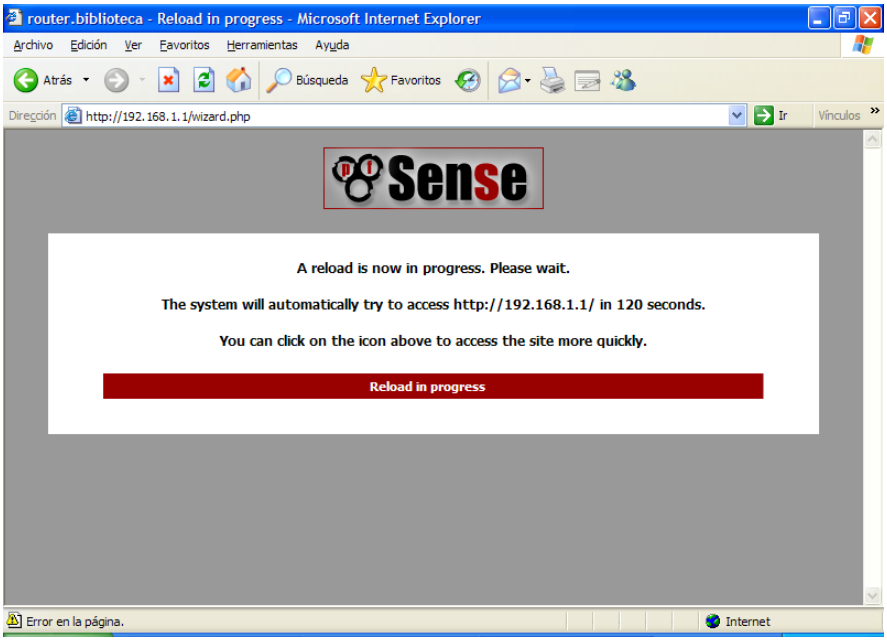


Figura 21. pfSense. Recarga en proceso

Si no apareció el asistente, es posible llamarlo desde el mismo ambiente en el menu System.

Configuración del portal cautivo

Para llevar a cabo la configuración del servicio de portal cautivo se accede, desde el entorno de configuración de pfSense, a la opción Captive portal dentro del menú Services (Figura 22):

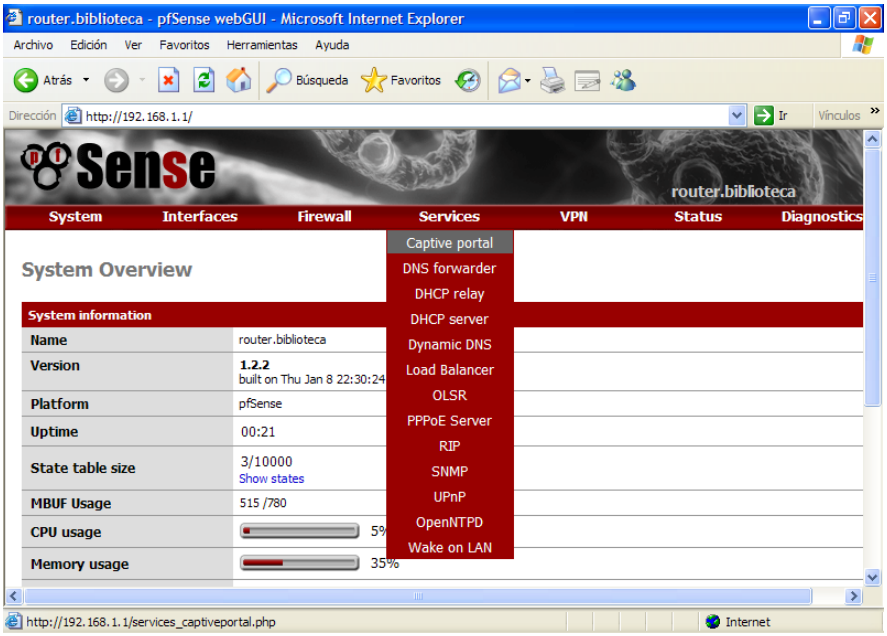


Figura 22. Portal cautivo, ingreso a la configuración del servicio

En la pantalla de configuración del servicio, se lo habilita colocando un visto en Enable captive portal, en Interface se selecciona LAN.

El parámetro Maximum concurrent connections especifica en cuántas terminales puede cargarse simultáneamente el portal cautivo (no hace referencia al número máximo de usuarios simultaneos) por tanto se establece el valor 0 que anula este límite.

En el parámetro Idle timeout se coloca un valor en minutos que será el tiempo de inactividad tras el cual el sistema expulsará automáticamente al usuario.

El parámetro Hard timeout sirve para especificar un tiempo en el cual sin importar la actividad o inactividad se expulsa al usuario (para este caso se especifica 60 minutos), aunque este puede reingresar inmediatamente realizando el proceso de login.

En este punto cabe aclarar que la autorización de uso de Internet se realiza al momento del login y la contabilización al momento del logout; por lo cual se podría dar el caso extremo de que un usuario haya consumido 9 horas, 59 minutos, y 59 segundos, es decir, tiene 1 segundo disponible por tanto el sistema le permitirá el uso de Internet, lo que aparentemente sería un error, pero si se considera que el usuario podría necesitar guardar las páginas que ha consultado y que forzosamente el sistema realizará un logout al cabo del tiempo especificado

en este parámetro (si no ocurriera que el usuario mismo ya ha cerrado su sesión), se le estará brindando al estudiante una concesión de máximo de 60 minutos para terminar sus tareas.

Se habilita la ventana pop-up de salida (Logout popup window) para que el usuario tengo la posibilidad de desconectarse a sí mismo del servicio (Figura 23).

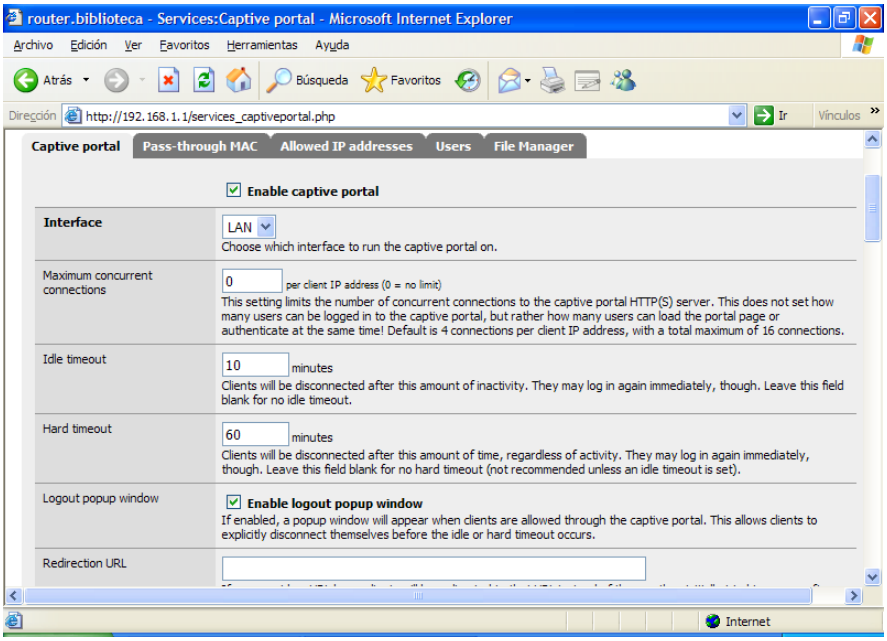


Figura 23. Portal cautivo. Configuración (parte 1)

La opción Disable concurrent logins elimina la posibilidad de que un usuario pueda iniciar sesión en más de un equipo a la vez. Solamente el último inicio de sesión es válido mientras que los demás se bloquean.

Se especifica la utilización de la Autenticación RADIUS, se incluye la dirección IP (192.168.1.2) y puerto (1812) del servidor RADIUS primario, y la palabra secreta para la encriptación de la conexión (fisei) (Figura 24):

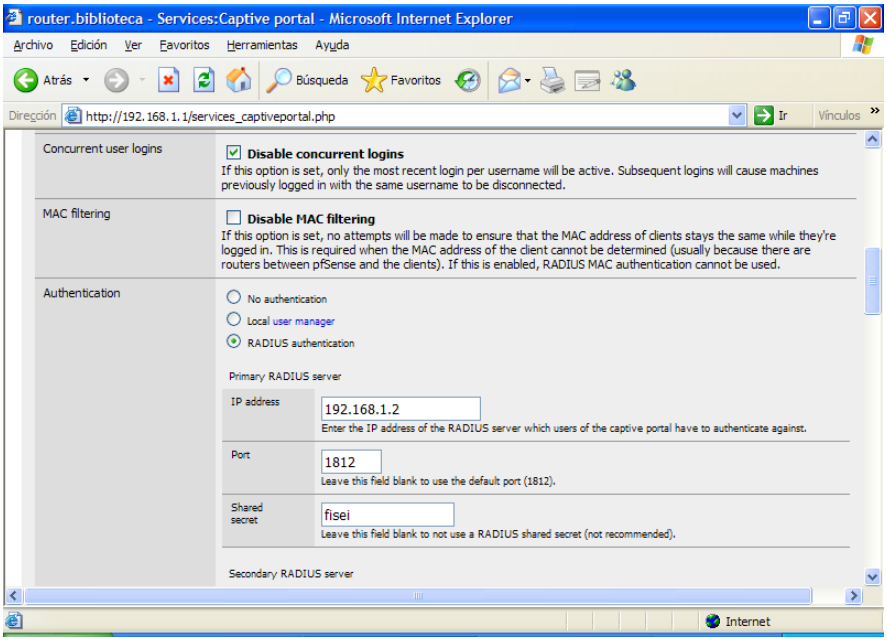


Figura 24. Portal cautivo. Configuración (parte 2)

Se habilita la contabilización (Accounting) en la sección correspondiente y se define el puerto del servicio (1813) (Figura 25):

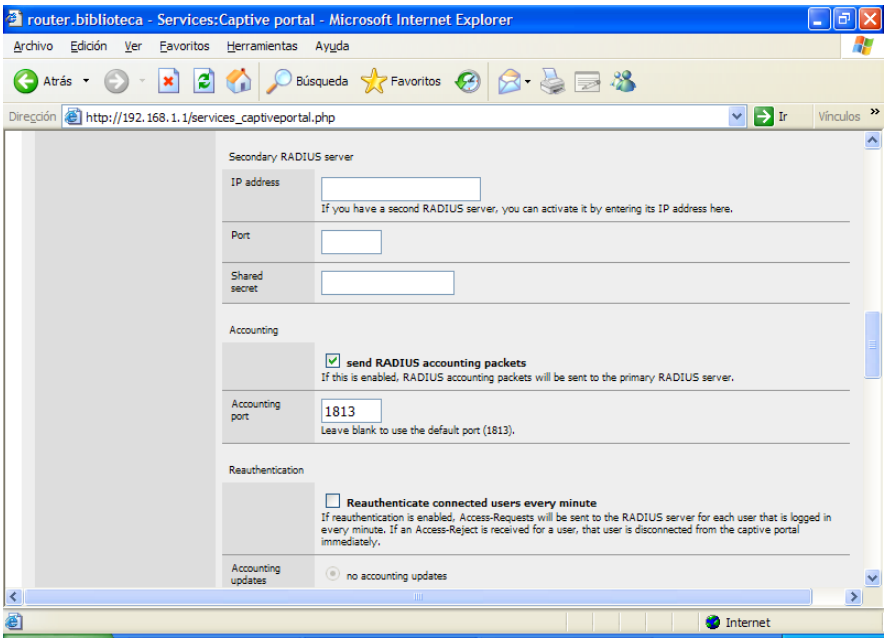


Figura 25. Portal cautivo. Configuración (parte 3)

En la parte inferior de la página se encuentra el botón Guardar (Save) que al mismo tiempo que guarda la configuración, inicia el servicio.

Configuración servidor DHCP

Es buena idea verificar que el servicio de Servidor DHCP se encuentre habilitado, para lo cual se accede a la opción DCHP server también en el menú Services (Figura 26).

Figura 26. Servidor DHCP

Una vez abierta la página de configuración se chequea que exista un visto en la opción Enable DHCP server on LAN interface (Figura 27). Esta pantalla también permite especificar el rango de direcciones que podrá ofrecer el servidor DHCP.

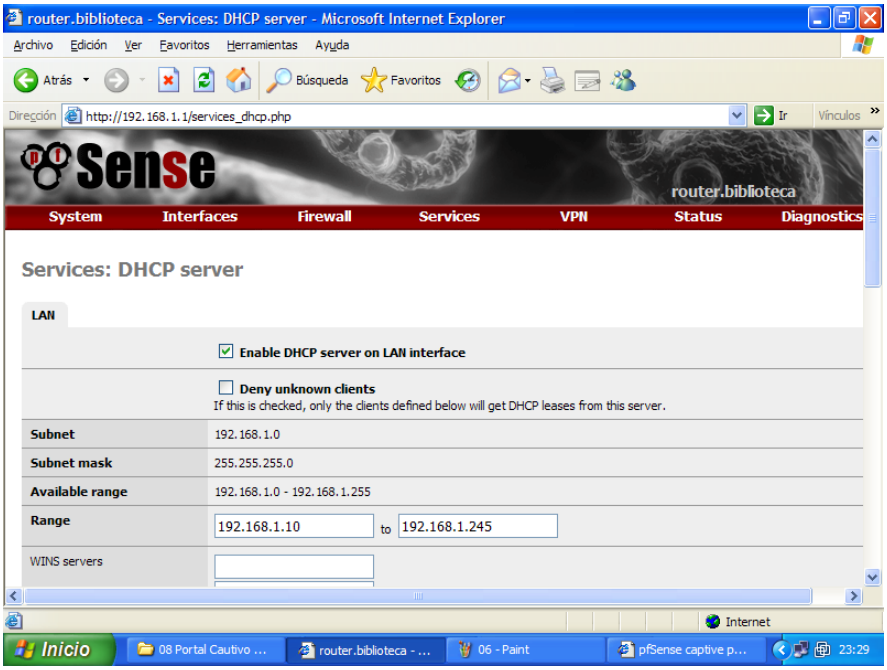


Figura 27. Configuración del servidor DHCP

En el equipo SERVER

Este equipo tiene como sistema operativo a Microsoft Windows 2003 Server, el cual debe ser un Controlador de dominio (biblioteca.fisei), por tanto tener correctamente configurado los servicios de Active Directory y DNS, considerando que su dirección IP sea la que se especifica en la Figura 28.

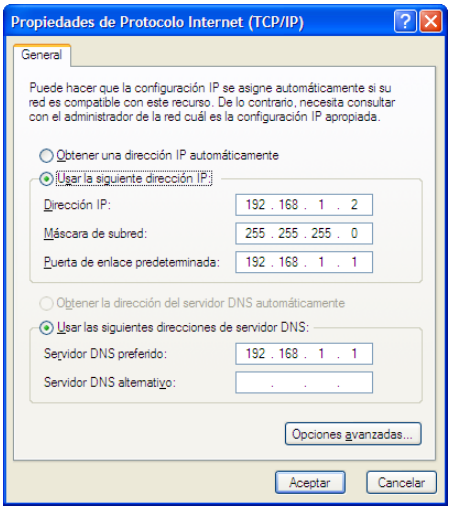


Figura 28. Configuración IP en Windows 2003 Server

También en el servidor DNS se debe incluir al equipo router (192.168.1.1) como parte del dominio para que las consultas puedan ser resueltas.

En Active Directory es necesario crear un grupo de seguridad de ámbito global cuyo nombre sea UsuariosInternet que más adelante contendrá los usuarios con permiso de acceder al servicio de Internet.

Adicionalmente se requiere la desactivación de las políticas de uso de contraseñas seguras para que los usuarios puedan utilizar su número de Cédula como contraseña.

Una vez tomadas en cuenta las consideraciones anteriores se verifica que se encuentren instalados .Net Framework 2.0 y Windows Installer 3.1.

Instalación de Microsoft SQL Server 2005 Express

Para el log IAS puede trabajar con archivos de texto o con base de datos de SQL Server. Para realizar tareas de accounting, es preferible utilizar la opción de la base de datos.

En este caso se usará la versión Express (gratuita) de Microsoft SQL Server 2005.

Lo importante durante la instalación es establecer en la pantalla correspondiente que, por el momento, se utilizará el Modo de autenticación de Windows (Figura 29).

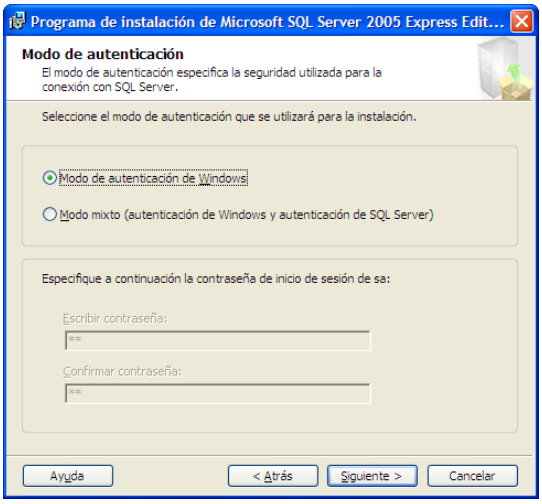


Figura 29. Modo de autenticación Windows

Instalación de SQL Server Management Studio Express

La versión Express de Microsoft SQL Server no incluye la herramienta de administración, por tanto es necesario instalarla por separado. Esta herramienta es esencial puesto que desde allí se puede crear los procedimientos almacenados y disparadores necesarios para el obtener el funcionamiento deseado.

Configuración de la cuenta del usuario 'sa'

Pese a que durante la instalación se estableció el 'Modo de autenticación Windows' para acceder a SQL Server, es preferible que la conexión se realice con 'Modo mixto' utilizando, generalmente, el usuario 'sa' de SQL Server, sin embargo esta cuenta se encuentra deshabilitada; para poder hacer uso de ella se realiza el siguiente proceso:

Ingresar a SQL Server Management Studio Express con Autenticación de Windows (Figura 30):

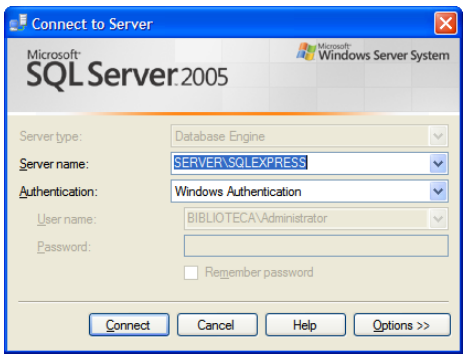


Figura 30. Ingreso a SQL Server Management Studio con Autenticación Windows

Clic derecho en el servidor y acceder a Propiedades, a la página de Seguridad, y escoger el Modo de Autenticación de Windows y SQL Server (Figura 31):

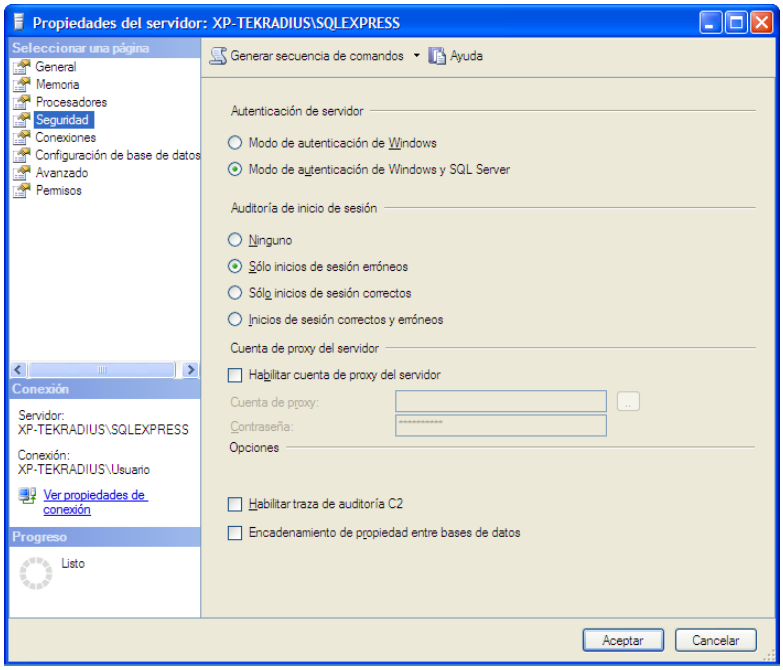


Figura 31. Propiedades del servidor SQL, página de Seguridad

Tras dar clic en Aceptar se recibe el aviso de que es necesario reiniciar el servicio de SQL Server para que los cambios surtan efecto. Se lo hace con clic derecho en el servidor, escoger Reiniciar (Figura 32):

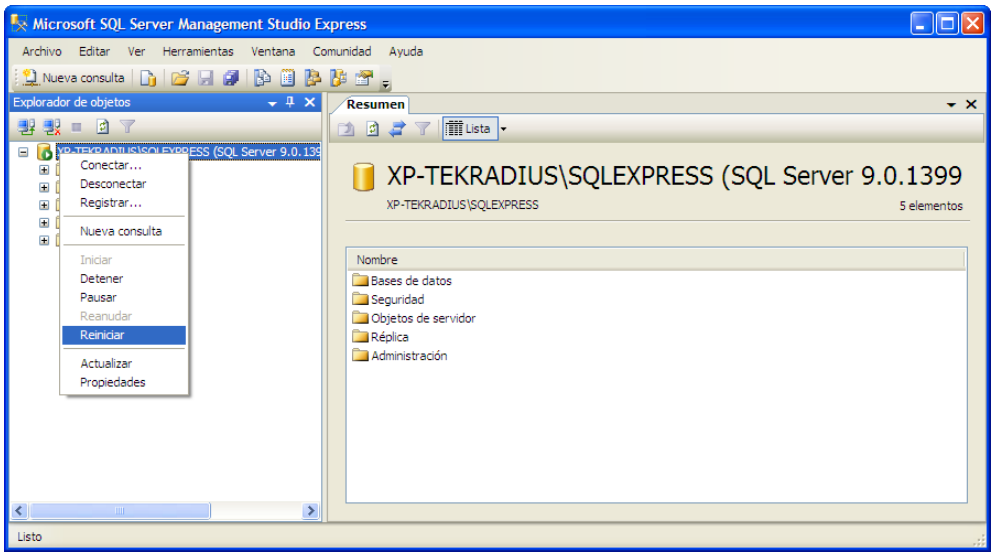


Figura 32. Reiniciar servicio de SQL Server

Ahora se expande el directorio Seguridad, dentro de él se expande Inicios de sesión. Clic derecho en el usuario 'sa' y acceder a Propiedades; en la página General se indica y confirma la contraseña para este usuario (Figura 33):

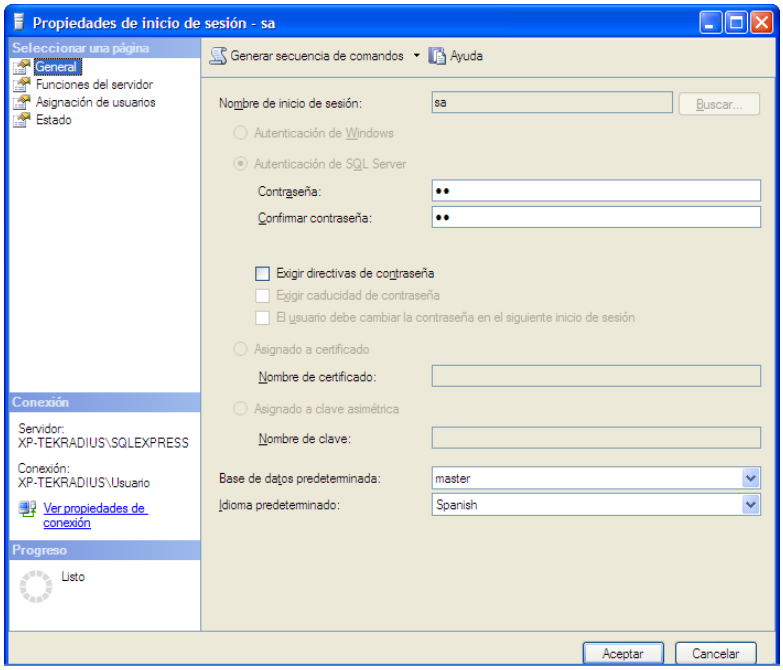


Figura 33. Propiedades del usuario 'sa', página General

A continuación se pasa a la página Estado, y se coloca el Inicio de sesión en 'Habilitada' (Figura 34):

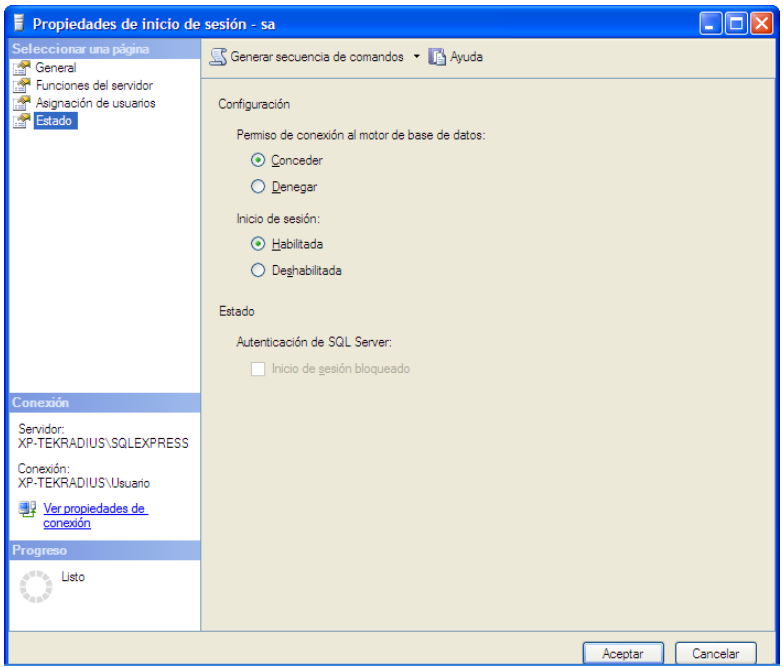


Figura 34. Propiedades del usuario 'sa', página Estado

Clic en Aceptar. Para comprobar que ha quedado habilitada la cuenta 'sa' es recomendable desconectarse del servidor dando clic derecho en él y escogiendo Desconectar; para reconectar accedemos 'Conectar Explorador de objetos…' en el menú Archivo, aparecerá el cuadro de ingreso a SQL Server 2005, pero ahora se escoge la Autenticación de SQL Server y se especifica el usuario y contraseña (Figura 35):

Figura 35. Ingreso a SQL Server Management Studio con usuario 'sa'

Si la conexión es exitosa se procede al siguiente paso de la configuración, caso contrario se verifica los pasos anteriores iniciando sesión nuevamente con Autenticación de Windows.

Creación de la base de datos

Para que IAS almacene su log en SQL Server 2005 Express es necesario crear una base de datos capaz de recoger toda la información generada. Esto se realiza fácilmente con un script disponible en el sitio web de Microsoft (http://technet.microsoft.com/en-us/library/cc778830(WS.10).aspx) y que se muestra a continuación:

```
IF EXISTS (SELECT name FROM master.dbo.sysdatabases WHERE name =
N'IASODBC')
      DROP DATABASE [IASODBC]
GO

CREATE DATABASE [IASODBC]  ON (NAME = N'IASODBC_Data', FILENAME =
N'C:\Program Files\Microsoft SQL Server\MSSQL\data\IASODBC_Data.MDF' ,
SIZE = 1, FILEGROWTH = 10%) LOG ON (NAME = N'IASODBC_Log', FILENAME =
N'C:\Program Files\Microsoft SQL Server\MSSQL\data\IASODBC_Log.LDF' ,
SIZE = 1, FILEGROWTH = 10%)
 COLLATE SQL_Latin1_General_CP1_CI_AS
GO

exec sp_dboption N'IASODBC', N'autoclose', N'false'
GO

exec sp_dboption N'IASODBC', N'bulkcopy', N'false'
```

```
GO

exec sp_dboption N'IASODBC', N'trunc. log', N'false'
GO

exec sp_dboption N'IASODBC', N'torn page detection', N'true'
GO

exec sp_dboption N'IASODBC', N'read only', N'false'
GO

exec sp_dboption N'IASODBC', N'dbo use', N'false'
GO

exec sp_dboption N'IASODBC', N'single', N'false'
GO

exec sp_dboption N'IASODBC', N'autoshrink', N'false'
GO

exec sp_dboption N'IASODBC', N'ANSI null default', N'false'
GO

exec sp_dboption N'IASODBC', N'recursive triggers', N'false'
GO

exec sp_dboption N'IASODBC', N'ANSI nulls', N'false'
GO

exec sp_dboption N'IASODBC', N'concat null yields null', N'false'
GO

exec sp_dboption N'IASODBC', N'cursor close on commit', N'false'
GO

exec sp_dboption N'IASODBC', N'default to local cursor', N'false'
GO

exec sp_dboption N'IASODBC', N'quoted identifier', N'false'
GO

exec sp_dboption N'IASODBC', N'ANSI warnings', N'false'
GO

exec sp_dboption N'IASODBC', N'auto create statistics', N'true'
GO

exec sp_dboption N'IASODBC', N'auto update statistics', N'true'
GO

if( ( (@@microsoftversion / power(2, 24) = 8) and (@@microsoftversion &
0xffff >= 724) ) or ( (@@microsoftversion / power(2, 24) = 7) and
(@@microsoftversion & 0xffff >= 1082) ) )
      exec sp_dboption N'IASODBC', N'db chaining', N'false'
GO

use [IASODBC]
GO

if exists (select * from dbo.sysobjects where id =
object_id(N'[dbo].[report_event]') and OBJECTPROPERTY(id, N'IsProcedure')
= 1)
drop procedure [dbo].[report_event]
GO
```

```
if exists (select * from dbo.sysobjects where id =
object_id(N'[dbo].[accounting_data]') and OBJECTPROPERTY(id,
N'IsUserTable') = 1)
drop table [dbo].[accounting_data]
GO

if exists (select * from dbo.systypes where name = N'ipaddress')
exec sp_droptype N'ipaddress'
GO

setuser
GO

EXEC sp_addtype N'ipaddress', N'nvarchar (15)', N'not null'
GO

setuser
GO

CREATE TABLE [dbo].[accounting_data] (
       [id] [int] IDENTITY (1, 1) NOT NULL ,
       [timestamp] [datetime] NOT NULL ,
       [Computer_Name] [nvarchar] (255) COLLATE
SQL_Latin1_General_CP1_CI_AS NOT NULL ,
       [Packet_Type] [int] NOT NULL ,
       [User_Name] [nvarchar] (255) COLLATE SQL_Latin1_General_CP1_CI_AS
NULL ,
       [F_Q_User_Name] [nvarchar] (255) COLLATE
SQL_Latin1_General_CP1_CI_AS NULL ,
       [Called_Station_Id] [nvarchar] (255) COLLATE
SQL_Latin1_General_CP1_CI_AS NULL ,
       [Calling_Station_Id] [nvarchar] (255) COLLATE
SQL_Latin1_General_CP1_CI_AS NULL ,
       [Callback_Number] [nvarchar] (255) COLLATE
SQL_Latin1_General_CP1_CI_AS NULL ,
       [Framed_IP_Address] [ipaddress] NULL ,
       [NAS_Identifier] [nvarchar] (255) COLLATE
SQL_Latin1_General_CP1_CI_AS NULL ,
       [NAS_IP_Address] [ipaddress] NULL ,
       [NAS_Port] [int] NULL ,
       [Client_Vendor] [int] NULL ,
       [Client_IP_Address] [ipaddress] NULL ,
       [Client_Friendly_Name] [nvarchar] (255) COLLATE
SQL_Latin1_General_CP1_CI_AS NULL ,
       [Event_Timestamp] [datetime] NULL ,
       [Port_Limit] [int] NULL ,
       [NAS_Port_Type] [int] NULL ,
       [Connect_Info] [nvarchar] (255) COLLATE
SQL_Latin1_General_CP1_CI_AS NULL ,
       [Framed_Protocol] [int] NULL ,
       [Service_Type] [int] NULL ,
       [Authentication_Type] [int] NULL ,
       [NP_Policy_Name] [nvarchar] (255) COLLATE
SQL_Latin1_General_CP1_CI_AS NULL ,
       [Reason_Code] [int] NULL ,
       [Class] [nvarchar] (255) COLLATE SQL_Latin1_General_CP1_CI_AS NULL
,
       [Session_Timeout] [int] NULL ,
       [Idle_Timeout] [int] NULL ,
       [Termination_Action] [int] NULL ,
       [EAP_Friendly_Name] [nvarchar] (255) COLLATE
SQL_Latin1_General_CP1_CI_AS NULL ,
       [Acct_Status_Type] [int] NULL ,
```

```
	[Acct_Delay_Time] [int] NULL ,
	[Acct_Input_Octets] [int] NULL ,
	[Acct_Output_Octets] [int] NULL ,
	[Acct_Session_Id] [nvarchar] (255) COLLATE
SQL_Latin1_General_CP1_CI_AS NULL ,
	[Acct_Authentic] [int] NULL ,
	[Acct_Session_Time] [int] NULL ,
	[Acct_Input_Packets] [int] NULL ,
	[Acct_Output_Packets] [int] NULL ,
	[Acct_Terminate_Cause] [int] NULL ,
	[Acct_Multi_Session_Id] [nvarchar] (255) COLLATE
SQL_Latin1_General_CP1_CI_AS NULL ,
	[Acct_Link_Count] [int] NULL ,
	[Acct_Interim_Interval] [int] NULL ,
	[Tunnel_Type] [int] NULL ,
	[Tunnel_Medium_Type] [int] NULL ,
	[Tunnel_Client_Endpoint] [nvarchar] (255) COLLATE
SQL_Latin1_General_CP1_CI_AS NULL ,
	[Tunnel_Server_Endpoint] [nvarchar] (255) COLLATE
SQL_Latin1_General_CP1_CI_AS NULL ,
	[Acct_Tunnel_Connection] [nvarchar] (255) COLLATE
SQL_Latin1_General_CP1_CI_AS NULL ,
	[Tunnel_Pvt_Group_Id] [nvarchar] (255) COLLATE
SQL_Latin1_General_CP1_CI_AS NULL ,
	[Tunnel_Assignment_Id] [nvarchar] (255) COLLATE
SQL_Latin1_General_CP1_CI_AS NULL ,
	[Tunnel_Preference] [int] NULL ,
	[MS_Acct_Auth_Type] [int] NULL ,
	[MS_Acct_EAP_Type] [int] NULL ,
	[MS_RAS_Version] [nvarchar] (255) COLLATE
SQL_Latin1_General_CP1_CI_AS NULL ,
	[MS_RAS_Vendor] [int] NULL ,
	[MS_CHAP_Error] [nvarchar] (255) COLLATE
SQL_Latin1_General_CP1_CI_AS NULL ,
	[MS_CHAP_Domain] [nvarchar] (255) COLLATE
SQL_Latin1_General_CP1_CI_AS NULL ,
	[MS_MPPE_Encryption_Types] [int] NULL ,
	[MS_MPPE_Encryption_Policy] [int] NULL ,
	[Proxy_Policy_Name] [nvarchar] (255) COLLATE
SQL_Latin1_General_CP1_CI_AS NULL ,
	[Provider_Type] [int] NULL ,
	[Provider_Name] [nvarchar] (255) COLLATE
SQL_Latin1_General_CP1_CI_AS NULL ,
	[Remote_Server_Address] [ipaddress] NULL ,
	[MS_RAS_Client_Name] [nvarchar] (255) COLLATE
SQL_Latin1_General_CP1_CI_AS NULL ,
	[MS_RAS_Client_Version] [nvarchar] (255) COLLATE
SQL_Latin1_General_CP1_CI_AS NULL
) ON [PRIMARY]
GO

SET QUOTED_IDENTIFIER ON
GO
SET ANSI_NULLS OFF
GO

CREATE PROCEDURE dbo.report_event
   @doc ntext
AS

SET NOCOUNT ON

DECLARE @idoc int
EXEC sp_xml_preparedocument @idoc OUTPUT, @doc
```

```
/*
       All RADIUS attributes written to the ODBC format logfile are
declared here.  One additional attribute is added: @record_timestamp.
       The value of @record_timestamp is the UTC time the record was
inserted in the database.

       Refer to IAS ODBC Formatted Log Files in Online Help for
information on interpreting these values.
*/

DECLARE @record_timestamp datetime

SET @record_timestamp = GETUTCDATE()

INSERT accounting_data
SELECT
       @record_timestamp,
       Computer_Name,
       Packet_Type,
       [User_Name],
       F_Q_User_Name,
       Called_Station_Id,
       Calling_Station_Id,
       Callback_Number,
       Framed_IP_Address,
       NAS_Identifier,
       NAS_IP_Address,
       NAS_Port,
       Client_Vendor,
       Client_IP_Address,
       Client_Friendly_Name,
       Event_Timestamp,
       Port_Limit,
       NAS_Port_Type,
       Connect_Info,
       Framed_Protocol,
       Service_Type,
       Authentication_Type,
       NP_Policy_Name,
       Reason_Code,
       Class,
       Session_Timeout,
       Idle_Timeout,
       Termination_Action,
       EAP_Friendly_Name,
       Acct_Status_Type,
       Acct_Delay_Time,
       Acct_Input_Octets,
       Acct_Output_Octets,
       Acct_Session_Id,
       Acct_Authentic,
       Acct_Session_Time,
       Acct_Input_Packets,
       Acct_Output_Packets,
       Acct_Terminate_Cause,
       Acct_Multi_Session_Id,
       Acct_Link_Count,
       Acct_Interim_Interval,
       Tunnel_Type,
       Tunnel_Medium_Type,
       Tunnel_Client_Endpoint,
       Tunnel_Server_Endpoint,
       Acct_Tunnel_Connection,
```

```
        Tunnel_Pvt_Group_Id,
        Tunnel_Assignment_Id,
        Tunnel_Preference,
        MS_Acct_Auth_Type,
        MS_Acct_EAP_Type,
        MS_RAS_Version,
        MS_RAS_Vendor,
        MS_CHAP_Error,
        MS_CHAP_Domain,
        MS_MPPE_Encryption_Types,
        MS_MPPE_Encryption_Policy,
        Proxy_Policy_Name,
        Provider_Type,
        Provider_Name,
        Remote_Server_Address,
        MS_RAS_Client_Name,
        MS_RAS_Client_Version
FROM OPENXML(@idoc, '/Event')
WITH (
        Computer_Name nvarchar(255) './Computer-Name',
        Packet_Type int './Packet-Type',
        [User_Name] nvarchar(255) './User-Name',
        F_Q_User_Name nvarchar(255) './Fully-Qualifed-User-Name',
        Called_Station_Id nvarchar(255) './Called-Station-Id',
        Calling_Station_Id nvarchar(255) './Calling-Station-Id',
        Callback_Number nvarchar(255) './Callback-Number',
        Framed_IP_Address nvarchar(15) './Framed-IP-Address',
        NAS_Identifier nvarchar(255) './NAS-Identifier',
        NAS_IP_Address nvarchar(15) './NAS-IP-Address',
        NAS_Port int './NAS-Port',
        Client_Vendor int './Client-Vendor',
        Client_IP_Address nvarchar(15) './Client-IP-Address',
        Client_Friendly_Name nvarchar(255) './Client-Friendly-Name',
        Event_Timestamp datetime './Event-Timestamp',
        Port_Limit int './Port-Limit',
        NAS_Port_Type int './NAS-Port-Type',
        Connect_Info nvarchar(255) './Connect-Info',
        Framed_Protocol int './Framed-Protocol',
        Service_Type int './Service-Type',
        Authentication_Type int './Authentication-Type',
        NP_Policy_Name nvarchar(255) './NP-Policy-Name',
        Reason_Code int './Reason-Code',
        Class nvarchar(255) './Class',
        Session_Timeout int './Session-Timeout',
        Idle_Timeout int './Idle-Timeout',
        Termination_Action int './Termination-Action',
        EAP_Friendly_Name nvarchar(255) './EAP-Friendly-Name',
        Acct_Status_Type int './Acct-Status-Type',
        Acct_Delay_Time int './Acct-Delay-Time',
        Acct_Input_Octets int './Acct-Input-Octets',
        Acct_Output_Octets int './Acct-Output-Octets',
        Acct_Session_Id nvarchar(255) './Acct-Session-Id',
        Acct_Authentic int './Acct-Authentic',
        Acct_Session_Time int './Acct-Session-Time',
        Acct_Input_Packets int './Acct-Input-Packets',
        Acct_Output_Packets int './Acct-Output-Packets',
        Acct_Terminate_Cause int './Acct-Terminate-Cause',
        Acct_Multi_Session_Id nvarchar(255) './Acct-Multi-Session-Id',
        Acct_Link_Count int './Acct-Link-Count',
        Acct_Interim_Interval int './Acct-Interim-Interval',
        Tunnel_Type int './Tunnel-Type',
        Tunnel_Medium_Type int './Tunnel-Medium-Type',
        Tunnel_Client_Endpoint nvarchar(255) './Tunnel-Client-Endpt',
        Tunnel_Server_Endpoint nvarchar(255) './Tunnel-Server-Endpt',
```

```
	Acct_Tunnel_Connection nvarchar(255) './Acct-Tunnel-Connection',
	Tunnel_Pvt_Group_Id nvarchar(255) './Tunnel-Pvt-Group-Id',
	Tunnel_Assignment_Id nvarchar(255) './Tunnel-Assignment-Id',
	Tunnel_Preference int './Tunnel-Preference',
	MS_Acct_Auth_Type int './MS-Acct-Auth-Type',
	MS_Acct_EAP_Type int './MS-Acct-EAP-Type',
	MS_RAS_Version nvarchar(255) './MS-RAS-Version',
	MS_RAS_Vendor int './MS-RAS-Vendor',
	MS_CHAP_Error nvarchar(255) './MS-CHAP-Error',
	MS_CHAP_Domain nvarchar(255) './MS-CHAP-Domain',
	MS_MPPE_Encryption_Types int './MS-MPPE-Encryption-Types',
	MS_MPPE_Encryption_Policy int './MS-MPPE-Encryption-Policy',
	Proxy_Policy_Name nvarchar(255) './Proxy-Policy-Name',
	Provider_Type int './Provider-Type',
	Provider_Name nvarchar(255) './Provider-Name',
	Remote_Server_Address nvarchar(15) './Remote-Server-Address',
	MS_RAS_Client_Name nvarchar(255) './MS-RAS-Client-Name',
	MS_RAS_Client_Version nvarchar(255) './MS-RAS-Client-Version'
	)

EXEC sp_xml_removedocument @idoc

SET NOCOUNT OFF
GO
SET QUOTED_IDENTIFIER OFF
GO
SET ANSI_NULLS ON
GO
```

A continuación, para realizar el control de tiempo de conexión se debe crear un trigger a ejecutarse después de la inserción de datos en la tabla accounting_data, la cual ocurre cuando un usuario cierra su sesión de navegación, que verificará que la suma del tiempo de sus sesiones no exceda el límite de 10 horas (36000 segundos):

```
USE [IASODBC]
GO
SET ANSI_NULLS ON
GO
SET QUOTED_IDENTIFIER ON
GO
CREATE TRIGGER [dbo].[deshabilitar_usuario]
	ON [dbo].[accounting_data]
	AFTER INSERT
AS
DECLARE
	@usuario_t nvarchar(10)
BEGIN
	SET NOCOUNT ON;

	IF (SELECT Acct_Session_Time FROM inserted) IS NOT NULL
	BEGIN

		SELECT @usuario_t = User_Name
		FROM inserted

		IF (SELECT SUM(Acct_Session_Time)
		    FROM (SELECT DISTINCT acct_session_id,
acct_session_time, User_Name
		          FROM accounting_data
```

```
                    WHERE Acct_Session_Time IS NOT NULL) a
                WHERE a.User_Name = @usuario_t) > 36000
                   EXEC sp_deshabilitar @usuario = @usuario_t;
      END
END
```

En caso de que se supere el límite de tiempo el mismo trigger hará correr un stored procedure, que se muestra a continuación:

```
USE [IASODBC]
GO
SET ANSI_NULLS ON
GO
SET QUOTED_IDENTIFIER ON
GO
CREATE PROCEDURE [dbo].[sp_deshabilitar]
      @usuario varchar(10) = '0',
      @cmd nvarchar(50) = 'cscript C:\desUsuario.vbs '
AS
BEGIN
      SET NOCOUNT ON;

      SELECT @cmd = 'cscript C:\desUsuario.vbs ' + @usuario
      EXEC master..xp_cmdshell @cmd;
END
```

Finalmente este stored procedure ejecutará un script llamado desUsuario.vbs ubicado en la raíz del disco C, que deshabilitará, en ActiveDirectory, la cuenta especificada.

```
'Controlamos que el número de argumentos sin nombre no sea más de uno
If WScript.Arguments.Unnamed.Count > 1 Then

      WScript.Echo "Error 1: se han pasado demasiados argumentos sin
nombre."
      WScript.Quit 1

'Controlamos que el número de argumentos sin nombre no sea inferior a uno
ElseIf WScript.Arguments.Unnamed.Count < 1 Then

      WScript.Echo "Error 2: no se ha pasado el argumento sin nombre
requerido"
      WScript.Quit 2

End If

'Controlamos que el número de argumentos con nombre no sea superior a 0
If WScript.Arguments.Named.Count > 0 Then

      WScript.Echo "Error 3: se han pasado demasiados argumentos con
nombre"
      WScript.Quit 3

End If



Set objArgs = WScript.Arguments
```

```
For I = 0 to objArgs.Count - 1
   WScript.Echo objArgs(I)
Next

On Error Resume Next

'/////////// BUSCAR EL CN DADO EL SAMACCOUNTNAME

Const ADS_SCOPE_SUBTREE = 2

Set objConnection = CreateObject("ADODB.Connection")
Set objCommand = CreateObject("ADODB.Command")
objConnection.Provider = "ADsDSOObject"
objConnection.Open "Active Directory Provider"
Set objCommand.ActiveConnection = objConnection

objCommand.Properties("Page Size") = 1000
objCommand.Properties("Searchscope") = ADS_SCOPE_SUBTREE

objCommand.CommandText = _
    "SELECT distinguishedName " & _
    "FROM 'LDAP://dc=biblioteca,dc=fisei' " & _
    "WHERE objectCategory='user' " & _
    "AND sAMAccountName = " & objArgs(0)

Set objRecordSet = objCommand.Execute

objRecordSet.MoveFirst
Do Until objRecordSet.EOF
    strDN = objRecordSet.Fields("distinguishedName").Value
    objRecordSet.MoveNext
Loop

'/////////// DESHABILITAR LA CUENTA

Const ADS_UF_ACCOUNTDISABLE = 2

Set objUser = GetObject("LDAP://" & strDN)
intUAC = objUser.Get("userAccountControl")

objUser.Put "userAccountControl", intUAC OR ADS_UF_ACCOUNTDISABLE
objUser.SetInfo

'/////////// MENSAJE DE CONFIRMACIÓN
'Wscript.Echo "Usuario " & objUser.Name & " ha sido Deshabilitado."
```

Configuración de IAS

Previo a la configuración de IAS, en el equipo server debe haber sido elevado a Controlador de Dominio y debe tener correctamente configurado Active Directory.

Instalación de IAS

La instalación de Internet Authentication Service se realiza como cualquier otro componente de Windows, es decir, a través del menú Inicio se accede al Panel de Control, de allí a Agregar o quitar programas, y finalmente a Agregar o quitar componentes de Windows. Se selecciona la opción de Servicios de red y se da clic en Detalles, en la ventana que aparece se pone un visto en Internet Authentication Service (Figura 36):

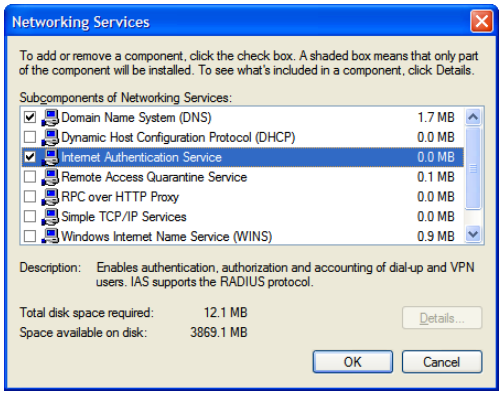


Figura 36. Instalación de Internet Authentication Service

Se da clic en Aceptar, a continuación clic en Siguiente, y clic en Finalizar.

Registro de IAS en Active Directory

Una vez instalado es necesario registrar el servicio en Active Directory. El acceso a Internet Authentication Service se encuentra entre las Herramientas Administrativas. Se da clic derecho en Internet Authentication Service (Local) y clic en Registrar Servidor en Active Directory (Figura 37):

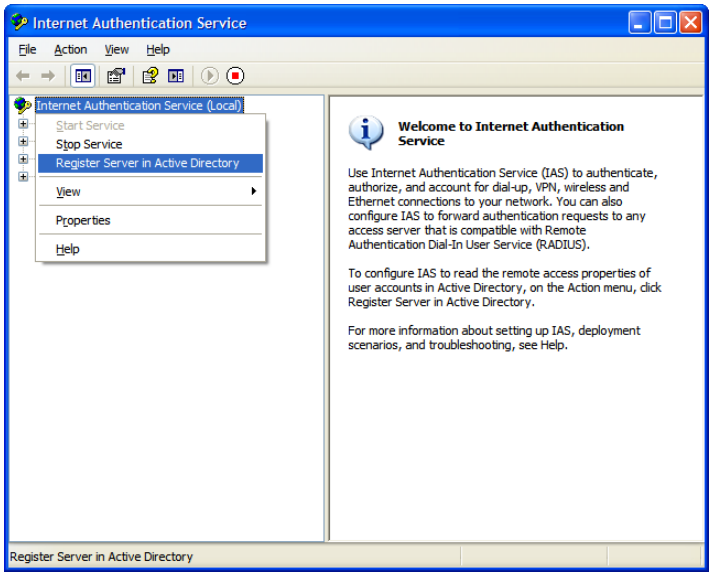


Figura 37. Registro de Internet Authentication Service en Active Directory

A continuación aparecen dos cuadros de diálogo, el primero pregunta si se desea autorizar a esta computadora a leer las propiedades dial-in de los usuarios del dominio, se da clic en Aceptar; el segundo cuadro de diálogo confirma lo anterior, también en este se da clic en Aceptar.

Comunicación entre IAS y pfSense

Para establecer la comunicación entre IAS y pfSense es necesario agregar este último como cliente RADIUS de IAS, para lo cual se da clic derecho en Clientes RADIUS, y se selecciona la opción Nuevo Cliente RADIUS, aparece un pequeño asistente. En la primera pantalla se especifica el nombre y la dirección IP del cliente RADIUS (Figura 38):

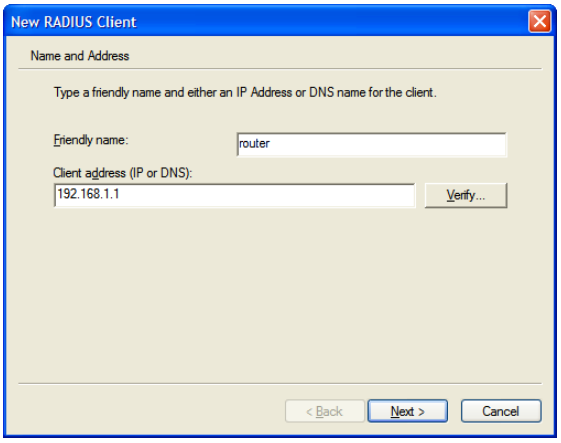


Figura 38. Nombre y dirección del Cliente RADIUS (pfSense)

En la segunda pantalla se selecciona RADIUS Standard y se especifica la palabra secreta para la encriptación de la conexión (fisei) (Figura 39):

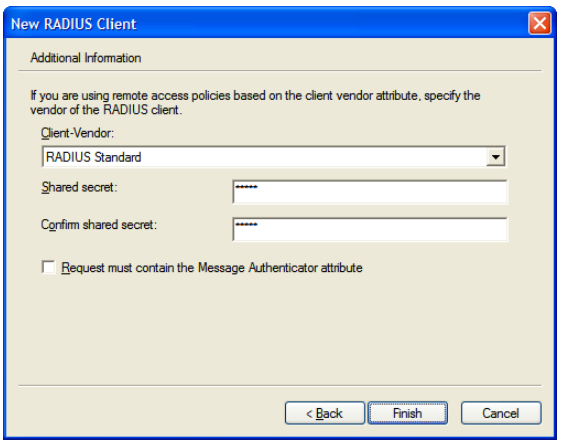


Figura 39. Tipo de Cliente RADIUS y palabra secreta

Clic en Finalizar. El Cliente RADIUS ha sido agregado.

Comunicación entre IAS y SQL Server

Para configurar la conexión entre IAS y SQL Server se selecciona Remote Access Logging tras lo cual en la parte derecha de la pantalla aparecerán las opciones de Archivo Local (Local File) y SQL Server, se da clic derecho en esta última y se elige Propiedades (Properties) (Figura 40):

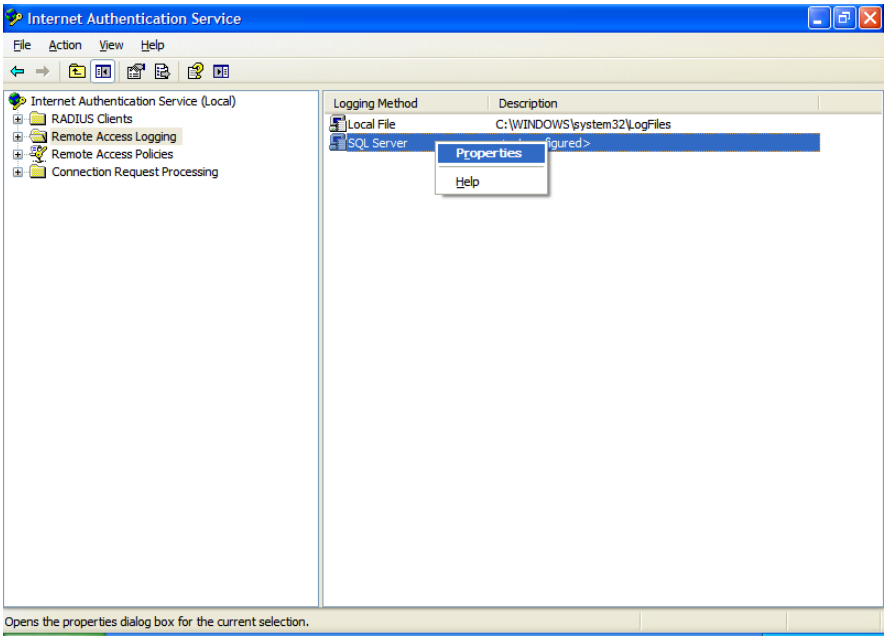


Figura 40. Configurar conexión entre IAS y SQL Server

En el cuadro de diálogo que aparece se seleccionan las tres opciones que hacen referencia a las Solicitudes de Contabilización, Solicitudes de Autenticación, y Estado periódico, respectivamente, luego se da clic en Configure… (Figura 41):

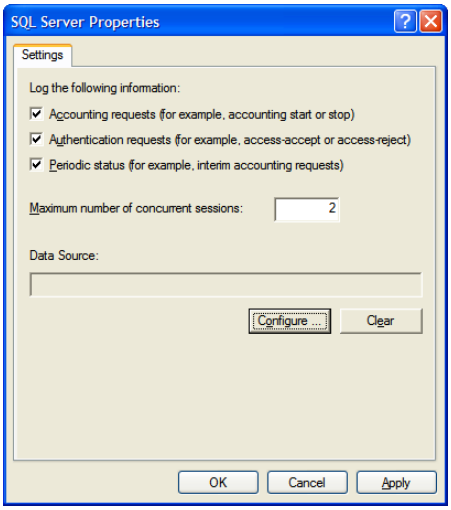


Figura 41. Propiedades del registro de eventos de SQL Server

En este diálogo se especifica la cadena de conexión, por lo que se especifica: el nombre del servidor SQL (SERVER\sqlexpress), el usuario mediante el cual se realizará la conexión (sa) con su respectiva contraseña, y se escoge la base de

datos creada con el script (IASODBC), es recomendable realizar una prueba de los ajustes realizados a través del botón Test Connection (Figura 42):

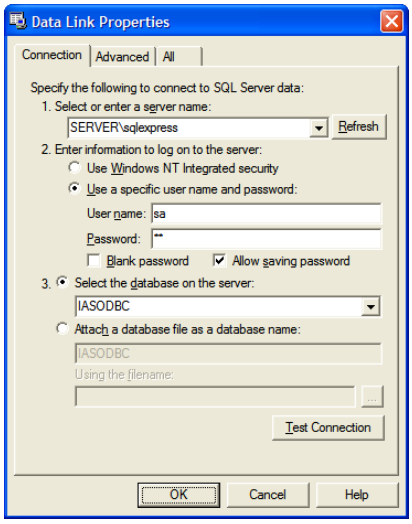


Figura 42. Cadena de conexión desde IAS hacia SQL Server

Especificación de Políticas de Acceso Remoto

En el panel de la izquierda se da clic derecho en Remote Access Policies y se escoge la opción New Remote Access Policy. Aparecerá un asistente, tras dar clic en Siguiente en la pantalla de bienvenida se muestra un diálogo que permite definir un nombre para la política y especificar que se trata de una política personalizada (custom) (Figura 43):

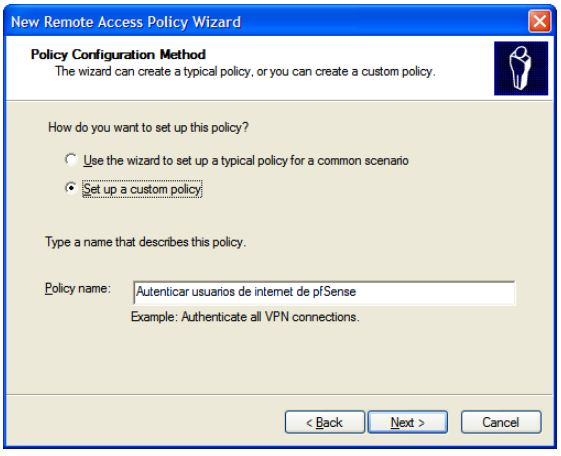


Figura 43. Nombre de política de acceso remoto personalizada

A continuación se deben elegir condiciones a ser cumplidas para que se aplique esta política. Dichas condiciones son las que se aprecia en la Figura 44:

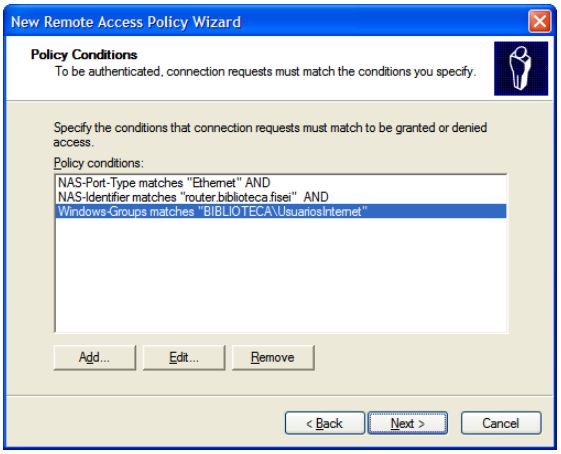


Figura 44. Condiciones de política de acceso remoto

En la siguiente pantalla se elige la opción de conceder permiso de acceso remoto (Grant remote access permission) (Figura 45), clic en Siguiente:

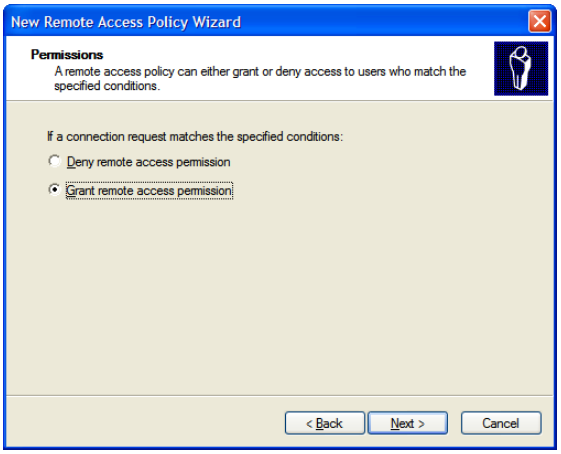


Figura 45. Permisos de política de acceso remoto

En la pantalla siguiente se da clic en Edit Profile… en el diálogo que aparece se visita la pestaña Authentication, allí se deselecciona todo y se activa la opción de autenticación no-encriptada (Unencrypted Authentication) (Figura 46):

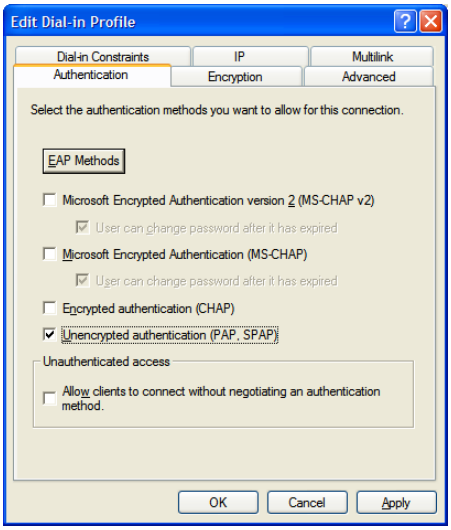


Figura 46. Autenticación del perfil Dial-In

Se da clic en Aceptar y en el cuadro de diálogo que aparece se responde que No. Clic en Siguiente y Finalizar.

Configuración de usuarios

Cualquier cuenta de usuario creada en Active Directory puede ser asignada al uso de Internet a través del portal cautivo que ofrece pfSense, para ello el usuario debe pertenecer al grupo UsuariosInternet, y en las propiedades del usuario, en la pestaña Dial-In debe estar permitido el acceso (Allow access) remoto a Dial-In o VPN.

En los equipos clientes

Actualmente los navegadores de Internet poseen la característica de bloquear ventanas emergentes o pop-up, lo cual puede interferir con el funcionamiento del portal cautivo ya que el logout se realiza precisamente con una ventana de este tipo. Por tanto se deben establecer excepciones para asegurar el correcto desempeño del portal.

Microsoft Internet Explorer

En Internet Explorer se accede a Opciones de Internet, en el menú Herramientas. En la pestaña Privacidad, se pulsa el botón Sitios y se agrega la dirección IP del ruteador (192.168.1.1).

En la pestaña Seguridad, se selecciona Intranet local, y se realiza el mismo procedimiento.

Mozilla Firefox

En el navegador Firefox se accede a la ventana de Opciones a través del menú Herramientas. En la sección de Contenido, junto a la opción Bloquear ventanas emergentes, se pulsa el botón Excepciones y se agrega la dirección IP del ruteador (192.168.1.1)

Comprobación del funcionamiento

Para comprobar el funcionamiento del servicio basta con acceder desde un equipo cliente y a través de un explorador de Internet a cualquier sitio web y se apreciará la redirección hacia el portal cautivo.

Más detalles sobre la interacción existente entre el usuario y el portal se presentan en la Guía de Uso que se encuentra como Anexo en la sección de Materiales de Referencia.

6.8 ADMINISTRACIÓN

La interacción con el sistema se puede contemplar desde dos puntos de vista: el bibliotecario, y el alumno. Para el bibliotecario se ofrece un Manual de Usuario en la sección de Anexos; y para el alumno una Guía de Uso también incluída en la sección de Anexos.

6.9 PREVISIÓN DE LA EVALUACIÓN

Para mantener correctamente operativa la solución software es absolutamente recomendable que cada semestre, en lo posible al terminar el período de matrículas, se encere la base de datos (borrar todos los usuarios y registros) para prevenir la excesiva expansión de dicha base.

También se recomienda que, al finalizar el primer semestre de aplicación de la solución software se realice una encuesta para evaluar la aceptación del mismo por parte de los usuarios.

MATERIALES DE REFERENCIA

1 BIBLIOGRAFÍA

- http://es.wikipedia.org/wiki/Acceso_a_Internet
  - Descripción de conexión o acceso a Internet.
- http://www.estrategiamagazine.com.ar/menu/glosario/glosario_busca.asp?termino=231&definicion=Internet%20Architecture%20Board%20(IAB)
  - Glosario: Internet Architecture Board (IAB).
- http://es.wikipedia.org/wiki/IANA
  - Glosario: Internet Assigned Numbers Authority (IANA).
- http://www.educaweb.com/noticia/2008/06/02/internet-educacion-hechos-otro-13013.html
  - Internet y educación. Relación entre las TIC y los modelos educativos.
- http://es.wikipedia.org/wiki/CLUF
  - Definición, clasificación y descripción de las Licencias de Software.
- http://www.uclm.es/profesorado/ricardo/WEBNNTT/Bloque%202/Internet.htm
  - Internet & Educación. Experiencias en el uso de Internet y computadores en instituciones educativas en España.
- http://es.wikipedia.org/wiki/NSF
  - Glosario: National Science Foundation (NSA).
- http://www.monografias.com/trabajos43/administracion-redes/administracion-redes.shtml
  - Introducción, importancia y descripción de la Administración de Redes.
- http://es.wikipedia.org/wiki/NSFNET
  - Glosario: National Science Foundation's Network (NSFNet).
- http://www.geocities.com/ingenieria_redes/
  - Redes de computadores. Topologías, medios, tipos y protocolos.
- http://es.wikipedia.org/wiki/Modelo_OSI
  - Glosario y definición de Modelo OSI (Open System Interconnection).
- http://www.leovinciconsulting.com/uploads/fichas_productos/Hotspots%20-%20Presentaci%C3%B3n.pdf
  - Sistema de puntos de acceso inalámbrico para acceso público. Ejemplos: Portal captivo, administración, ampliaciones de la red.
- http://ldapman.org/articles/sp_intro.html
  - Introducción a LDAP.
- http://www.isftic.mepsyd.es/w3/programa/usuarios/ayudas/tipo_conexion.htm
  - Tipos de conexión a Internet. Información sobre los tipos más comunes de acceso o conexión a Internet.

- http://www.alegsa.com.ar/Dic/hotspot.php
  - Glosario: Hotspot (Punto caliente).
- http://en.wikipedia.org/wiki/Hotspot_(Wi-Fi)
  - Hotspots. Historia, usos, tipos, seguridad y control.
- http://www.alegsa.com.ar/Dic/honeypot.php
  - Glosario: Honeypot.
- http://www.alegsa.com.ar/Dic/hotspot%20falso.php
  - Glosario: Hotspot falso.
- http://www.microsoft.com/spain/empresas/tecnologia/hotspot.mspx
  - Hotspot. Modelos de negocio y tecnología.
- http://www.zonawifi.biz/hotspotwifi.html
  - Hotspots WiFi. Un servicio WiFi indispensable para una oferta moderna y competitiva.
- http://jpill.wordpress.com/2008/08/11/46/
  - Portal Captivo Chillispot. Requisitos mínimos.
- http://pof.eslack.org/PFC/pfc.pdf
  - Diseño e implementación de un HotSpot-in-a-box. Integración de diferentes herramientas Open Source. Aplicaciones en entornos corporativos como desde el punto de vista de usuario final. Estudio del modelo de negocio con el correspondiente análisis económico de implantación.
- http://es.wikipedia.org/wiki/LDAP
  - LDAP (Lightweight Directory Access Protocol). Implementaciones.
- http://www.optenet.com/es/education.asp
  - Educación. Administración de Internet en Centros Educativos.
- http://es.wikipedia.org/wiki/Sociedad_de_la_informaci%C3%B3n
  - Sociedad de la información. Historia y definición del término.
- http://es.wikipedia.org/wiki/L%C3%ADnea_de_abonado_digital
  - Línea de abonado digital. Introducción a las conexiones DSL.
- http://es.wikipedia.org/wiki/Point-to-Point_Protocol
  - Point-to-Point Protocol (PPP). Definición, descripción y funcionamiento.
- http://es.wikipedia.org/wiki/PPPoE
  - Point-to-Point Protocol over Ethernet (PPPoE). Aprovechamiento de características de PPP en redes Ethernet.
- http://technet.microsoft.com/en-us/library/cc778830(WS.10).aspx
  - Conceptos clave para el registro de eventos de IAS en SQL Server.

2 ANEXOS

2.1 MANUAL DE USUARIO PARA EL BIBLIOTECARIO

2.2 GUÍA DE USO PARA EL ALUMNO

2.3 COPIAS DE DOCUMENTOS DE FUNDAMENTACIÓN LEGAL

MANUAL DE USUARIO

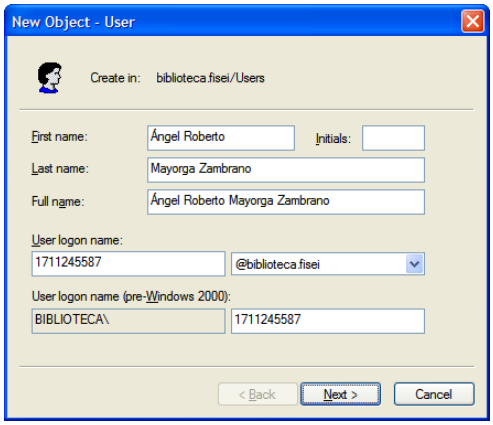
Las responsabilidades del bibliotecario en el sistema son las siguientes:

- Creación de usuarios.
- Expulsión de usuarios.

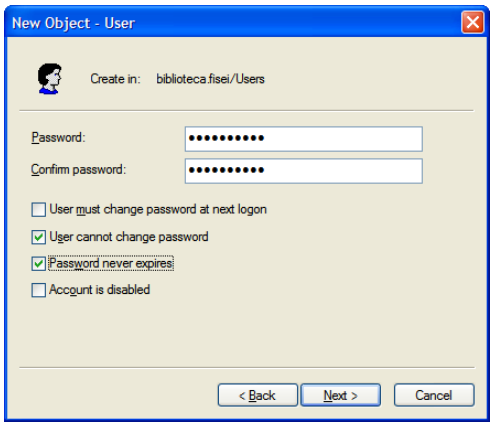
CREACIÓN DE USUARIOS

La creación de usuarios debe ser realizada cada semestre, preferiblemente a continuación de que ha concluido el período de matriculación.

Se ingresa a Active Directory Users and Computers, se da clic derecho en Users, se escoge la opción New, y la sub-opción User. Aparece el asistente de creación de usuarios en el cual se indica los nombres (en el campo "First name"), los apellidos (en el campo "Last name")y el número de cédula (en el campo "User logon name").

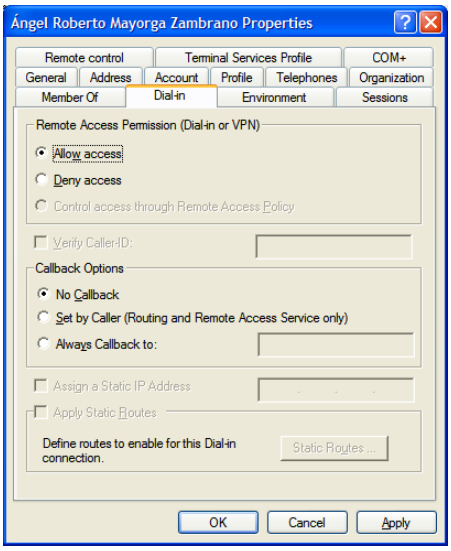


A continuación se especifica la contraseña del estudiante, que será el mismo número de Cédula. También se deshabilita la opción de que el usuario deba cambiar su contraseña en su siguiente inicio de sesión (User must change password at next logon), y se habilitan las opciones de que el usuario no puede cambiar la contraseña (User cannot change password), y que la contraseña nunca expira (Password never expires).

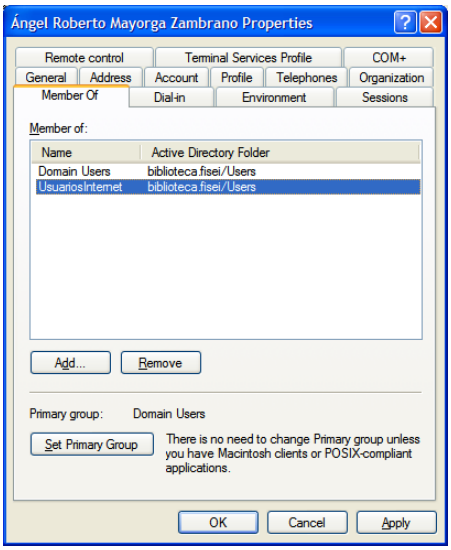


Tras dar clic en Siguiente se muestra un resumen de la información introducida, se da clic en Finalizar.

A continuación en la panel de la derecha se ubica el usuario que se ha creado y se da doble clic en su nombre para abrir la ventana de propiedades del usuario. Se acude a la pestaña Dial-In y se selecciona la opción Allow access:



Luego se visita la pestaña Member Of. Se da clic en el botón Add y en el cuadro de diálogo que aparece se escribe UsuariosInternet. Clic en Aceptar:



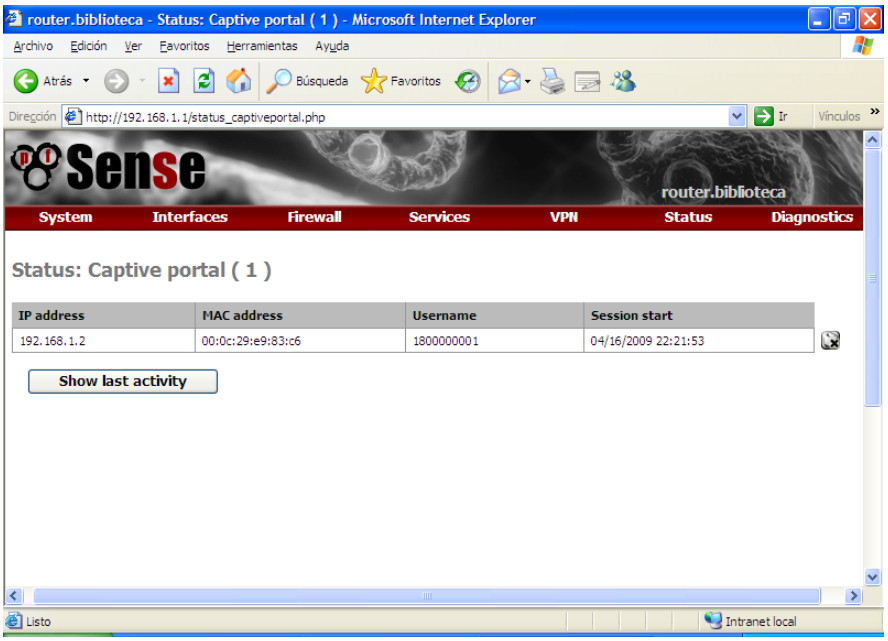
Finalmente, se da clic en Aceptar y el usuario ha sido creado.

EXPULSIÓN DE USUARIOS

Bajo ciertas circunstancias el bibliotecario tendrá la necesidad de expulsar o terminar la conexión de un usuario. Por ejemplo, si accidentalmente el usuario cerró la ventana de logout y por tanto no puede terminar su sesión él mismo.

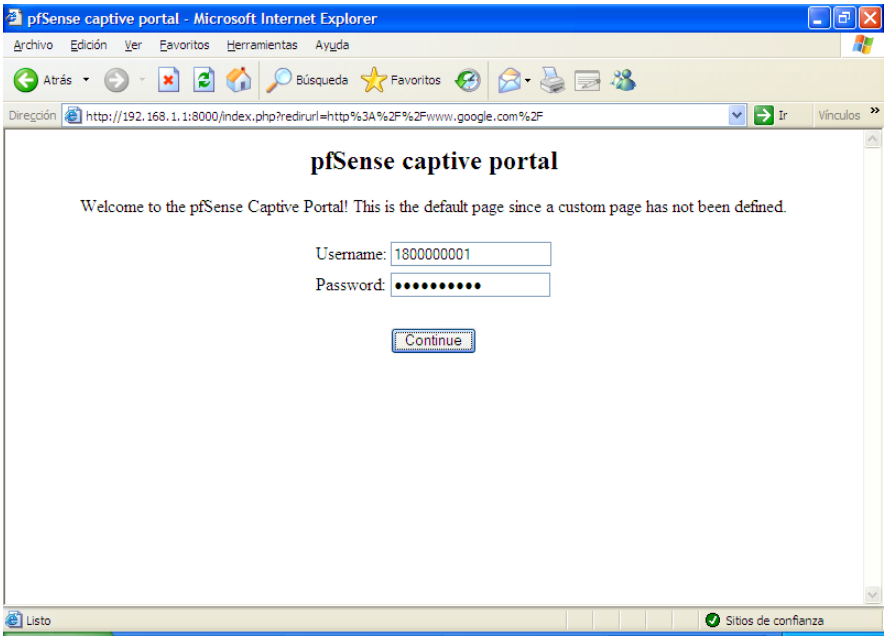
Para esto se accede al portal web de configuración de pfSense, digitando http://router.biblioteca.fisei o su equivalente http://192.168.1.1 en el navegador de Internet.

En el menú Status se accede a la opción Captive Portal, se identifica al usuario en la columna Username y se da clic en el botón ubicado a la derecha del mismo.

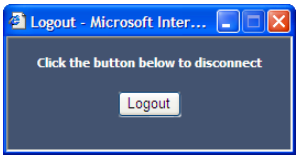


GUÍA DE USO

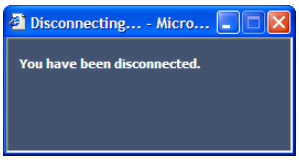
Al intentar ingresar a un sitio web, el usuario es re-direccionado a la página de login, en la cual debe ingresar su número de Cédula de Ciudadanía tanto en el campo Username como en el campo Password, a continuación se da clic en el botón Continue.



Si el nombre de usuario y la contraseña han sido ingresados correctamente, y corresponden a un usuario existente en el sistema, aparecerá una ventana pop-up con el botón que permite hacer logout. Esta ventana no debe ser cerrada pues de hacerlo no será posible abandonar el sistema sin la ayuda del bibliotecario.



Cuando se desea salir del sistema se pulsa el botón Logout, en un par de segundos cambiará el mensaje, notificando que ha sido desconectado.



Por las diferencias existentes entre los diferentes navegadores es posible que este mensaje no aparezca, por lo que se recomienda pulsar el botón Logout en dos ocasiones, cerrar esta ventana, y verificar que ya no es posible la navegación.

Si en el portal se ingresa un usuario y/o contraseña incorrecta se muestra una página con mensaje de error de autenticación, y un vínculo para regresar a la página de login.