UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERIA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

CARRERA DE INGENIERIA EN SISTEMAS COMPUTACIONAL E INFORMATICA

TEMA

“SEGURIDAD DE REDES USANDO REDES PRIVADAS VIRTUALES”

Trabajo de graduación modalidad: Seminario de Graduación o trabajo estructurado de manera independiente.

AUTORA: **Kattia Marisela Rodríguez Mora**

TUTOR: **Ing. Javier Sánchez**

AMBATO – ECUADOR

Mayo - 2010

APROBACIÓN DEL TUTOR

En mi calidad de tutor del trabajo de investigación sobre el tema: Seguridad de redes utilizando redes privadas virtuales, de Kattia Marisela Rodríguez Mora, estudiante de la Carrera de Ingeniería en Sistemas, 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 Art. 45 del Capítulo III Seminarios, del Reglamento de Graduación de Pregrado de la Universidad Técnica de Ambato.

Ambato abril 20, 2008

EL TUTOR

Ing. Javier Sánchez

AUTORÍA

El presente trabajo de investigación titulado: seguridad de redes usando redes privadas virtuales. 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 abril 20, 2009

Kattia Rodriguez M.
CC: 160050608-1

DEDICATORIA:

Dedico esta tesis a la memoria de mi madre quien me supo dar ese cariño y calor humano necesario para seguir adelante, a quien le debo horas de consejos, de regaños, de reprimidas de tristezas de las cuales estoy muy segura las ha hecho con todo el amor del mundo.

A mi padre quien supo velar por mi salud, mis estudios, mi educación, quien supo brindarme siempre su apoyo en donde sus consejos nunca faltaron para formarme como un ser integral.

Mi triunfo es para mis padres de quienes me siento extremadamente orgullosa.

Kattia Rodriguez M.

AGRADECIMIENTO:

Muchas han sido las personas que de manera directa o indirecta me han ayudado en la realización de esta tesis. Quiero dejar constancia de todas ellas y agradecerles con sinceridad su participación.

A Dios, gracias por darme la vida, por poner en mi camino a personas maravillosas, por las bendiciones y los regalos que recibo día tras día.

Al Ing. Javier Sánchez, porque su cordialidad y su apoyo para conmigo han sido muy grandes durante todo este tiempo de duro trabajo quien ha puesto todos los medios necesarios para que pudiera realizar mi tesis.

A mis amigos, para quienes tengo sólo palabras de agradecimiento, especialmente por aquellos momentos en los que pude ser inferior a sus expectativas: ha sido un camino largo y duro en el que, algunas veces, la fijación por lograr tus objetivos te hace olvidar la importancia del contacto humano. Sin embargo, como en todas las actividades de la vida, siempre al final hay algunos criterios que te permiten priorizar y es por ello que debo resaltar mis agradecimientos para algunas personas.

Y, por supuesto, el agradecimiento más profundo y sentido va para mi familia. Sin su apoyo, colaboración e inspiración habría sido imposible llevar a cabo este duro trabajo.

Kattia Rodriguez M.

INDICE

CAPITULO III

METODOLOGIA

CAPITULO IV

ANALISIS E INTERPRETACION DE RESULTADOS

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

CAPITULO VI

PROPUESTA

RESUMEN EJECUTIVO

El cambio en la forma de hacer los negocios ha sido tan profundo que es muy diferente del de hace una década tan solo: Los negocios hoy ya no son locales, es más, ni siquiera regionales, deben ser mundiales, es decir capaces de interactuar a escala global.

Empresas con sucursales en los diferentes continentes, empresas pequeñas y medianas trabajando para otras empresas o asociadas entre si, ejecutivos y personal de la empresa viajando constantemente, tienen un mismo problema: la comunicación, es más la interacción con recursos o información que está centralizada en la sede central o en otras sucursales. Pero ¿como acceder a esos recursos de forma fácil y segura?

Así, la seguridad en Internet cobra cada vez mayor importancia, ya que no sólo se deben proteger los servidores de la empresa con Firewalls, sino también la comunicación que se realizan a través de Internet, que es una red pública susceptible de ser interceptada por millones de usuarios.

Una respuesta al problema de seguridad de la información, fue la creación de la criptografía, técnica de codificación que hace que lo transmitido por Internet sólo pueda ser decodificado por quienes se desea; lo cual facilito la posibilidad de crear redes privadas virtuales (VPN) institucionales sobre Internet.(de negocios, educativas, militares, etc.)

Este tipo de redes facilita la conexión de sitios remotos como las sucursales de las empresas que estarán interconectadas entre si. Por si fuera poco, se puede acceder a la red corporativa desde la computadora portátil en cualquier parte del mundo, formando una única red corporativa. Todos podrán compartir recursos y la institución ahorrará recursos, tan escasos hoy en día.

CAPITULO I
EL PROBLEMA

1.1. Tema

ESTUDIO DE SEGURIDADES USANDO REDES PRIVADAS VIRTUALES

1.2 Planteamiento del Problema

1.2.1 Contextualización

A nivel mundial las Redes Virtuales Privadas (VPN) es la nueva manera de entender el mundo del Networking en todos sus ámbitos, desde las redes de área extensas hasta las redes de área local, desde los servicios de voz, hasta los datos y multimedia llegando al usuario que accede a los servicios a través del PC, estas redes, además de garantizar conexión permanente, permiten el flujo de información de una forma segura. Las redes se han convertido en el principal canal de comunicación de las empresas, pues permiten el flujo de su información, por ende su funcionalidad es vital para la operación del negocio. Las organizaciones son cada vez más dependientes de sus redes informáticas y un problema que las afecte por mínimo que sea, puede llegar a comprometer la continuidad de las operaciones. Los empleados de las empresas pasan muchas horas de su tiempo fuera de la oficina. Sin embargo, en aras de una mayor rapidez en las operaciones y una mejor relación con clientes y proveedores, es absolutamente necesario que estén conectados con la

oficina. Esas conexiones se llevan a cabo a través de muchos tipos distintos de dispositivos, pero fundamentalmente a través de ordenadores portátiles y redes inalámbricas, ADSL o módem.

En el Ecuador se muestra que en todas las regiones se ve al incremento de la productividad como el principal beneficio de la movilidad, aunque los ejecutivos reconocen la existencia de un amplio rango de ventajas adicionales que van desde mejorar el servicio al cliente y reducir los costos operativos y de infraestructura hasta facilitar la continuidad y disponibilidad de los negocios en todo momento. Lograr las ganancias de productividad deseadas requiere de claridad de pensamiento por parte del equipo de gestión sobre cómo se lleva a cabo el proceso de migración de tecnologías móviles y aplicaciones a IP. Todas las compañías que necesiten transferir información de una forma segura entre un ente (sucursal, empleado remoto, socios, etc.), y algunos servicios en la compañía, deben pensar en la implementación de una red VPN. La ventaja de este tipo de red es indudablemente el aumento de la productividad de los empleados, desde cualquier parte del mundo con conexión a Internet, es posible tener todos los servicios de la red, como si el empleado estuviera sentado en su puesto de trabajo. Incluso mediante la interacción de tecnología como telefonía IP y VPNs de IPSec, si un cliente llama a la extensión telefónica del empleado este puede contestar desde su computador sin importar el lugar del mundo donde se encuentre.

En Tungurahua es necesario unificar las múltiples delegaciones que una organización pueda tener (incluidos trabajadores móviles) en una única red ya que cada uno trabaja aisladamente. Estas redes requieren ser gestionadas con la finalidad de lograr proactividad adelantándose a sucesos que podrían hacer que nuestra red no funcionase durante algún período de tiempo afectando la productividad de la empresa, es por eso, siempre se recomendará y configurará adecuadamente el software de gestión pudiendo evitar, en la medida de lo posible, la caída de la red. Las VPNs pueden ser usadas para suministrar un canal seguro entre dos

sistemas (PCs), entre dos sitios (La central de una compañía con una sucursal), o el acceso a un usuario remoto (Un vendedor en campo con su central), a través de Internet sin necesidad probablemente de entrar en costos de conexiones dedicadas o probablemente de llamadas de larga distancia (RAS).

1.2.2 Análisis Crítico

La no existencia de seguridades mediante VPNs, se debe a la falta de conocimiento y del personal que no está preparado para manejar este sistema , la escasa disponibilidad de recursos, así como la inexistencia de un plan estratégico para la gestión del rendimiento desde la evaluación previa a la implementación, la monitorización y la gestión continuada hasta la optimización y la planificación de un crecimiento futuro, con lo cual se genera un aspecto negativo para la gestión del rendimiento corporativo, ya que un aspecto puede afectar al otro.

Además no se estaría aprovechando la red global que brinda transporte escalable y seguro, con esto se puede eliminar las complejidades de redes y proveedores múltiples.

Las VPN son una salida al costo que puede significar el pagar una conexión de alto costo, para usar líneas alquiladas que estén conectadas a otros puntos que puedan hacer uso de la conexión a Internet o para hacer negocios con clientes frecuentes a través de la red, los datos son codificados o cifrados e inmediatamente enviados a través de la conexión, para de esa manera asegurar la información y la contraseña que se esté enviando, de esta manera se esta obteniendo la omnipresencia de Internet, la seguridad de una red privada y las economías de una red compartida, todo en un solo puerto.

El servicio IP VPN le permite implementar redes y circuitos de backbone rápidamente, sin problemas de interoperabilidad.

1.2.3 Prognosis

De continuarse trabajando sin redes VPN, la información va a sufrir un grave retraso en cuanto se refiere al manejo de la tecnología especialmente en las empresas que requieren de este tipo de redes. Esta tecnología proporciona un medio para aprovechar un canal público de Internet como un canal privado o propio para comunicar datos que son privados. Más aún, con un método de codificación y encapsulamiento, una VPN básica, crea un camino privado a través de Internet. Esto reduce el trabajo y riesgo en una gestión de red.

Disponer de datos analíticos sobre la red, las aplicaciones y las transmisiones de VoIP permite observar con claridad el efecto que el tráfico de datos ejerce sobre la calidad de las llamadas y el efecto de VoIP sobre la calidad de los datos, lo que representa una ventaja significativa sobre los productos centrados únicamente en la voz.

Con este sistema de redes VPN se pretende poner a disposición de las pequeñas empresas soluciones de telefonía en red, perfectamente adaptadas a sus necesidades, las cuales permitan realizar negocios desde múltiples localizaciones. Seria de suma importancia que la empresa cuente con servicios de implementación con altos niveles de seguridad, disponibilidad y desempeño.

Con una red VPN, una compañía puede reinventar tanto sus redes de comunicaciones como toda su organización. Esta red apoya aplicaciones vitales para estructurar el negocio Telefonía IP, videoconferencia en colaboración y Administración de Relaciones con el Cliente (CRM) que contribuyen a que la empresa sea más eficiente, efectiva y ágil con sus clientes. Las soluciones VPN nos hacen más productivos, pues simplifican el usar aplicaciones y compartir información. Tener una red para la administración significa que el ancho de banda será usado lo más eficientemente posible, a la vez que permite otras eficiencias y ahorros de

costos: en personal, mantenimiento, cargos de interconexión, activaciones, mudanzas y cambios.

Las VPNs permiten una mayor integración de nuevas aplicaciones y tecnologías, interconexión total a la red de todos los comerciales (empleados), de forma segura a través de una infraestructura pública, así como una mayor facilidad en la administración, están diseñadas sobre una arquitectura abierta y standard de forma tal que permite la integración de medios de comunicación actuales y futuros, dando soluciones a telefonía IP, centros de contacto virtuales, mensajería unificada, e-learning, TV broadcast, entre otras más.

1.2.4 Formulación del problema

¿Qué incidencia tiene las seguridades usando VPNs en el desarrollo y competitividad de una empresa?

1.2.5 Preguntas Directrices

1.3.1.1 ¿Cuál es la situación actual de una empresa?
1.3.1.2 ¿Cuáles son las operaciones que en la actualidad se realizan en el área de redes?
1.3.1.3 ¿Qué etapas se deben considerar para mejorar una red?
1.3.1.4 ¿Qué cambios se deben realizar en el área de redes?
1.3.1.5 ¿Cuáles son los recursos necesarios para mejorar una red?
1.3.1.5. ¿Cómo debe ser la seguridad en una red VPN?

1.2.6 Delimitación del Problema

En la presente investigación se realizará un estudio de todo lo referente a las seguridades usando VPN. El tiempo estimado para la investigación será de cinco meses del 10 de Noviembre del 2008 al 30 de Marzo del 2009. Se trabajará con una población integrada por ocho docentes.

1.3 Justificación

El presente trabajo investigativo en el área de redes, busca realizar un estudio de seguridades usando VPN, que permita alta escalabilidad, privacidad y seguridad garantizada en sus comunicaciones.

En los últimos años las redes se han convertido en un factor crítico para cualquier organización. Cada vez en mayor medida, las redes transmiten información vital, por tanto dichas redes cumplen con atributos tales como seguridad, fiabilidad, alcance geográfico y efectividad en costos.

Se ha demostrado en la actualidad que las redes reducen en tiempo y dinero los gastos de las empresas, eso ha significado una gran ventaja para las organizaciones sobre todo las que cuentan con oficinas remotas a varios kilómetros de distancia, pero también es cierto que estas redes remotas han despertado la curiosidad de algunas personas que se dedican a atacar los servidores y las redes para obtener información confidencial. Por tal motivo la seguridad de las redes es de suma importancia, es por eso que escuchamos hablar tanto de las famosas VPN.

Los costos de una VPN son bajos porque solo se realiza llamadas locales, además de tener la posibilidad de que mis datos viajen encriptados y seguros, con una buena calidad y velocidad. El avance de las redes no sólo se ha hecho presente a nivel empresarial, sino que cada vez son más los hogares y grupos de amigos, donde se plantea la necesidad de crear un lazo entre computadoras para así aprovechar al máximo el potencial que brindan los equipos modernos.

Mediante una VPN creada entre un grupo de usuarios, cada uno de ellos puede acceder de manera transparente y confidencial a los recursos del equipo del otro, es decir utilizar no sólo sus accesorios como impresoras,

scanners y demás, sino también obtener acceso a documentos y aplicaciones, siempre asegurando la integridad, confidencialidad y seguridad de los datos.

Esta comunicación remota entre computadoras se establece mediante dicha red VPN, que a su vez ha sido creada dentro de una red más grande, que habitualmente suele ser Internet. La VPN es una red privada dentro de una red pública, con lo que sólo pueden tener acceso los usuarios que pertenezcan a esa red.

Es importante señalar que los datos que viajan a través de la VPN se trasladan encriptados, por lo que sólo podrán acceder a ellos los usuarios de dicha VPN, garantizando así la privacidad de los datos. En realidad, las VPN funcionan de la misma manera que cualquier otro tipo de red, por lo que cada equipo que sea parte de una determinada VPN tendrá una IP establecida que le permitirá acceder a dicha red privada.

La principal motivación del uso y difusión de esta tecnología es la reducción de los costos de comunicaciones directos, tanto en costos de llamados de larga distancia como en vínculos dedicados. Anterior a la ubicuidad de Internet, las compañías que querían que las redes de sus empresas trascendieran más allá del ámbito de la oficina e incluyeran a los trabajadores y centros de información de otros edificios, ciudades, estados o incluso otros países, tenían que invertir en hardware y servicios de telecomunicaciones costosos y proporcionales a las distancias implicadas para crear redes amplias de servicio. Sin embargo, con Internet, las compañías tienen la posibilidad de crear una VPN que demanda una inversión relativamente pequeña de hardware y prácticamente independiente de las distancias, utilizando esta posibilidad de alcance global para la conexión entre los puntos de la red.

Cada usuario remoto de la red empresarial puede comunicarse de manera segura y confiable utilizando Internet para conectarse a su red

privada local. Una VPN puede crecer para adaptarse a más usuarios y diferentes lugares mucho más fácil que las líneas dedicadas. De hecho, la escalabilidad es otra de las grandes ventajas de una VPN sobre las líneas rentadas.

1.4 Objetivos de la Investigación

1.4.1 Objetivo General

1.4.1.1 Realizar un estudio de seguridades mediante VPN

1.4.2 Objetivos Específicos

1.4.2.1 Establecer cual es la situación actual de la empresa
1.4.2.2 Determinar las operaciones que actualmente realiza la empresa
1.4.2.3 Establecer las etapas que se realizan en el estudio para mejorar una red
1.4.2.4 Determinar los cambios que se deben realizar en el área de redes
1.4.2.5 Determinar cuáles son los recursos necesarios para mejorar una red
1.4.2.6. Realizar un estudio para seguridades mediante VP

CAPITULO II
MARCO TEORICO

2.1 Antecedentes Investigativos

Se puede manifestar que la presente investigación realizada en la Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato no existe ningún proyecto de tesis similar al tema que escogí para realizar mi trabajo de investigación.

2.2 Fundamentación

2.2.1 Fundamentación Legal

Considerando que, la regulación debe basarse en criterios objetivos, no discriminatorios, proporcionales y transparentes. En ejercicio de sus facultades legales.

Resuelve:

ARTICULO 1.- Definir como “Ciber Cafés” a los “Centros de Información y Acceso a la red de Internet, “ que permiten a sus usuarios acceder a dicha red mediante terminales de usuario final, en un punto, local o ubicación determinados, abiertos al público o a un grupo definido de personas, mediante el uso de equipos de computación y demás terminales relacionados.

ARTICULO 2.-Se prohíbe expresamente la prestación de servicios de telecomunicaciones finales o portadores sin contar con el título habilitante correspondiente y solo se los podrá prestar mediante convenios de reventa, de conformidad con lo dispuesto en la legislación vigente.

ARTICULO 3.-La Voz sobre Internet podrá ser ofrecida por los Centros de Información y Acceso a la Red de Internet o “Ciber Cafés” de acuerdo a las siguientes condiciones:

a) La Voz sobre Internet podrá ofrecerse exclusivamente para tráfico internacional saliente, prohibiéndose su utilización para la realización de llamadas locales, regionales, llamadas de larga distancia nacional, llamadas a servicios celulares o llamadas a servicio móvil avanzado.

b) El número de equipos terminales asignados para uso de Voz sobre Internet, en ningún caso podrá exceder del 25% (veinticinco por ciento) de la capacidad total de terminales instalados para atención al público en los Centros de Información y Acceso a la red Internet o “Ciber Cafés”.

c) Los Centros de Información y Acceso a la red de Internet o “Ciber Cafés” que cuenten con dos (2) o tres (3) terminales totales, podrán asignar solo uno para uso de Voz sobre Internet.

d) Los Centros de Información y Acceso a la red de Internet o “Ciber Cafés” que ofrezcan Voz sobre Internet de conformidad con lo señalado en los literales a) y b) del presente artículo requerirán únicamente de un certificado de registro, de conformidad con el artículo 7 de la presente Resolución.

e) Los Centros de Información y Acceso a la red de Internet o “Ciber Cafés” deberán presentar semestralmente a la Secretaría Nacional de Telecomunicaciones reportes relacionados con las aplicaciones prestadas

por los Ciber Cafés en los formatos a publicarse en la página web del CONATEL.

f) Los Centros de Información y Acceso a la red de Internet o “Ciber Cafés” deberán presentar semestralmente a la Secretaría Nacional de Telecomunicaciones y a la Superintendencia de Telecomunicaciones, reportes relativos al tráfico de voz que cursan por Internet en los formatos a publicarse en la página web del CONATEL.

ARTICULO 4.-Se prohíbe a los “Centros de Información y Acceso a la Red de Internet” o “Ciber Cafés” el uso de dispositivos de conmutación, tales como Gateways o similares que permitan conectar las llamadas sobre Internet a la red telefónica pública conmutada, a las redes de telefonía móvil celular o del servicio móvil avanzado y de esta manera permitan la terminación de llamadas en dichas redes.

ARTICULO 5.- Quedan excluidos de la presente regulación los establecimientos que deseen ofrecer Voz sobre Internet y que no cumplan con las condiciones establecidas en los Artículos 3 y 4 de la presente Resolución, independientemente de la facilidad tecnológica que utilicen; dichos establecimientos deberán sujetarse a lo que se establece en el “Reglamento del Servicio de Telefonía Pública”.

ARTICULO 6.- Quedan excluidos de la presente regulación los locutorios, cabinas y otros establecimientos que ofrezcan el servicio de transmisión de voz, ya sea por medio de conmutación de paquetes o utilizando conmutación de circuitos. Estos establecimientos deberán sujetarse a lo que se establece en el “Reglamento del Servicio de Telefonía Pública, o a la reventa de servicios”.

ARTICULO 7.- Los “Centros de Información y Acceso a la red de Internet” o “Ciber Cafés”, previo a su operación, tienen que obtener un registro en

la Secretaría Nacional de Telecomunicaciones, para lo cual deberán cumplir con los siguientes requisitos:

Para personas naturales:

- Solicitud dirigida al señor Secretario Nacional de Telecomunicaciones.
- Copia del RUC.
- Copia de la cédula de ciudadanía y certificado de votación del peticionario (para solicitantes ecuatorianos), o copia del pasaporte debidamente visado (para solicitantes extranjeros).
- Copia del contrato firmado con el respectivo proveedor del servicio de Internet autorizado (ISP).
- Copia del contrato firmado con la empresa de servicios portadores o de servicios finales que provea el enlace hacia el ISP, y,
- Formulario de Registro a publicarse en la página web del CONATEL, el cual deberá contener como información mínima:

  i. Tipo de red utilizada: Cableada o Inalámbrica
  ii. Detalle del número total de terminales.
  iii. Detalle del número de terminales destinados para navegación;
  iv. Detalle del número de terminales destinados para Voz sobre Internet.
  v. Diagrama esquemático de la red a implementarse en el establecimiento.

Para personas jurídicas:

- Solicitud dirigida al señor Secretario Nacional de Telecomunicaciones.
- Copia de la escritura de constitución de la compañía o, en caso de sociedades extranjeras, de la que contenga su domiciliación en el Ecuador.

- Copia del nombramiento del representante legal, debidamente inscrito en el Registro Mercantil. Las sociedades extranjeras presentarán, por su lado, copia del respectivo poder, asimismo inscrito en el Registro Mercantil.
- Copia del RUC.
- Copia de la cédula de ciudadanía y certificado de votación del representante legal de la compañía.
- Copia del contrato firmado con el respectivo proveedor de Internet autorizado (ISP);
- Copia del contrato firmado con la empresa de servicios portadores o de servicios finales que provea el enlace hacia el ISP, y,
- Formulario de Registro a publicarse en la página web del CONATEL, el cual deberá contener como información mínima:

  i. Tipo de red utilizada: Cableada o Inalámbrica
  ii. Detalle del número total de terminales.
  iii. Detalle del número de terminales destinados para navegación;
  iv. Detalle del número de terminales destinados para Voz sobre Internet.
  v. Diagrama esquemático de la red a implementarse en el establecimiento.

ARTICULO 8.- Los Ciber Cafés que utilicen redes de área local inalámbricas, a fin de obtener el certificado de registro correspondiente, deberán cumplir con lo establecido en el Art. 23 del Reglamento de Radiocomunicaciones (Resolución 556-21-CONATEL- 2000, publicado en el Registro Oficial 215 del 30 de noviembre de 2000).

ARTICULO 9.- Una vez presentada la documentación completa para el registro de Centros de Información y Acceso a la red de Internet o “Ciber Cafés”, y luego del análisis favorable correspondiente, la Secretaría

Nacional de Telecomunicaciones, procederá a entregar el certificado de registro, previo el pago de los derechos correspondientes.

ARTICULO 10.- Por derechos de registro, los Centros de Información y Acceso a la red de Internet o “Ciber Cafés”, cancelarán a la Secretaría el valor de trescientos dólares (300), por una sola vez.

Adicionalmente, por concepto de costos administrativos de la emisión del certificado de registro, los Centros de Información y Acceso a la red de Internet o “Ciber Cafés”, cancelarán a la Secretaría el valor de cien (100) dólares. Los Centros de Información y Acceso a la red de Internet o “Ciber Cafés”, cancelarán a la Secretaría el valor único de cien (100) dólares, en los siguientes casos:

- Cuando dispongan de sólo dos (2) terminales totales; y,
- Cuando operen en zonas rurales y urbano marginales determinadas por la Secretaría Nacional de Telecomunicaciones.

Los Centros de Información y Acceso a la red de Internet o “Ciber Cafés” que ofrezcan servicio sin costo directo o indirecto al usuario, estarán exentos del pago de cualquier rubro por registro o emisión del certificado. Para el efecto, deberán probar documentadamente su condición de proveedor de servicios gratuitos.

ARTICULO 11.- El certificado de Registro, tendrá vigencia por un año y deberá ser renovado en el transcurso de los sesenta (60) días previos a su terminación, para lo cual deberá remitirse el formulario de registro con la información actualizada allí requerida y, posteriormente, realizar el pago de los derechos correspondientes por concepto de costos administrativos de la emisión del certificado de registro. De no solicitarse la renovación dentro del plazo establecido, el certificado de registro caducará sin necesidad de notificación alguna.

ARTICULO 12.- De registrarse cambios en la operación de los Centros de Información y Acceso a la red de Internet o “Ciber Cafés”, ya sea en el tipo de red, número de terminales o proveedores de los servicios portadores y/o finales, así como del ISP, estos cambios deberán ser registrados en la Secretaría Nacional de Telecomunicaciones máximo 30 días luego de ser realizados.

ARTICULO 13.- Dentro del “Plan de difusión y masificación del uso de Internet” y de las políticas del Consejo Nacional de Telecomunicaciones para la conectividad en el Ecuador se crea el Plan “Internet para todos”, bajo los siguientes principios de operación:

1. El objetivo del Plan “Internet para todos” es promocionar, facilitar y permitir el acceso de los sectores más vulnerables de la sociedad, que por su condición económica, social, cultural, étnica o localización geográfica tienen escasa posibilidad de acceder a la red de Internet.

2. Los centros de información y Acceso a la red Internet o “Ciber cafés” que deseen formar parte del Plan “Internet para Todos” podrán manifestar su voluntad expresa de hacerlo al momento de registrarse en la Secretaría Nacional de Telecomunicaciones, o en cualquier momento posterior una vez obtenido el correspondiente registro.

3. Como prestación social al ser parte del Plan deberá permitir el uso del 40% del total de los terminales para navegación gratuita y correo electrónico a los miembros de gremios, asociaciones, fundaciones o instituciones que sean designadas por el Consejo Nacional de Telecomunicaciones como beneficiarios del Plan.

4. La aplicación de este Plan para la navegación gratuita y correo electrónico se realizará por 4 horas diarias, de conformidad con el horario establecido en el Registro, el cual deberá ser debidamente difundido.

5. En casos especiales la Secretaría podrá autorizar a los Centros de Información y Acceso a la Red Internet a conectarse a los Proveedores del Servicio de Internet mediante enlaces propios, siempre y cuando se verifique la imposibilidad de medios de acceso de empresas debidamente autorizadas o que la calidad de los servicios finales o portadores en dicha localidad no garantiza la calidad del servicio.

6. Aquellos Centros de Información y Acceso a la Red Internet que participen del Plan “Internet para todos” se encuentran exentos del pago de derechos establecidos en el artículo diez de la presente resolución.

7. Sin perjuicio de que en el futuro, el Consejo Nacional de Telecomunicaciones incluya otros gremios, asociaciones, fundaciones o instituciones, se consideran beneficiarios del Plan “Internet para todos” a:

   a) Alumnos de instituciones de educación primaria, secundaria y superior.
   b) Docentes de instituciones educativas.
   c) Médicos colegiados.
   d) Personal de Fuerzas Armadas y Policía Nacional.

ARTICULO 14.- Salvo el caso expresado en el artículo trece, numeral 5, la red de acceso entre los Centros de Información y Acceso a la red de

Internet o “Ciber Cafés” y los proveedores de servicios de Valor Agregado, puede presentarse bajo las siguientes modalidades:

a) Mediante un contrato de servicios portadores, con una empresa debidamente autorizada; o,

b) Utilizando servicios finales, con una empresa debidamente autorizada.

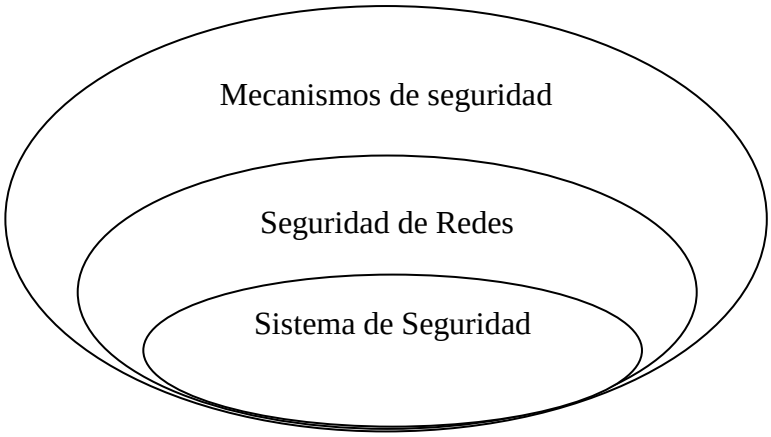
ARTICULO 15.- Las actividades de los establecimientos regulados por el presente instrumento, serán supervisadas y controladas por la Superintendencia de Telecomunicaciones de acuerdo con la Ley.

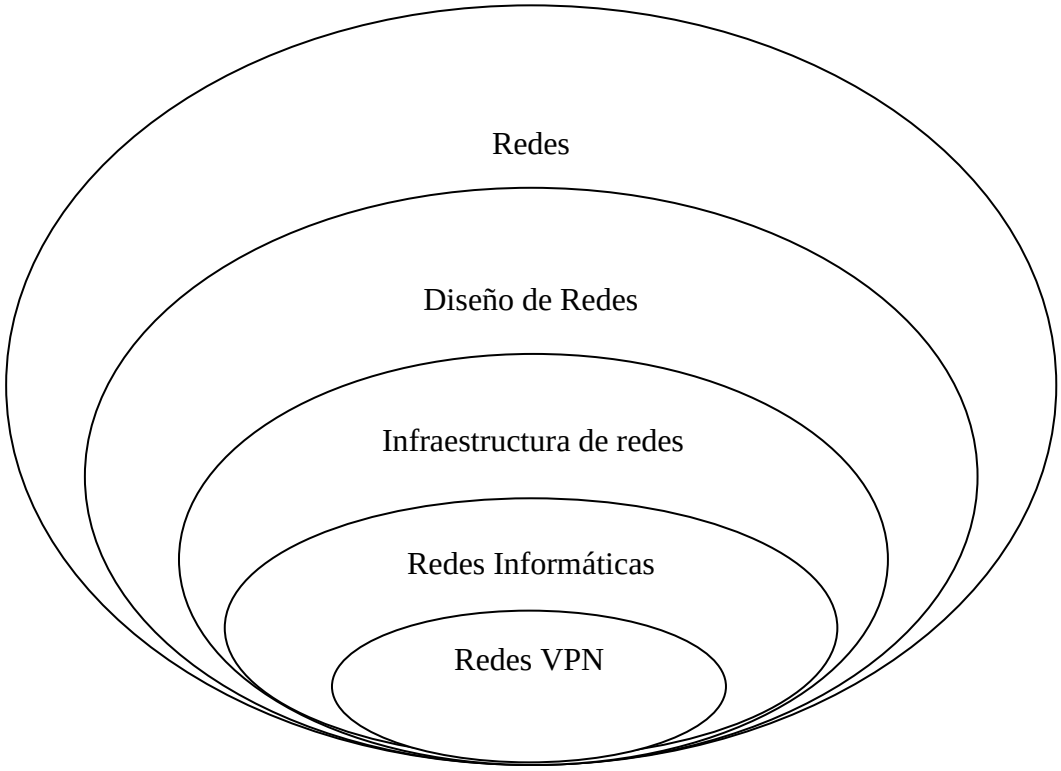
ARTICULO 16.- Los establecimientos regulados por el presente instrumento tienen la obligación de prestar, en todo momento, las facilidades del caso a la Superintendencia de Telecomunicaciones para la inspección de las instalaciones y para que se realicen las pruebas necesarias que permitan determinar si el funcionamiento del establecimiento está conforme con el registro correspondiente. No será necesaria notificación escrita previa para la inspección.

ARTICULO 17.- Los actuales titulares de registros vigentes emitidos por la Secretaría Nacional de Telecomunicaciones, deberán adecuar su funcionamiento y operación a las disposiciones que constan en esta resolución y en un plazo no mayor a sesenta días (60) contados desde su publicación en el Registro Oficial. Sin perjuicio de lo anterior, se aclara que tales titulares podrán seguir realizando sus actividades al amparo de los registros concedidos.

ARTICULO 18.- Las infracciones serán aquellas establecidas en la Ley Especial de Telecomunicaciones.

2.3 Categorías Fundamentales





1. Redes

El término genérico red hace referencia a un conjunto de entidades conectadas entre sí. Por lo tanto, una red permite que circulen elementos materiales o inmateriales entre estas entidades, según reglas bien definidas.

- **red**: Conjunto de equipos y dispositivos periféricos conectados entre sí. Se debe tener en cuenta que la red más pequeña posible está conformada por dos equipos conectados.

- **redes**: implementación de herramientas y tareas para conectar equipos de manera que puedan compartir recursos en la red.

Según el tipo de entidad involucrada, el término utilizado variará:

- **red de transporte**: conjunto de infraestructuras y vehículos usados para transportar personas y bienes entre diferentes áreas geográficas.
- **red telefónica**: infraestructura usada para transportar señales de voz desde una estación telefónica a otra.
- **red neural**: conjunto de neuronas conectadas entre sí.
- **red criminal**: conjunto de estafadores complotados (donde hay un estafador, por lo general hay otro).
- **red informática**: conjunto de equipos conectados entre sí mediante líneas físicas que intercambian información bajo la forma de datos digitales.

Las redes están formadas por conexiones entre grupos de computadoras y dispositivos asociados que permiten a los usuarios la transferencia electrónica de información. Normalmente se trata de transmitir datos, audio y vídeo por ondas electromagnéticas a través de diversos medios. La red de área local es un ejemplo de la configuración utilizada en muchas oficinas y empresas.

Las diferentes computadoras se denominan estaciones de trabajo y se comunican entre sí a través de un cable o línea telefónica conectada a los servidores. Éstos son computadoras como las estaciones de trabajo, pero poseen funciones administrativas y están dedicados en exclusiva a supervisar y controlar el acceso de las estaciones de trabajo a la red y a los recursos compartidos.

Un módem (modulador/demodulador) permite a las computadoras transferir información a través de las líneas telefónicas normales. El módem convierte las señales digitales en analógicas y viceversa, y permite la comunicación entre computadoras muy distantes entre sí. Las redes informáticas se han vuelto cada vez más importantes en el desarrollo de la tecnología de computadoras. El módem es por todas estas razones el método más popular de acceso a la Internet por parte de los usuarios privados y también de muchas empresas.

Las redes son grupos de computadoras interconectados mediante sistemas de comunicación. La red pública Internet es un ejemplo de red informática planetaria. Las redes permiten que las computadoras conectadas intercambien rápidamente información y, en algunos casos, compartan una carga de trabajo, con lo que muchas computadoras pueden cooperar en la realización de una tarea. Se están desarrollando nuevas tecnologías de equipo físico y soporte lógico que acelerarán los dos procesos mencionados.

1.1 Fundamentos de Redes

En las redes se necesita transmitir unidades de información o mensajes: secuencias de items de datos de longitudes arbitrarias. Se divide el mensaje en paquetes antes de ser transmitido. La forma más sencilla de éstos es una secuencia de datos binarios, de una longitud determinada acompañada con información para identificar los computadores origen y destino. Los paquetes deben tener una longitud limitada:

- De esta manera se puede reservar el espacio de almacenamiento para el almacenamiento de un paquete más largo que pudría llegar a recibirse.
- Para evitar retardos que podrían ocurrir si se estuviera esperando a que los canales estén libres el tiempo suficiente para enviar un mensaje largo sin dividir.

1.2 Tipos de redes

Entre los diferentes tipos más comunes de redes de ordenadores

- **Red pública**: una red pública se define como una red que puede usar cualquier persona y no como las redes que están configuradas con clave de acceso personal. Es una red de computadoras interconectadas, capaz de compartir información y que permite comunicar a usuarios sin importar su ubicación geográfica.

- **Red privada**: una red privada se definiría como una red que puede usarla solo algunas personas y que están configuradas con clave de acceso personal.

- **Red de área Personal (PAN)**: (Personal Area Network) es una red de ordenadores usada para la comunicación entre los dispositivos de la computadora (teléfonos incluyendo las ayudantes digitales personales) cerca de una persona. Los dispositivos pueden o no pueden pertenecer a la persona en cuestión. El alcance de una PAN es típicamente algunos metros.

  Las PAN se pueden utilizar para la comunicación entre los dispositivos personales de ellos mismos o para conectar con una red de alto nivel y el Internet. Las redes personales del área se pueden conectar con cables con los buses de la computadora tales

como USB y FireWire. Una red personal sin hilos del área (WPAN) se puede también hacer posible con tecnologías de red tales como IrDA y Bluetooth.

- **Red de área local (LAN)**: una red que se limita a un área especial relativamente pequeña tal como un cuarto, un solo edificio, una nave, o un avión. Las redes de área local a veces se llaman una sola red de la localización. Nota: Para los propósitos administrativos, LANs grande se divide generalmente en segmentos lógicos más pequeños llamados los Workgroups. Un Workgroups es un grupo de las computadoras que comparten un sistema común de recursos dentro de un LAN.

- **Red del área del campus (CAN)**: Se deriva a una red que conecta dos o más LANs los cuales deben estar conectados en un área geográfica específica tal como un campus de universidad, un complejo industrial o una base militar.

- **Red de área metropolitana (MAN)**: una red que conecta las redes de un área dos o más locales juntos pero no extiende más allá de los límites de la ciudad inmediata, o del área metropolitana. Las rebajadoras múltiples, los interruptores y los cubos están conectados para crear a una MAN.

- **Red de área amplia (WAN)**: es una red de comunicaciones de datos que cubre un área geográfica relativamente amplia y que utiliza a menudo las instalaciones de transmisión proporcionadas por los portadores comunes, tales como compañías del teléfono. Las tecnologías WAN funcionan generalmente en las tres capas más bajas del Modelo de referencia OSI: la capa física, la capa de transmisión de datos, y la capa de red.

1.3 Clasificación de las redes de ordenadores

Por capa de red

Las redes de ordenadores se pueden clasificar según la capa de red en la cual funcionan según algunos modelos de la referencia básica que se consideren ser estándares en la industria tal como el modelo OSI de siete capas y el modelo del TCP/IP de cinco capas.

Por la escala

Las redes de ordenadores se pueden clasificar según la escala o el grado del alcance de la red, por ejemplo como red personal del área (PAN), la red de área local (LAN), red del área del campus (CAN), red de área metropolitana (MAN), o la red de área amplia (WAN).

Por método de la conexión

Las redes de ordenadores se pueden clasificar según la tecnología que se utiliza para conectar los dispositivos individuales en la red tal como HomePNA, línea comunicación, Ethernet, o LAN sin hilos de energía.

Por la relación funcional

Las redes de ordenadores se pueden clasificar según las relaciones funcionales que existen entre los elementos de la red, servidor activo por ejemplo del establecimiento de una red, de cliente y arquitecturas del Par-a-par (workgroup). También, las redes de ordenadores son utilizadas para enviar datos a partir del uno a otro por el hardrive.

Por topología de la red

Define como están conectadas computadoras, impresoras, dispositivos de red y otros dispositivos. En otras palabras, una topología de red describe la disposición de los cables y los dispositivos, así como las rutas utilizadas

para las transmisiones de datos. La topología influye enormemente en el funcionamiento de la red.

Las topologías son las siguientes: bus, anillo o doble anillo, estrella, estrella extendida, jerárquica y malla.

Por los servicios proporcionados

Las redes de ordenadores se pueden clasificar según los servicios que proporcionan, por ejemplo redes del almacén, granjas del servidor, redes del control de proceso, red de valor añadido, red sin hilos de la comunidad, etc.

Por protocolo

Las redes de ordenadores se pueden clasificar según el protocolo de comunicaciones que se está utilizando en la red. Ver los artículos sobre la lista de los apilados del protocolo de red y la lista de los protocolos de red para más información.

2. DISEÑO DE REDES

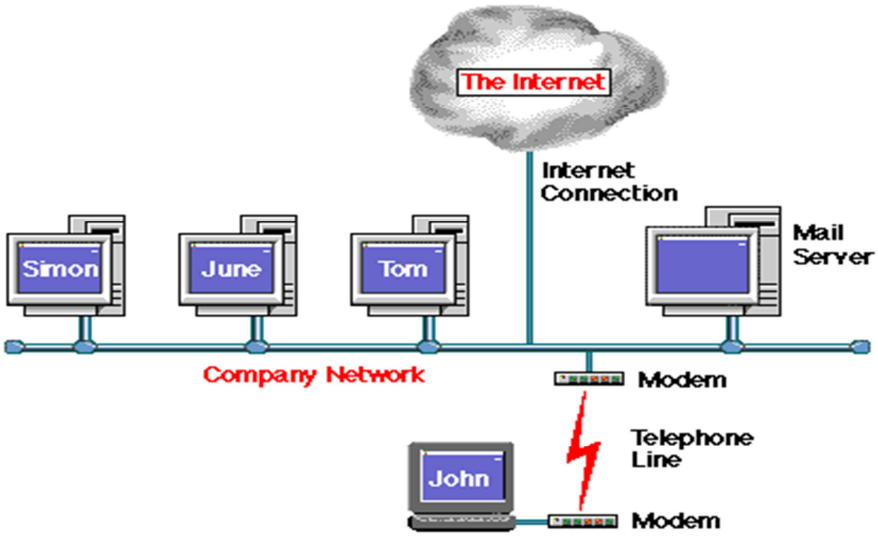


Fig. Nº 2.1 Red Lan

El diseño de una red informática es determinar la estructura física la red. Un buen diseño de la red informática es fundamental para evitar problemas de perdidas de datos, caídas continuas de la red, problemas de lentitud en el procesamiento de la información y problemas de seguridad informática.

En todo diseño de la red se ha de determinar los equipos a utilizar en la red informática: número de switch, switch intermedios ó para grupos, routers, tarjetas Ethernet, así como la disposición de los conectores RJ45. Se debe determinar:

- Tipo de hardware que tiene cada ordenador.
- Elegir el servidor o servidores para las conexiones entre ordenadores.
- Determinar el tipo de adaptadores de red que se necesitan.
- El hardware necesario: modems, routers, switchs, hub, tipo de cable, canaletas.
- Medición del espacio entre los ordenadores y el servidor.

2.1 Análisis para el Diseño de una Red

2.1.1 Topología:

Cuando hablamos de topología de una red, hablamos de su configuración. Esta configuración recoge tres campos: físico, eléctrico y lógico. El nivel físico y eléctrico se puede entender como la configuración del cableado entre máquinas o dispositivos de control o conmutación. Cuando hablamos de la configuración lógica tenemos que pensar en como se trata la información dentro de nuestra red, como se dirige de un sitio a otro o como la recoge cada estación.

Es una manera de tender el cable a estaciones de trabajo individuales; por muros, suelos y techos del edificio. Existe un número de factores a

considerar para determinar cual topología es la más apropiada para una situación dada.

Bus:

En esta topología, los elementos que constituyen la red se disponen linealmente, es decir, en serie y conectados por medio de un cable; el bus. Las tramas de información emitidas por un nodo (terminal o servidor) se propagan por todo el bus (en ambas direcciones), alcanzado a todos los demás nodos. Cada nodo de la red se debe encargar de reconocer la información que recorre el bus, para así determinar cual es la que le corresponde, la destinada a él.

Es el tipo de instalación más sencillo y un fallo en un nodo no provoca la caída del sistema de la red. Por otra parte, una ruptura del bus es difícil de localizar (dependiendo de la longitud del cable y el número de terminales conectados a él) y provoca la inutilidad de todo el sistema.

Como ejemplo más conocido de esta topología, encontramos la red *Ethernet* de Xerox. El método de acceso utilizado es el *CSMA/CD*, método que gestiona el acceso al bus por parte de los terminales y que por medio de un algoritmo resuelve los conflictos causados en las colisiones de información. Cuando un nodo desea iniciar una transmisión, debe en primer lugar escuchar el medio para saber si está ocupado, debiendo esperar en caso afirmativo hasta que quede libre. Si se llega a producir una colisión, las estaciones reiniciarán cada una su transmisión, pero transcurrido un tiempo aleatorio distinto para cada estación.

Esta es una breve descripción del protocolo de acceso *CSMA/CD*, pues actualmente se encuentran implementadas cantidad de variantes de dicho método con sus respectivas peculiaridades. El bus es la parte básica para la construcción de redes Ethernet y generalmente consiste de algunos

segmentos de bus unidos ya sea por razones geográficas, administrativas u otras.

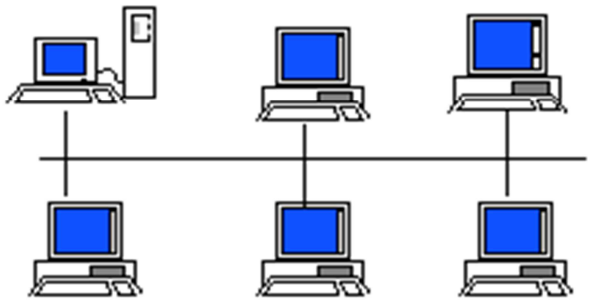


Fig. Nº 2.1.1.1 Topología Bus

Anillo:

Los nodos de la red se disponen en un anillo cerrado conectado a él mediante enlaces punto a punto. La información describe una trayectoria circular en una única dirección y el nodo principal es quien gestiona conflictos entre nodos al evitar la colisión de tramas de información. En este tipo de topología, un fallo en un nodo afecta a toda la red aunque actualmente hay tecnologías que permiten mediante unos conectores especiales, la desconexión del nodo averiado para que el sistema pueda seguir funcionando.

La topología de anillo esta diseñada como una arquitectura circular, con cada nodo conectado directamente a otros dos nodos. Toda la información de la red pasa a través de cada nodo hasta que es tomado por el nodo apropiado. Este esquema de cableado muestra alguna economía respecto al de estrella.

El anillo es fácilmente expandido para conectar más nodos, aunque en este proceso interrumpe la operación de la red mientras se instala el nuevo nodo. Así también, el movimiento físico de un nodo requiere de dos

pasos separados: desconectar para remover el nodo y otra vez reinstalar el nodo en su nuevo lugar.

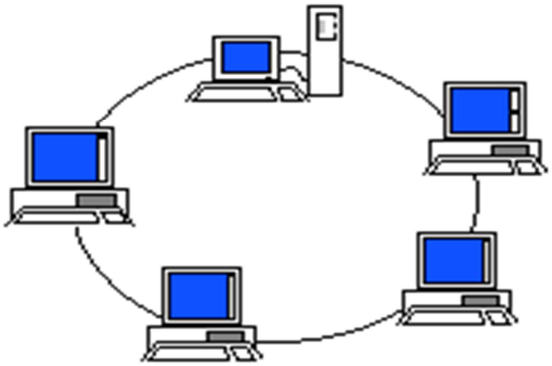


Fig. Nº 2.1.1.2 Topología Anillo

Estrella:

Todos los elementos de la red se encuentran conectados directamente mediante un enlace punto a punto al nodo central de la red, quien se encarga de gestionar las transmisiones de información por toda la estrella. Evidentemente, todas las tramas de información que circulen por la red deben pasar por el nodo principal, con lo cual un fallo en él provoca la caída de todo el sistema. Por otra parte, un fallo en un determinado cable sólo afecta al nodo asociado a él; si bien esta topología obliga a disponer de un cable propio para cada terminal adicional de la red. La topología de Estrella es una buena elección siempre que se tenga varias unidades dependientes de un procesador, esta es la situación de una típica mainframe, donde el personal requiere estar accesando frecuentemente esta computadora. En este caso, todos los cables están conectados hacia un solo sitio, esto es, un panel central.

Equipo como unidades de multiplexaje, concentradores y pares de cables solo reducen los requerimientos de cableado, sin eliminarlos y produce alguna economía para esta topología. Resulta económica la instalación de un nodo cuando se tiene bien planeado su establecimiento, ya que este

requiere de un cable desde el panel central, hasta el lugar donde se desea instalarlo.

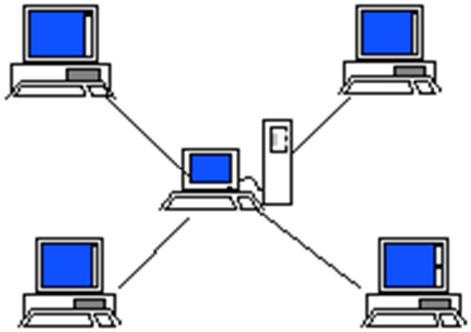


Fig. Nº 2.1.1.3 Topología Estrella

2.1.2 Perdida de las Datos:

La pérdida de datos es producida por algún virus o por otro tipo de incidencia, los mas comunes son mal manejo por parte del usuario o personas inescrupulosas que acceden al sistema o mediante Internet, estos puede incidentes pueden evitarse de tal manera que en las estaciones de trabajo se instalan códigos para que así tengan acceso solo personal autorizado, en cuanto a Internet hay muchos software en el mercado mejor conocidos como Muros de fuego, que sirve para detener a los intrusos.

2.1.3 Caídas Continuas de la Red:

La caída continua en una Red se debe en la mayoría de los casos a una mala conexión

2.1.4 El procesamiento de la información es muy lento:

Cuando el procesamiento de información de una Red es muy lento tenemos que tomar en cuenta el tipo de Equipos que elegimos, (Servidor,

Cableado, Concentrador, Estaciones de Trabajo y otros, ya que si tomamos una decisión errónea perderemos tanto tiempo como dinero.

2.1.5 Utilidades y Funciones:

Un sistema de cableado genérico de comunicaciones para edificios comerciales. Medios, topología, puntos de terminación y conexión, así como administración, bien definidos. Un soporte para entornos multi proveedor multi protocolo. Instrucciones para el diseño de productos de comunicaciones para empresas comerciales. Capacidad de planificación e instalación del cableado de comunicaciones para un edificio sin otro conocimiento previo que los productos que van a conectarse.

2.1.6 Beneficios:

Flexibilidad, Asegura compatibilidad de Tecnologías, Reduce Fallas, Traslado, adiciones y cambios rápidos

2.2 Determinación de los Equipos a utilizar en una Red

2.2.1 Estaciones de Trabajo:

Dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando otros tipos de información. Estos permiten que los usuarios intercambien rápidamente información y en algunos casos, compartan una carga de trabajo.

Las estaciones de trabajo usualmente ofrecen más alto rendimiento de lo que es normalmente encontrado en las computadoras personales, especialmente con lo que respecta a gráficos, poder de procesamiento y habilidades multi-tareas.

Generalmente nos enfocamos en los ordenadores más costosos ya que posee la última tecnología, pero para el diseño de una Red de Área Local solamente necesitamos unas estaciones que cumpla con los requerimientos exigidos, tengamos cuidado de no equivocarnos ya que si damos fallo a un ordenador que no cumpla los requerimientos perderemos tiempo y dinero.

2.2.2 Switch o (HUB):

Es el dispositivo encargado de gestionar la distribución de la información del Servidor (HOST), a las Estaciones de Trabajo y/o viceversa. Las computadoras de Red envían la dirección del receptor y los datos al HUB, que conecta directamente los ordenadores emisor y receptor. Tengamos cuidado cuando elegimos un tipo de concentrador (HUB), esto lo decimos ya que se clasifican en 3 categorías. Solo se usaran concentradores dependiendo de las estaciones de trabajo que así lo requieran.

2.2.3 Switch para Grupos de Trabajo:

Un Switch para grupo de trabajo conecta un grupo de equipos dentro de su entorno inmediato.

2.2.4 Switchs Intermedios:

Se encuentra típicamente en el closet de comunicaciones de cada planta. Los cuales conectan los Concentradores de grupo de trabajo.

2.2.5 Switch Corporativos:

Representa el punto de conexión central para los sistemas finales conectados los concentradores Intermedio.

2.2.6 Modem:

Equipo utilizado para la comunicación de computadoras a través de líneas analógicas de transmisión de datos. El módem convierte las señales digitales del emisor en otras analógicas susceptibles de ser enviadas por teléfono. Cuando la señal llega a su destino, otro módem se encarga de reconstruir la señal digital primitiva, de cuyo proceso se encarga la computadora receptora.

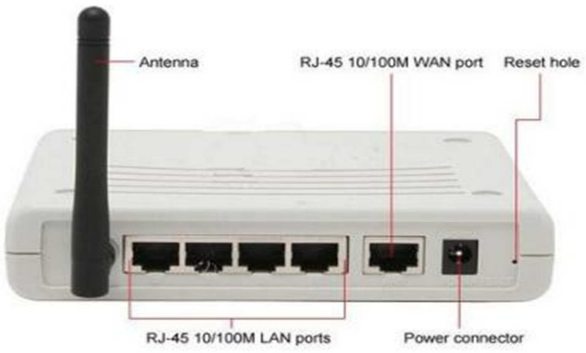


Fig. Nº 2.2.6.1 Modem

2.2.5 Tarjetas Ethernet (Red):

Una tarjeta Ethernet se usa para crear una red, ya sea doméstica o en una oficina, cuando tienes mas de un ordenador y quieres que se comuniquen entre ellos; o conectar a la misma ISP (proveedor de servicios de Internet).

En una red de casa, las posibilidades son grandes ya que podemos aprovecharnos de las ventajas de una red de cableado de alta velocidad, contratando solo un acceso a Internet y compartiéndolo entre todos los PC’s. Habremos creado una LAN rápida y fiable donde compartir archivos, información, datos y jugar en red a velocidades de vértigo. Desde hace décadas, se ha probado que Ethernet es la solución de red mas barata y popular para negocios y empresas.

La tecnología Ethernet permite a productos Ethernet, tales como tarjetas y cables, unir ordenadores, estaciones de trabajo y servidores de cualquier marca y modelo.

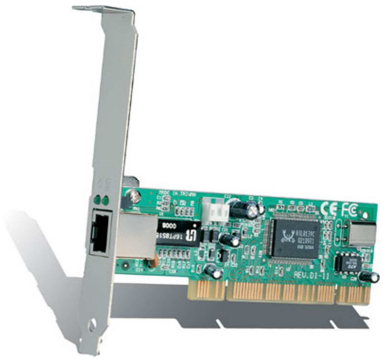


Fig. Nº 2.2.5.1 Tarjeta de Red

Para conectar un cable ethernet a un ordenador, las personas normalmente usan un adaptador de red, también conocido como NIC (*Network Interface Card*).

Entonces, las tarjetas de red “hablarán” con el sistema interno del PC y los cables, transferirán los datos al ordenador al cual está conectado.

2.2.6 Conectores RJ45:

El conector **RJ45** (RJ significa *Registered Jack*) es uno de los conectores principales utilizados con tarjetas de red Ethernet, que transmite información a través de cables de par trenzado. Por este motivo, a veces se le denomina *puerto Ethernet*:

Fig. Nº 2.2.6.1 Conector RJ45

2.2.7 Cableado:

Es el medio empleado para trasmitir la información en la Red, es decir el medio de interconexión entre y las estaciones de trabajo.

3. INFRAESTRUCTURA DE REDES

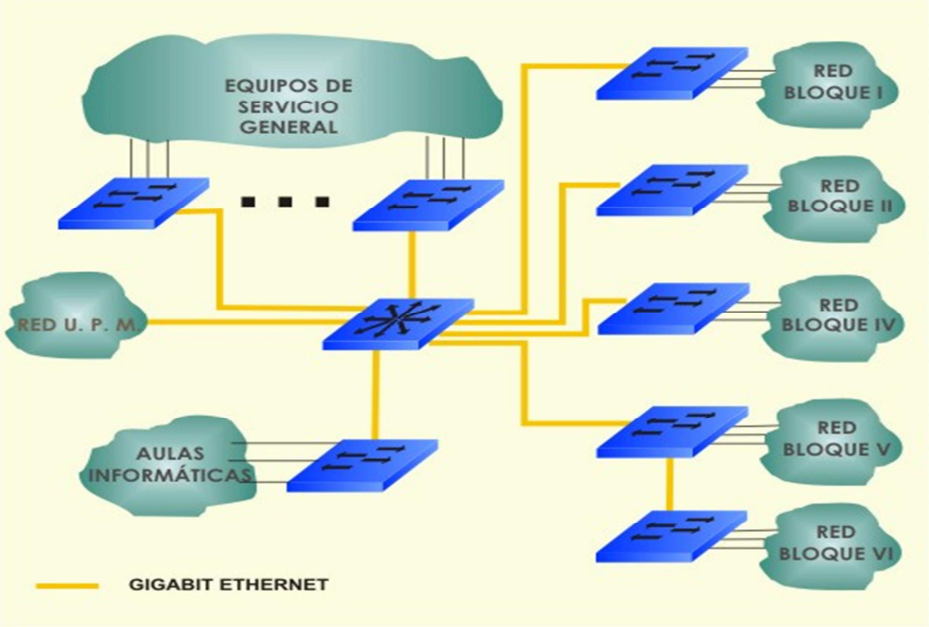


Fig. Nº 3.1 Infraestructura de una Red

Para que su empresa cuente con el mejor desempeño se requiere de una infraestructura tecnológica adecuada que abarca desde la red de alimentación eléctrica hasta una red que sirva de puente a todos los elementos informáticos dentro y fuera de su empresa.

Hoy en día es imposible pensar un sistema informático competitivo que no trabaje en red operando e interactuando entre diversos sectores de la empresa. Tener una RED significa poder compartir recursos; impresoras, unidades de almacenamiento, archivos, conexiones a Internet y mucho más. Lo que resume en un trabajo más eficiente y a menor costo.

Las redes de comunicaciones de datos han crecido en prestaciones y complejidad requiriendo de un tratamiento profesional y especializado

para combinar las mejores alternativas tecnológicas de conectividad acorde a sus necesidades.

4. REDES INFORMATICAS

Las redes informáticas también llamadas según el lugar redes de computadoras o redes de ordenadores, son una serie de de computadoras o dispositivos o de ambos, que están conectados entre si bien por un medio físico (cable) o de manera inalámbrica. Los elementos de la red pueden compartir la información sus archivos, recursos como por ejemplo las impresoras y los servicios como el correo electrónico, juegos, chats etc.. Los administradores de redes, pueden permitir los accesos a los recursos por categorías o prioridades según las necesidades o cargos de cada usuario o grupo de ellos.

Una red es un sistema donde los elementos que lo componen son autónomos y están conectados entre sí por medios físicos y/o lógicos y que pueden comunicarse para compartir recursos. Independientemente a esto, definir el concepto de red implica diferenciar entre el concepto de red física y red de comunicación.

Respecto a la estructura física, los modos de conexión física, los flujos de datos, etc; una red la constituyen dos o más ordenadores que comparten determinados recursos, sea hardware (impresoras, sistemas de almacenamiento...) o sea software (aplicaciones, archivos, datos...). Desde una perspectiva más comunicativa, podemos decir que existe una red cuando se encuentran involucrados un componente humano que comunica, un componente tecnológico (ordenadores, televisión, telecomunicaciones) y un componente administrativo (institución o instituciones que mantienen los servicios). En fin, una red, más que varios ordenadores conectados, la constituyen varias personas que solicitan, proporcionan e intercambian experiencias e informaciones a través de

sistemas de comunicación. Si bien estamos acostumbrados a imaginar una red como formada por computadoras, también pueden intervenir otros equipos como impresoras.

Las redes pueden clasificarse de acuerdo a diversos criterios:

4.1 En base a su extensión:

Redes de área local. Son redes cuya extensión física está limitada a un edificio o una porción del mismo, generalmente dentro de la misma zona, por ejemplo un conjunto de oficinas.

Redes de área amplia (WAN= Wide Area Network). Son redes que abarcan varios edificios más o menos distantes entre si, sobrepasando las fronteras de las ciudades, pueblos o naciones.

Internets. Un internet es una red formada por la interconexión de varias redes a través de ruteadores o puertas de enlace.

Internet: Se trata de una red formada por la interconexión de muchísimas redes distribuidas a través del mundo.

Intranet: Se trata de una red formada por computadoras y ruteadores en forma privada (por lo regular esto se usa en escuelas, comunidades y empresas) y no se puede tener acceso a ella desde internet a menos que tenga la autorización necesaria.

4.2 En base a su funcionamiento

Redes compañero a compañero (P2P=Peer to peer). Son redes en donde todos los equipos tienen el mismo nivel jerárquico y tanto pueden entregar como recibir información.

Redes cliente-servidor. En estas redes, uno o más servidores almacenan la información y los clientes acceden a la misma para utilizarla o modificarla.

4.3 Componentes de una Red

Una red de computadoras esta conectada tanto por hardware como por software. El hardware incluye tanto las tarjetas de interfaz de red como los cables que las unen, y el software incluye los controladores (programas que se utilizan para gestionar los dispositivos y el sistema operativo de red que gestiona la red. A continuación se listan los componentes:

- Servidor.
- Estaciones de trabajo.
- Placas de interfaz de red (NIC).
- Recursos periféricos y compartidos.

Servidor: este ejecuta el sistema operativo de red y ofrece los servicios de red a las estaciones de trabajo.

4.4 Tipos de servidores

En las siguientes listas, hay algunos tipos comunes de servidores y de su propósito.

- **Servidor de archivos**: Una empresa en la que se administre un gran número de documentos puede utilizar un servidor de archivos para un almacenamiento centralizado que permite crear una especie de biblioteca de documentos. Cuando un usuario necesita un archivo, lo busca en el servidor de archivos, trabaja con él localmente en su escritorio y después lo devuelve.

- **Servidor de impresiones**: controla una o más impresoras y acepta trabajos de impresión de otros clientes de la red, poniendo en cola

los trabajos de impresión (aunque también puede cambiar la prioridad de las diferentes impresiones), y realizando la mayoría o todas las otras funciones que en un sitio de trabajo se realizaría para lograr una tarea de impresión si la impresora fuera conectada directamente con el puerto de impresora del sitio de trabajo. En ocasiones, el mismo servidor funciona como servidor de archivos y de impresión.

- **Servidor de correo**: almacena, envía, recibe, enruta y realiza otras operaciones relacionadas con e-mail para los clientes de la red, a través de redes corporativas y a través de internet.

- **Servidor de fax**: un servidor de correo funciona como una oficina postal de red para la administración y el almacenamiento de mensajes: entrega el correo electrónico a los PC cliente o lo aloja para que los usuarios remotos tengan acceso a sus mensajes cuando consideren oportuno.

- **Servidor de la telefonía**: realiza funciones relacionadas con la telefonía, como es la de contestador automático, realizando las funciones de un sistema interactivo para la respuesta de la voz, almacenando los mensajes de voz, encaminando las llamadas y controlando también la red o el Internet, p. ej., la entrada excesiva del IP de la voz (VoIP), etc.

- **Servidor proxy**: realiza un cierto tipo de funciones a nombre de otros clientes en la red para aumentar el funcionamiento de ciertas operaciones (p. ej., prefetching y depositar documentos u otros datos que se soliciten muy frecuentemente), también sirve para la seguridad, esto es, tiene un Firewall. Permite administrar el acceso a internet en una Red de computadoras permitiendo o negando el acceso a diferentes sitios Web.

- **Servidor del acceso remoto (RAS)**: controla las líneas de módem de los monitores u otros canales de comunicación de la red para que las peticiones conecten con la red de una posición remota, responden llamadas telefónicas entrantes o reconocen la petición de la red y realizan los chequeos necesarios de seguridad y otros procedimientos necesarios para registrar a un usuario en la red.

- **Servidor de uso**: realiza la parte lógica de la informática o del negocio de un uso del cliente, aceptando las instrucciones para que se realicen las operaciones de un sitio de trabajo y sirviendo los resultados a su vez al sitio de trabajo, mientras que el sitio de trabajo realiza el interfaz operador o la porción del GUI del proceso (es decir, la lógica de la presentación) que se requiere para trabajar correctamente.

- **Servidor web**: almacena documentos HTML, imágenes, archivos de texto, escrituras, y demás material Web compuesto por datos (conocidos colectivamente como contenido), y distribuye este contenido a clientes que la piden en la red.

- **Servidor de reserva**: tiene el software de reserva de la red instalado y tiene cantidades grandes de almacenamiento de la red en discos duros u otras formas del almacenamiento (cinta, etc.) disponibles para que se utilice con el fin de asegurarse de que la pérdida de un servidor principal no afecte a la red. Esta técnica también es denominada *clustering*.

- **Impresoras**: muchas impresoras son capaces de actuar como parte de una red de ordenadores sin ningún otro dispositivo, tal como un ***"print server"***, a actuar como intermediario entre la impresora y el dispositivo que está solicitando un trabajo de impresión de ser terminado.

- **Terminal tonto**: muchas redes utilizan este tipo de equipo en lugar de puestos de trabajo para la entrada de datos. En estos sólo se exhiben datos o se introducen. Este tipo de terminales, trabajan contra un servidor, que es quien realmente procesa los datos y envía pantallas de datos a los terminales.

- **Otros dispositivos**: hay muchos otros tipos de dispositivos que se puedan utilizar para construir una red, muchos de los cuales requieren una comprensión de conceptos más avanzados del establecimiento de una red de la computadora antes de que puedan ser entendidos fácilmente. En las redes caseras y móviles, que conecta la electrónica de consumidor los dispositivos tales como consolas vídeo del juego está llegando a ser cada vez más comunes.

4.5 Estaciones de Trabajo: Cuando una computadora se conecta a una red, la primera se convierte en un nodo de la ultima y se puede tratar como una estación de trabajo o cliente. Muchas de las veces esta computadora ejecuta su propio sistema operativo y ya dentro, se añade al ambiente de la red. Las estaciones de trabajos pueden ser computadoras personales con el DOS, Macintosh, Unix, OS/2 o estaciones de trabajos sin discos.

4.6 Tarjetas o Placas de Interfaz de Red: Toda computadora que se conecta a una red necesita de una tarjeta de interfaz de red que soporte un esquema de red específico, como Ethernet, ArcNet o Token Ring. Actúan como la interfaz entre un ordenador y el cable de red. La función de la tarjeta de red es la de preparar, enviar y controlar los datos en la red. El cable de red se conectara a la parte trasera de la tarjeta.

4.7 Sistema de Cableado: El sistema de la red esta constituido por el cable utilizado para conectar entre si el servidor y las estaciones de trabajo. Si se está considerando conectar sus equipos de cómputo y de

comunicaciones a un sitio central desde el cual pueda administrarlos, enlazar sus centros de comunicaciones dispersos en su área geográfica o suministrar servicios de alta velocidad a sus computadoras de escritorio, debe pensar en el diseño e implementación de infraestructuras de fibra y cableados que cumplirán con éxito todas sus demandas de voz, datos y video.

Los sistemas de cableado estructurado constituyen una plataforma universal por donde se transmiten tanto voz como datos e imágenes y constituyen una herramienta imprescindible para la construcción de edificios modernos o la modernización de los ya construidos. Ofrece soluciones integrales a las necesidades en lo que respecta a la transmisión confiable de la información, por medios sólidos; de voz, datos e imagen.

La instalación de cableado estructurado debe respetar las normas de construcción internacionales más exigentes para datos, voz y eléctricas tanto polarizadas como de servicios generales, para obtener así el mejor desempeño del sistema.

4.8 Recursos y Periféricos Compartidos: Entre los recursos compartidos se incluyen los dispositivos de almacenamiento ligados al servidor, las unidades de discos ópticos, las impresoras, los trazadores y el resto de equipos que puedan ser utilizados por cualquiera en la red.

4.9 Construcción de una red informática

4.9.1 Una red simple

Una red de ordenadores sencillo se puede construir de dos ordenadores agregando un adaptador de la red (controlador de interfaz de red (NIC) a cada ordenador y conectándolos mediante un cable especial llamado cable cruzado (el cual es un cable de red con algunos cables invertidos,

para evitar el uso de un router o switch). Este tipo de red es útil para transferir información entre dos ordenadores que normalmente no se conectan entre sí por una conexión de red permanente o para usos caseros básicos del establecimiento de una red. Alternativamente, una red entre dos computadoras se puede establecer sin aparato dedicado adicional usando una conexión estándar tal como el puerto serial RS-232 en ambos ordenadores, conectándolos entre sí vía un cable especial cruzado nulo del módem.

En este tipo de red solo es necesario configurar una dirección IP pues no existe un Servidor que les asigne IP automáticamente.

4.9.2 Redes prácticas

Redes prácticas constan generalmente de más de dos ordenadores interconectados y generalmente requieren dispositivos especiales además del controlador de interfaz de red con el cual cada ordenador se debe equipar. Ejemplos de algunos de estos dispositivos especiales son los concentradores (hubs), multiplexores (switches) y enrutadores (routers).

4.9.3 Medios físicos

El medio físico es el encargado de transmitir señales electromagnéticas que son interpretadas por el protocolo de enlace de datos como **bits**. En principio, cualquier medio físico podría ser utilizado, a condición que asegure la transmisión de toda la información sin interferencias. De hecho, las líneas telefónicas, las de televisión por cable y las de energía eléctrica pueden ser utilizadas con ese fin. Sin embargo, en redes locales se utilizan cableados dedicados lo que mejora las velocidades de transmisión.

Otra posibilidad es la transmisión a través del aire, en forma de señales de radio, microondas, etc. La forma en que se interconectan entre sí los distintos **nodos** de la red, determinan su **topología**.

4.10 Servicios de una Red

Para que el trabajo de una red sea efectivo, debe prestar una serie de servicios a sus usuarios, como son:

1. Acceso, este servicios de acceso a la red comprenden tanto la verificación de la identidad del usuario para determinar cuales son los recursos de la misma que puede utilizar, como servicios para permitir la conexión de usuarios de la red desde lugares remotos.

2. Ficheros, el servicio de ficheros consiste en ofrecer a la red grandes capacidades de almacenamiento para descargar o eliminar los discos de las estaciones. Esto permite almacenar tanto aplicaciones como datos en el servidor, reduciendo los requerimientos de las estaciones. Los ficheros deben ser cargados en las estaciones para su uso.

3. Impresión, este servicio permite compartir impresoras entre múltiples usuarios, reduciendo así el gasto. En estos casos, existen equipos servidores con capacidad para almacenar los trabajos en espera de impresión. Una variedad de servicio de impresión es la disponibilidad de servidores de fax.

4. Correo, el correo electrónico, aplicación de red más utilizada que ha permitido claras mejoras en la comunicación frente a otros sistemas. Este servicio además de la comodidad, ha reducido los costos en la transmisión de información y la rapidez de entrega de la misma.

5. Información, los servidores de información pueden bien servir ficheros en función de sus contenidos como pueden ser los documentos hipertexto, como es el caso de esta presentación. O

bien, pueden servir información dispuesta para su proceso por las aplicaciones, como es el caso de los servidores de bases de datos.

6. Otros, generalmente existen en las redes más modernas que poseen gran capacidad de transmisión, en ellas se permite transferir contenidos diferentes de los datos, como pueden ser imágenes o sonidos, lo cual permite aplicaciones como: estaciones integradas (voz y datos), telefonía integrada, servidores de imágenes, videoconferencia de sobremesa, etc.

5. REDES VPN

Es una red privada que se extiende, mediante un proceso de encapsulación y en su caso de encriptación, de los paquetes de datos a distintos puntos remotos mediante el uso de unas infraestructuras públicas de transporte.

Los paquetes de datos de la red privada viajan por medio de un "túnel" definido en la red pública.

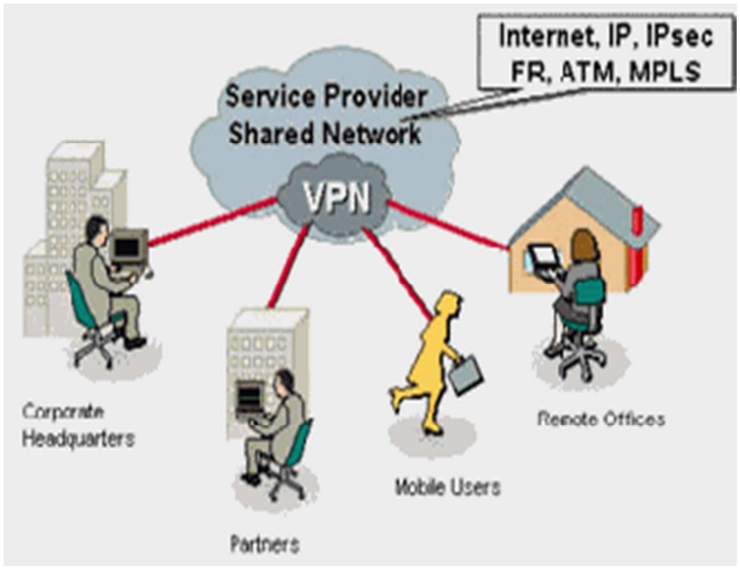


Fig. Nº 5. 1 Redes Privadas

5.1 Tecnología de túnel

Las redes privadas virtuales crean un túnel o conducto de un sitio a otro para transferir datos a esto se le conoce como encapsulación además los paquetes van encriptados de forma que los datos son ilegibles para los extraños.

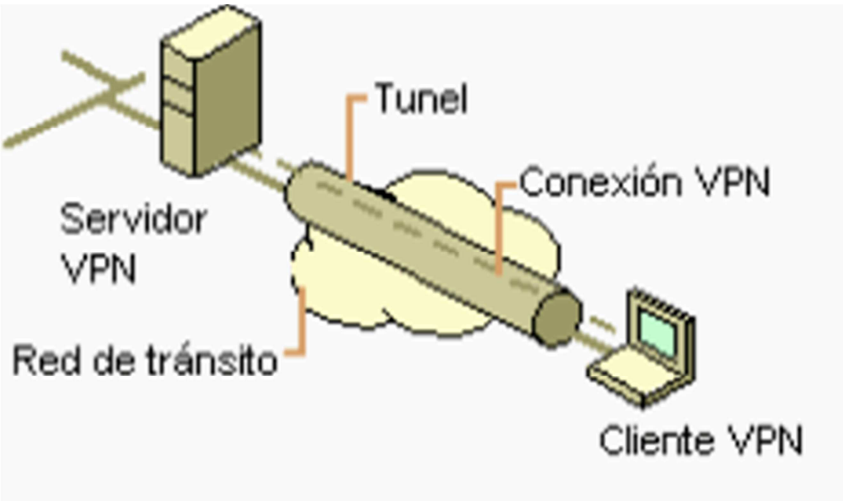


Fig. Nº 5.1.1 Tecnología Túnel

El servidor busca mediante un ruteador la dirección IP del cliente VPN y en la red de transito se envían los datos sin problemas.

5.2 Requerimientos básicos de una VPN

Por lo general cuando se desea implantar una VPN hay que asegurarse que esta proporcione:

- Identificación de usuario
- Administración de direcciones
- Codificación de datos
- Administración de claves

- Soporte a protocolos múltiples
- Identificación de usuario

La VPN debe ser capaz de verificar la identidad de los usuarios y restringir el acceso a la VPN a aquellos usuarios que no estén autorizados. Así mismo, debe proporcionar registros estadísticos que muestren quien acceso, que información y cuando.

Administración de direcciones
La VPN debe establecer una dirección del cliente en la red privada y debe cerciorarse que las direcciones privadas se conserven así.

Codificación de datos
Los datos que se van a transmitir a través de la red pública deben ser previamente encriptados para que no puedan ser leídos por clientes no autorizados de la red.

Administración de claves
La VPN debe generar y renovar las claves de codificación para el cliente y el servidor.

Soporte a protocolos múltiples
La VPN debe ser capaz de manejar los protocolos comunes que se utilizan en la red pública. Estos incluyen el protocolo de internet(IP), el intercambio de paquete de internet(IPX) entre otros.

5.3 Herramientas de una VPN

- VPN Gateway
- Software
- Firewall
- Router

- Dispositivos con un software y hardware especial para proveer de capacidad a la VPN
- Software
- Esta sobre una plataforma PC o Workstation, el software desempeña todas las funciones de la VPN.

5.4 Ventajas de una VPN

Dentro de las ventajas más significativas podremos mencionar la integridad, confidencialidad y seguridad de los datos.

- Sencilla de usar.
- Sencilla instalación del cliente en cualquier PC Windows.
- Control de Acceso basado en políticas de la organización
- Herramientas de diagnostico remoto.
- Los algoritmos de compresión optimizan el tráfico del cliente.
- Evita el alto costo de las actualizaciones y mantenimiento a las PC´s remotas.
- Extensión de conectividad a nivel geográfico
- Mejoras de seguridad
- Reduce costes al ser instalado frente a las redes WAN más utilizadas
- Mejora la productividad
- Simplifica la topología de red
- Proporciona oportunidades de comunicación adicionales

5.5 Pros y Contras de las Redes Virtuales

Tal como en otras tecnologías de redes, existe algo de exageración alrededor del marketing de las redes privadas virtuales. En realidad, las VPN proporcionan unas cuantas ventajas específicas sobre otras formas más tradicionales de redes WAN.

Estas ventajas pueden ser significativas, pero no son gratuitas. Los problemas potenciales con estas redes son superiores a las ventajas y son generalmente más difíciles de entender. Sin embargo, las desventajas no necesariamente sobrepasan a las ventajas. Desde los aspectos de seguridad y desempeño hasta la incompatibilidad entre productos de diferentes proveedores, la decisión de usar o no las redes virtuales no puede tomarse sin una preparación y planificación exhaustivas.

5.6 Tecnología detrás de las Redes VPN

Como resultado del desarrollo de las redes privadas virtuales, se han popularizado varios protocolos de red:

- PPTP
- L2TP
- IPsec
- SOCKS

Estos protocolos enfatizan la autenticación y la encriptación en las redes virtuales. La autenticación permite a los clientes y servidores VPN, establecer correctamente la identidad de los usuarios de la red. La encriptación permite esconder la información confidencial del público general.

5.7 Hardware y Software para Redes Virtuales Privadas

Algunas organizaciones emplean soluciones de hardware VPN para aumentar la seguridad, mientras que otras utilizan las implementaciones basadas en software o protocolos. Hay muchos fabricantes con soluciones de hardware VPN tales como Cisco, Nortel, IBM y Checkpoint. Hay una solución libre de VPN basada en software para Linux llamada FreeS/Wan que utiliza una implementación estandarizada de *IPSec* (o Protocolo de Internet de Seguridad). Estas soluciones VPN, sin importar si

están basadas en hardware o software, actúan como enrutadores especializados que se colocan entre la conexión IP desde una oficina a la otra.

5.8 El futuro de las Redes VPN

Las VPN han crecido en popularidad por el ahorro de dinero que representa para los negocios el acceso remoto a sus redes por parte de los empleados. Muchas empresas también han adoptado las redes VPN como una solución de seguridad para las redes inalámbricas privadas. Se espera un crecimiento en el uso de la tecnología VPN en los próximos años.

5.9 Soluciones VPN y sus Características

Una VPN proporciona conectividad en distancias potencialmente grandes. En este aspecto, una VPN es una forma de red WAN. Las VPN permiten compartir archivos, video conferencias y servicios de red similares. Las VPN generalmente no proporcionan ninguna funcionalidad que no sea ya ofrecida por otras alternativas, pero una VPN implementa esos servicios con mayor eficiencia y economía en la mayoría de los casos.

Así, las **VPN** constituyen una estupenda combinación entre la seguridad y garantía que ofrecen las costosas redes privadas y el gran alcance, lo asequible y lo escalable del acceso a través de Internet. Esta combinación hace de las Redes Privadas Virtuales o VPNs una **infraestructura confiable y de bajo costo** que satisface las necesidades de comunicación de cualquier organización.

Una característica importante de una VPN es su capacidad de trabajar tanto sobre redes privadas como en públicas como la Internet. Utilizando un método llamado "tunneling", una VPN puede usar la misma infraestructura de hardware de las conexiones de Internet o Intranet

existentes. Las tecnologías VPN incluyen varios mecanismos de seguridad para proteger las conexiones virtuales privadas.

5.10 Las Redes VPN soportan cuando menos tres modos de uso

- Conexiones de clientes con acceso remoto
- Interconexiones LAN a LAN
- Acceso controlado dentro de una Intranet

5.10.1 Redes VPN para Acceso Remoto

También conocidas como VPND,usada por una compañía que tienes empleados que necesitan conectarse a la red privada desde distintas localizaciones, es quizás el modelo más usado actualmente, y consiste en usuarios o proveedores que se conectan con la empresa desde sitios remotos (oficinas comerciales, domicilios, hoteles, aviones preparados, etcétera) utilizando Internet como vínculo de acceso.

Una vez autentificados tienen un nivel de acceso muy similar al que tienen en la red local de la empresa. Muchas empresas han reemplazado con esta tecnología su infraestructura dial-up (módems y líneas telefónicas).

En años recientes, muchas organizaciones han aumentado la movilidad de sus colaboradores, permitiendo que más empleados teletrabajen. Los empleados que viajan se enfrentan a una creciente necesidad de permanecer conectados a las redes de su oficina.

Una VPN puede establecerse para soportar acceso remoto protegido a las oficinas corporativas a través de la Internet. Una solución VPN con Internet utiliza un diseño cliente / servidor como sigue:

1. Un huésped remoto (Cliente) que desea ingresar a la red de la empresa, se conecta en primer lugar con un proveedor de servicio de Internet (ISP).

2. En seguida, el huésped inicia una conexión VPN con el servidor VPN de la empresa. Esta conexión se hace vía un software cliente VPN instalado en el huésped remoto.

3. Una vez establecida la conexión, el cliente remoto puede comunicarse con los sistemas internos de la empresa a través de la Internet, tal como si fuera un huésped local.

Antes de las VPN, los trabajadores remotos accesaban las redes empresariales por medio de líneas privadas rentadas o a través de marcado telefónico a servidores remotos.

Si bien es cierto que los clientes y servidores VPN requieren de una instalación cuidadosa de hardware y software, una VPN con Internet constituye una solución superior en muchos casos.

5.10.2 Redes VPN para interconexión entre redes LAN

Además de utilizar las VPN para acceso remoto, también se pueden usar para puentear dos redes locales. En este modo de operación, una red remota completa (No tan solo un cliente remoto) puede conectarse a una red diferente de la empresa para formar una Intranet extendida. Esta solución utiliza una conexión de servidor VPN a servidor VPN.

5.10.3 Redes VPN en redes locales Intranet

También las redes internas (Intranets) pueden usar la tecnología VPN para implementar acceso controlado a subredes individuales dentro de una red privada. En este modo de operación, los clientes VPN se conectan a un servidor VPN que actúa como la compuerta (Gateway) de la red.

Este tipo de aplicación de las VPN no involucra a un Proveedor de Servicio de Internet (ISP) ni al cableado de una red pública. Sin embargo

permite que se implementen los beneficios de seguridad de una VPN dentro de una organización. Esta solución se ha hecho popular especialmente como una forma de que los negocios protejan sus redes inalámbricas locales.

5.11 Las implementaciones

Todas las distintas opciones disponibles en la actualidad caen en tres categorías básicas: soluciones de hardware, soluciones basadas en firewall y aplicaciones VPN por software.

Cada tipo de implementación utiliza diversas combinaciones de protocolos para garantizar las tres características fundamentales mencionadas más arriba: Autenticación, Integridad y Confidencialidad.

El protocolo estándar de hecho es el IPSEC, pero también tenemos PPTP, L2TP, SSL/TLS, SSH, etc. Cada uno con sus ventajas y desventajas en cuanto a seguridad, facilidad, mantenimiento y tipos de clientes soportados.

Actualmente hay una línea de productos en crecimiento relacionada con el protocolo SSL/TLS, que intenta hacer más amigable la configuración y operación de estas soluciones.
Las soluciones de hardware casi siempre ofrecen mayor rendimiento y facilidad de configuración, aunque no tienen la flexibilidad de las versiones por software. Dentro de esta familia tenemos a los productos de Cisco, Linksys, Netscreen, Symantec, Nokia, US Robotics. Etc.

En el caso basado en firewalls, se obtiene un nivel de seguridad alto por la protección que brinda el firewall, pero se pierde en rendimiento. Muchas veces se ofrece hardware adicional para procesar la carga vpn. Ejemplo Checkpoint NG, Cisco Pix.

Las aplicaciones VPN por software son las más configurables y son ideales cuando surgen problemas de interoperatividad en los modelos anteriores. Obviamente el rendimiento es menor y la configuración más delicada, porque se suma el sistema operativo y la seguridad del equipo en general. Aquí tenemos por ejemplo a las soluciones nativas de Windows, Linux y los Unix en general. Por ejemplo productos de código abierto (Open Source) como OpenSSH, OpenVPN y FreeS/Wan.

Las VPN representan una gran solución para las empresas en cuanto a seguridad, confidencialidad e integridad de los datos y prácticamente se ha vuelto un tema importante en las organizaciones, debido a que reduce significativamente el costo de la transferencia de datos de un lugar a otro, el único inconveniente que pudieran tener las VPN es que primero se deben establecer correctamente las políticas de seguridad y de acceso porque si esto no esta bien definido pueden existir consecuencias serias.

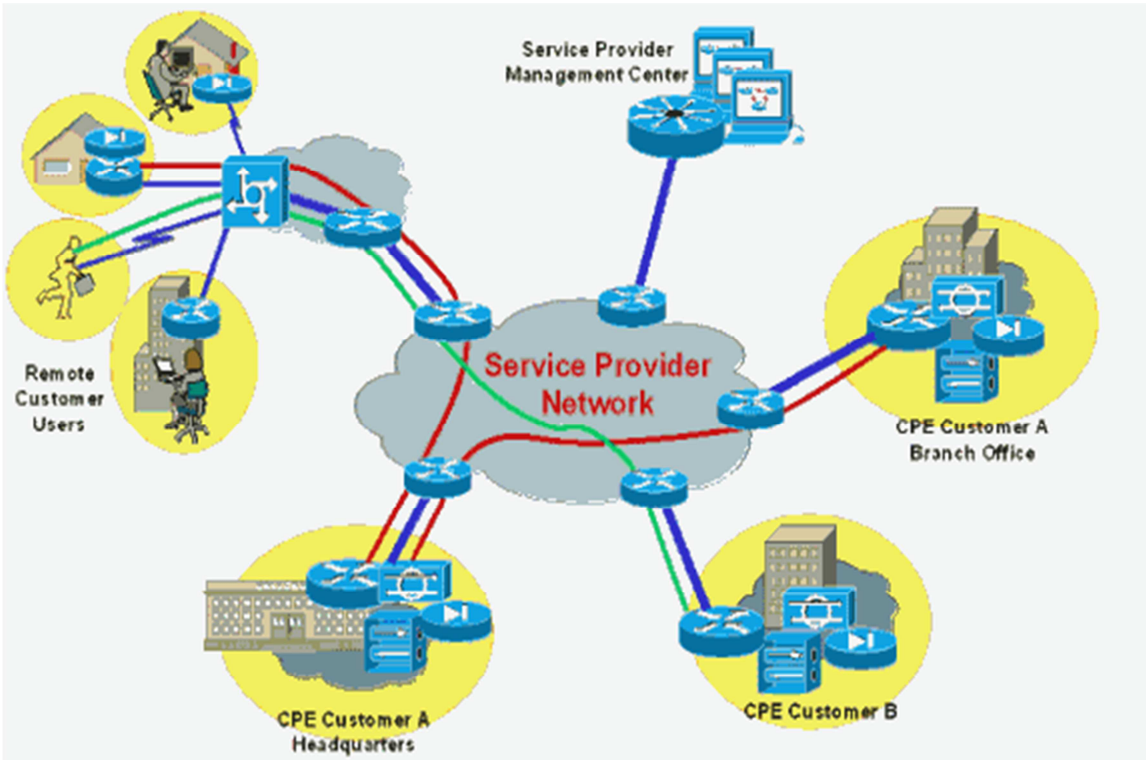


Fig. Nº 5.11.1 Red VPN

6. SEGURIDAD EN REDES

Toda organización debe estar a la vanguardia de los procesos de cambio. Donde disponer de información continua, confiable y en tiempo, constituye una ventaja fundamental.

Donde la información se reconoce como:

- **Crítica**, indispensable para garantizar la continuidad operativa de la organización.
- **Valiosa**, es un activo corporativo que tiene valor en sí mismo.
- **Sensitiva**, debe ser conocida por las personas que necesitan los datos.

Donde identificar los riesgos de la información es de vital importancia.
La seguridad en una red debe garantizar:

- La **Disponibilidad** de los sistemas de información.
- El **Recupero** rápido y completo de los sistemas de información
- La **Integridad** de la información.
- La **Confidencialidad** de la información.

6.1 Diferentes tipos de ataques

Ataques de acceso: un ataque de acceso en un sistema o red para nosotros sería perjudicial por que al entrar en la red o sistema puede alterar documentos, cambiar contraseñas, borrar archivos. Un **Incidente** envuelve un conjunto de ataques que pueden ser distinguidos de otro grupo por las características del mismo.

Sniffers, es un programa de captura de tramas de red. Al tener en nuestra red intrusos podemos darnos cuenta que la persona que realiza el ataque obtiene el camino directo para administrar parte de lo que él pueda cifrar, y con eso perjudicar a la empresa o red involucrada.

Ataques con programas ejecutados en lenguaje máquina, son bastante peligrosos por que entran a nuestra red sin que los dueños nos percatemos en algún archivo o descarga web, y desde el interior del sistema suministra datos a la persona que realiza el ataque. A través de los años se han desarrollado formas cada vez más sofisticadas de ataque para explotar "agujeros" en el diseño, configuración y operación de los sistemas.

Ataques web cuando en páginas piden claves, números de tarjeta, ip de maquinas con eso damos acceso a posibles ataque peligrosos para la red. El ataque de virus en la red es muy peligroso también, no solo los visibles en el sistema operativo sino los que se encuentran en la red misma por ejemplo los que borran los paquetes de bits y con ello no dejan llegar la información

6.2 Métodos y técnicas

Bloquear el acceso a la red a un determinado número de intentos de acceso. Por ejemplo que al tercer intento de poner una contraseña se bloquee el sistema y que solo el administrador pueda recuperar al sistema.

Utilizar muros contra fuegos o firewall que protege para que no puedan ingresar al sistema programas nocivos o de dudosa procedencia.

Utilizar un antivirus actualizado y de último nivel el 70% de las invasiones y daños en la red son provocados por virus y la mayoría simples que borran archivos de la computadora.

Cambiar continuamente de contraseñas de acceso a la red, especialmente cuando alguien salga de la empresa. Controlar los paquetes de bits que ingresan a la máquina con software el especificado

con eso evitamos un ataque en el sistema. Monitorear la red tanto física como lógica constantemente con el objetivo de detectar la presencia de intrusos en la red.

2.4 Hipótesis

Una red VPN, permitirá compartir y transmitir información entre un círculo cerrado de usuarios que están situados en diferentes localizaciones geográficas. Es una red de gran seguridad que permite la transmisión de información confidencial entre la empresa y sus sucursales, socios, proveedores, distribuidores, empleados y clientes, utilizando Internet como medio de transmisión.

2.5 Variables

2.5.1 Variable Independiente

Estudio de Seguridades

2.5.2 Variable Dependiente

Redes Privadas Virtuales

CAPITULO III
METODOLOGIA

3.1 Enfoque

La presente investigación se realizará bajo la óptica del paradigma cuali-cuantitativo porque se efectuará una investigación desde el punto de origen de una red, estudiando de manera científica una muestra reducida de objetos de investigación, la información proporcionada servirá de referencia para interpretarla con el sustento científico y profesional, con lo que se pretende solucionar el problema.

Se considera la parte cuantitativa que estará enmarcada en un análisis de resultados de calidad en base al marco teórico consultado y que servirá de base para la toma de decisiones.

3.2 Modalidad básica de la investigación

3.2.1 Investigación Bibliográfica - Documental

Se realizará una investigación bibliográfica - documental para poder obtener información mas profunda con respecto a problemas similares, de esta manera recopilar información valiosa que servirá de apoyo en la realización del proyecto, constituyéndose en una estrategia donde se observe y se reflexione sistemáticamente sobre realidades, utilizando técnicas muy precisas.

3.3 Nivel o tipo de Investigación

3.3.1 Exploratorio

Es exploratorio porque se realizara un análisis preliminar de la situación con un mínimo de costo y tiempo, buscando indicios acerca de la naturaleza general del problema, además que es apropiada en situaciones de reconocimiento y definición del problema, siendo útil para la identificación de cursos alternativos de acción, en el cual utilizamos métodos de recolección de información, altamente flexibles, no estructurados y cualitativos.

3.3.2 Descriptivo

Es descriptivo porque se desea llegar a conocer las situaciones predominantes a través de la descripción exacta de las actividades para la realización del proyecto, de esta manera su meta no se limita a la recolección de datos, sino a la predicción e identificación de las relaciones que existen entre dos o más variables.

3.4 Población y muestra

3.4.1 Población

La presente investigación se realizará con el asesoramiento de nueve docentes que trabajarán en el seminario.

3.4.2 Muestra

Se tiene una población pequeña por lo tanto se trabajará con todo el universo.

3.5 Recolección de información

3.5.1 Plan de Recolección de Información

La información será recolectada una vez realizado el análisis del problema, cuya información será proporcionada por los docentes de redes y de esta manera elaborar el sistema de la mejor manera posible.

3.6 Procesamiento y análisis de la Información

3.6.1 Plan que se empleará para procesar la información recogida.

Lo primero que se realizará antes de recopilar la información, será conocer con exactitud el problema y una vez recopilados los datos se estudiará el problema, de esta manera se asegurará que los datos sean lo más reales posibles, y se los procesará para la obtención de resultados.

3.6.2 Plan de análisis interpretación de resultados

Los datos que se obtendrán de la recolección de información, contribuirán a tener un conocimiento completo del problema, también se realizará una investigación profunda del origen del mismo y de los posibles factores que ayudarán al estudio de seguridades mediante VPN, ya que esto será parte fundamental de la propuesta.

CAPITULO IV
ANALISIS E INTERPRETACION DE RESULTADOS

4.1Concepto: Son líneas alquiladas que están conectadas a otros puntos y puedan hacer uso de la conexión a Internet o para hacer negocios con clientes frecuentes a través de la red.

4.2 Extensión: La de una red local sobre una red pública o no controlada.

4.3 Medio de comunicación: privada

4.4 Medio de transmisión que utiliza: Una conexión VPN router a router es realizada por un router, y este a su vez se conecta a una red.

En este estudio se realizo un análisis para Redes Privadas Virtuales, permitiendo diferente resultados que garanticen la fiabilidad y buen progreso de una red, se podría desarrollar un plan integral de seguridad que se pretenda cubrir distintas fases como:

- Consultoría y análisis de sus redes, estudiando y analizando sus puntos débiles.
- Elaboración de un plan de acción y estudios de los equipos a instalar en sus instalaciones.
- Instalación y puesta en marcha de la electrónica.
- Formación de todas las personas implicadas en el plan de seguridad de la empresa.

- Mantenimiento de todos los equipos y redes.
- Supervisión y análisis continúo de sus redes.

Para llevar a cabo las políticas de seguridad en cualquier compañía se debe contar con un equipo humano especialmente cualificado

Dependiendo del tipo de VPN, se tendrán que poner en su sitio, ciertos elementos para poder construir una VPN. Se podrían incluir:

- Un software de cliente para cada usuario remoto que se quiera conectar.
- Un hardware dedicado, como un concentrado VPN y/o un firewall.
- Un servidor VPN dedicado para dar servicios de marcado (dial-up), que es simplemente lo que hace un modem para acceder a la red.
- Un RAS o servidor de acceso usado por el proveedor de servicios para los usuarios remotos.
- La red VPN y el centro de gestión de políticas.

Al no haber un estándar ampliamente aceptado para implementar VPN, muchas compañías han desarrollado algunas soluciones por si mismas, con sus propios equipamientos y servicios.

CAPITULO V
CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

Las redes **VPN** disminuyen significativamente costos adicionales por comunicación y/o compartición de recursos entre dependencias de una misma empresa que se encuentran geográficamente distantes; a diferencia de enlaces WAN que representan altos costos mensuales. Por lo tanto se puede concluir que el uso de VPNs es conveniente para una empresa.

Se utiliza una conexión **VPN** de acceso remoto para facilitar la comunicación entre un empleado fuera de la empresa con los servicios y usuarios de la red LAN interna. Se puede concluir, con el estudio realizado, que mientras un usuario remoto se encuentre conectado a la red **VPN** de la empresa, únicamente podrá acceder a los servicios y sitios dentro de la Intranet, restringiendo el acceso del usuario remoto hacia Internet.

Durante el estudio realizado, en un escenario **VPN** de Acceso Remoto, se determinó que cuando más de un usuario está asociado a una única conexión a Internet; por ejemplo, en un Cybercafe, solo se podrá conectar un usuario remoto a la vez, debido a que el servidor **VPN,** registra la dirección IP pública con la que se está accediendo al túnel, por lo que no se podrán tener más de una conexión con la misma dirección pública.

5.2 Recomendaciones

Si se desea implementar una **VPN,** se recomienda brindar servicios adicionales aprovechando el túnel establecido, por lo que el presente brindar el servicio de VoIP. Entre los servicios que se pueden brindar a través del túnel se encuentra el servicio de escritorio remoto, teletrabajadores, video conferencia, compartición de recursos como documentos e impresoras, etc.

Se recomienda que las contraseñas tengan un periodo corto de duración y el administrador del túnel las cambie periódicamente, de esta manera se evita que algún usuario no autorizado acceda al túnel.

Se recomienda mantener una base de datos en donde se almacenen las extensiones telefónicas con sus respectivas identificaciones, usuarios, número de extensión y contraseñas. En caso de que se llegue a tener un gran número de usuarios y de extensiones en la central.

CAPITULO VI
PROPUESTA

6.1. Datos Informativos

Tema:

Estudio de Seguridades usando redes privadas virtuales.

Autora:

Kattia Marisela Rodríguez Mora

Tutor:

Ing. Javier Sánchez

Fecha Duración:

06/11/08 - 06/04/09

6.2 Antecedentes de la propuesta

La seguridad de la información es un componente crítico de la estrategia de negocio de cualquier organización. En los últimos años habido un enorme desarrollo tecnológico en el área de telecomunicaciones; ejemplo

de esto son la convergencia de diferentes redes de voz y datos a redes con tecnología IP, las redes inalámbricas locales, redes inalámbricas de banda ancha y su integración con las redes de telefonía celular, el uso de Internet para redes privadas (VPN), etc.

Para poder ofrecer una propuesta adecuada que contemple todos los aspectos necesarios se realizó un estudio detallado sobre el tráfico real entre diferentes delegaciones y una central, así como las aplicaciones con las que trabajaban y los tiempos de respuesta obtenidos, dentro cualquier empresa a la que se desee implantar este sistema.

También se consideraron los diferentes escenarios actuales y futuros, con la consiguiente estimación de cómo podrían afectar a las comunicaciones que se pretendería instalar.

El resultado fue una propuesta que permitiera el uso de líneas alquiladas que estén conectadas a otros puntos que puedan hacer uso de la conexión a Internet o para hacer negocios con clientes frecuentes a través de la red, es decir la implantación de redes VPN, de esta manera, se podría seguir trabajando como si todos los equipos informáticos estuvieran conectados a la misma LAN.

La idea es montar un sistema en el que la persona que tenga mejor disponibilidad, conexión, haga de nodo central para ir conectando con ellos, independientemente de otras VPNS que tengamos con el resto de nodos.

Las VPN representan una gran solución para las empresas en cuanto a seguridad, confidencialidad e integridad de los datos y ha pasado a ser un tema importante en las organizaciones, debido a que reduce significativamente el costo de la transferencia de datos de un lugar a otro.

6.3 Justificación

La mayoría de las empresas necesitan trabajar con agilidad, ser capaces de adaptar las funciones a las nuevas necesidades o introducirse rápidamente en nuevos mercados para responder a las nuevas demandas. La estructura de las comunicaciones puede rentalizar estos procesos. Cuando se habla con compañías telefónicas locales o con compañías de telecomunicaciones a larga distancia sobre los costos de instalar una red de área amplia o WAN corporativa de línea cedida, es probable que se sufra una fuerte sorpresa. A pesar de la extraordinaria explosión de la red Internet y del advenimiento de la fibra óptica de alta velocidad, la anchura de banda y especialmente la anchura de banda de larga distancia siguen resultando extraordinariamente costosas. Y como la cantidad de proveedores de líneas cedidas sigue siendo bastante limitada, los precios no van a descender a corto plazo.

A través de la investigación se pudo detectar las necesidades y problemática que poseen las redes en diferentes empresas, es por ese motivo que cada vez más directores IS están recurriendo a redes privadas virtuales, VPNs (Virtual Private Networks) que utilizan la red Internet para conectar a localizaciones remotas y a personas que trabajan en casa con sus oficinas principales. Como las redes VPN dependen de la Internet y no de líneas cedidas dedicadas, ofrecen una forma más económica de establecer conexiones WAN, especialmente en trayectos largos.

6.4 Objetivos

6.4.1 Objetivo General

Conseguir una red a un coste asequible en infraestructura y posterior mantenimiento, pero al mismo tiempo proteger toda la información transmitida.

6.4.2 Objetivo Específicos

- Configurar una Red Privada Virtual sobre la red pública Internet, optimizando de esta forma los recursos y reduciendo costes.

- Con una Red Privada Virtual establecemos una serie de túneles entre los centros remotos y la sede principal, permitiendo el acceso a los servidores de la Intranet central a todos los usuarios de cada delegación como si se encontrasen en una misma red local.

- Obtener beneficios tales como: privacidad (todos los datos transmitidos van encriptados, por lo que se garantiza la confidencialidad de los mismos), integridad (existen mecanismos por los que se garantiza el mensaje no ha sido modificado durante el envío), autenticación (el emisor firma sus mensajes digitalmente, de forma que el receptor puede comprobar que realmente fue enviado por él).

- Dar una solución para las comunicaciones, sencilla de implantar y que proporciona beneficios a corto plazo

6.5 Análisis de factibilidad

6.5.1 Factibilidad Tecnológica

El presente estudio contempla la posibilidad de realizar el proyecto, se realizó un análisis de la propuesta a desarrollar y las características de hardware y software del proyecto son totalmente accesibles, se tiene las capacidades técnicas requeridas por cada alternativa del diseño que se esté considerando. También se debe considerar si la organización en la que se desea desarrollar el proyecto tiene el personal que posea la

experiencia técnica requerida para diseñar, implementar, operar y mantener el sistema propuesto. Si el personal no tiene esta experiencia, puede entrenársele o pueden emplearse nuevos o consultores que la tengan. Sin embargo, una falta de experiencia técnica dentro de la organización puede llevar al rechazo de una alternativa particular.

6.5.2 Factibilidad Económica

Este proyecto es posible implementarlo dentro de cualquier empresa que cuente con el presupuesto necesario para poder realizarlo. Los costos de implementación incluyen comúnmente el costo remanente de la investigación de sistemas, los costos de hardware y software, los costos de operación del sistema para su vida útil esperada, y los costos de mano de obra, material, energía, reparaciones y mantenimiento.

6.5.3 Factibilidad Operativa

El proyecto es operativo, en virtud que es posible conectar un conjunto de computadoras personales formando una red que permita que un grupo o equipo de personas involucrados en proyectos similares puedan comunicarse fácilmente y compartir programas.

6.6 Fundamentación Teórica

Red Privada

Enfoque

Intercomunicación y conexión de oficinas de una misma empresa.

Servicios

Cada servicio extra o implementación de nueva tecnología incurre en un costo de Inversión

Seguridad

Se puede detallar de forma específica, el nivel de seguridad que la empresa requiera.

Control

Se tiene el control total de los recursos, de la administración (anchos de banda y topología de la red), manipulación y entrega de la información.

Red Pública

Enfoque

Comunicación fuera de las empresas. Interconexión de Redes Privadas.

Servicios

Reducción de los costos de Valor Agregado. Facilidad para mantenerse en la vanguardia tecnológica

Seguridad

El proveedor suele ofrecer cierto nivel de seguridad, pero por el hecho de ser una red pública el acceso de cualquier persona no autorizada a la red es muy sencillo.

Inversiones

Los costos de inversión se reducen dramáticamente para el usuario, solo se necesita invertir en equipo de acceso a la red.

Conectividad

Capacidad de transmisión a todos los puntos de enlace de la red. Facilidad para dar de alta a nuevos usuarios.

Protocolo de túnel punto a punto (PPTP)

PPTP permite la transferencia segura de datos desde un equipo remoto a un servidor privado al crear una conexión de red privada virtual a través de redes de datos basadas en IP. PPTP acepta redes privadas virtuales bajo demanda y multiprotocolo a través de redes públicas, como Internet.

Desarrollado como una extensión del Protocolo punto a punto (PPP), PPTP agrega un nuevo nivel de seguridad mejorada y comunicaciones multiprotocolo a través de Internet.

PPTP encapsula los protocolos IP en datagramas PPP. Esto significa que puede ejecutar de forma remota aplicaciones que dependen de protocolos de red específicos. El servidor de túnel ejecuta todas las comprobaciones y validaciones de seguridad, y activa el cifrado de los datos, lo que hace mucho más seguro el envío de información a través de redes no seguras. También se puede utilizar PPTP para establecer conexiones de LAN a LAN privadas.

PPTP requiere conectividad IP entre el equipo y el servidor. Si está directamente conectado a una LAN IP y puede tener acceso a un servidor, puede establecer un túnel PPTP en la LAN. Si va a establecer un túnel a través de Internet y normalmente tiene acceso a Internet a través de una conexión de acceso telefónico con un ISP, debe conectarse a Internet antes de establecer el túnel.

Protocolo de túnel de capa dos (L2TP)

L2TP es un protocolo estándar de túnel para Internet que tiene casi la misma funcionalidad que el Protocolo de túnel punto a punto (PPTP). La implementación de L2TP en la familia de Windows Server 2003 se ha diseñado para ejecutarse de forma nativa a través de redes IP.

Al igual que PPTP, L2TP encapsula las tramas del Protocolo punto a punto (PPP), que a su vez encapsulan los protocolos IP, con lo que permiten que los usuarios ejecuten de forma remota aplicaciones que dependen de protocolos de red específicos.

Con L2TP, el equipo que ejecuta un miembro de la familia Windows Server 2003 en el que va a iniciar la sesión ejecuta todas las comprobaciones y validaciones de seguridad, y activa el cifrado de los datos, lo que hace mucho más seguro el envío de información a través de redes no seguras.

Teletrabajo

El teletrabajo es una forma flexible de organización del trabajo en la que éste se realiza, con la ayuda de las tecnologías de la información y las comunicaciones, en un lugar distinto y alejado del que ocupa la organización o la persona para la que se realiza el trabajo. El teletrabajo implica, por tanto, el uso de métodos de procesamiento electrónico de la información y de algún medio de telecomunicación para el contacto con la empresa o los clientes.
El teletrabajo abarca las actividades laborales por cuenta ajena realizadas total y parcialmente fuera de las empresas, el trabajo en casa o desde centros específicos y el trabajo móvil o nómada de aquellos trabajadores cuya actividad requiere desplazamientos permanentes, siempre que se trate de un trabajo soportado por las tecnologías de la información y las comunicaciones.

Dentro del concepto de teletrabajo se incluyen también las actividades por cuenta propia realizadas para clientes distantes utilizando las telecomunicaciones. Se puede teletrabajar mediante contrato por obra o servicio, a tiempo parcial o completo, en nómina, como colaborador o en forma independiente, estos es, con las mismas modalidades de contratación que en el trabajo tradicional.

La actual expansión del teletrabajo es el resultado de dos factores que se interrelacionan de forma dinámica: la aplicación laboral de las tecnologías de la información y la existencia de una infraestructura de telecomunicaciones razonablemente avanzada.

Acceso Remoto

Es una manera de acceder desde una computadora a un recurso ubicado físicamente en otra computadora, a través de una red local o externa (como internet).

En el acceso remoto se ven implicados protocolos para la comunicación entre máquinas, y aplicaciones en ambas computadoras que permitan recibir/enviar los datos necesarios. Además deben contar con un fuerte sistema de seguridad (tanto la red, como los protocolos y las aplicaciones).

Remotamente se puede acceder prácticamente a cualquier recurso que ofrece una o más computadoras. Se pueden acceder a archivos, dispositivos periféricos (como impresoras), configuraciones, etc. Por ejemplo, se puede acceder a un servidor de forma remota para configurarlo, controlar el estado de sus servicios, transferir archivos, etc.

Autenticación

Las técnicas de autenticación son esenciales en las VPNs, ya que aseguran a los participantes de la misma que están intercambiando información con el usuario o dispositivo correcto. La autenticación en VPNs es conceptualmente parecido al logeo en un sistema como nombre de usuario y contraseña, pero con necesidades mayores de aseguramiento de validación de identidades. La mayoría de los sistemas

de autenticación usados en VPN están basados en un sistema de claves compartidas.

La autenticación es llevada a cabo generalmente al inicio de una sesión, y luego aleatoriamente durante el curso de la misma, para asegurar que no haya algún tercer participante que se haya intrometido en la conversación. La autenticación también puede ser usada para asegurar la integridad de los datos.

Encriptación

Todas las VPNs tienen algún tipo de tecnología de encriptación, que esencialmente empaqueta los datos en un paquete seguro. La encriptación es considerada tan esencial como la autenticación, ya que protege los datos transportados de poder ser vistos y entendidos en el viaje de un extremo a otro de la conexión. Existen dos tipos de técnicas de encriptación que se usan en las VPN: encriptación de clave secreta, o privada, y encriptación de clave pública.

En la encriptación de clave secreta, se utiliza una contraseña secreta conocida por todos los participantes que necesitan acceso a la información encriptada. Dicha contraseña se utiliza tanto para encriptar como para desencriptar la información. Este tipo de encriptación posee el problema que, como la contraseña es compartida por todos los participantes y debe mantenerse secreta, al ser revelada, debe ser cambiada y distribuida a los participantes, con lo cual se puede crear de esta manera algún problema de seguridad.

La encriptación de clave pública implica la utilización de dos claves, una pública y una secreta. La primera es enviada a los demás participantes. Al encriptar, se usa la clave privada propia y la clave pública del otro participante de la conversación. Al recibir la información, ésta es desencriptada usando su propia clave privada y la pública del generador

de la información. La gran desventaja de este tipo de encriptación es que resulta ser más lenta que la de clave secreta.

En las VPNs, la encriptación debe ser realizada en tiempo real. Por eso, los flujos encriptados a través de una red son encriptados utilizando encriptación de clave secreta con claves que son solamente buenas para sesiones de flujo.

IPsec

Es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos.

IPsec está implementado por un conjunto de protocolos criptográficos para:

- Asegurar el flujo de paquetes
- Garantizar la autenticación mutua
- Establecer parámetros criptográficos.

La arquitectura de seguridad IP utiliza el concepto de asociación de seguridad (SA) como base para construir funciones de seguridad en IP. Una asociación de seguridad es simplemente el paquete de algoritmos y parámetros (tales como las claves) que se está usando para cifrar y autenticar un flujo particular en una dirección. Por lo tanto, en el tráfico normal bidireccional, los flujos son asegurados por un par de asociaciones de seguridad.

IPSec autentifica los equipos y cifra los datos para su transmisión entre hosts en una red, intranet o extranet, incluidas las comunicaciones entre

estaciones de trabajo y servidores, y entre servidores. El objetivo principal de IPSec es proporcionar protección a los paquetes IP.

IPSec está basado en un modelo de seguridad de extremo a extremo, lo que significa que los únicos hosts que tienen que conocer la protección de IPSec son el que envía y el que recibe. Cada equipo controla la seguridad por sí mismo en su extremo, bajo la hipótesis de que el medio por el que se establece la comunicación no es seguro.

IPSec aumenta la seguridad de los datos de la red mediante:

- La autenticación mutua de los equipos antes del intercambio de datos. IPSec puede utilizar Kerberos V5 para la autenticación de los usuarios.

- El establecimiento de una asociación de seguridad entre los dos equipos. IPSec se puede implementar para proteger las comunicaciones entre usuarios remotos y redes, entre redes e, incluso, entre equipos cliente dentro de una red de área local (LAN).

El protocolo también proporciona las ventajas siguientes:

- Compatibilidad con la infraestructura de claves públicas.
- Compatibilidad con claves compartidas.
- Transparencia de IPSec para los usuarios y las aplicaciones.
- Administración centralizada y flexible de directivas mediante Directiva de grupo.
- Estándar abierto del sector. IPSec proporciona una alternativa de estándar industrial abierto ante las tecnologías de cifrado IP patentadas. Los administradores de la red aprovechan la interoperabilidad resultante.

Existen dos modos de operaciones del IPsec:

Modo transporte (Transport mode): En este modo, solamente la carga útil (el mensaje) del paquete IP es encriptada.

Modo túnel (Tunnel mode): en este modo, el paquete IP completo es encriptado. Debe ser luego encapsulado en un nuevo paquete IP para tareas de ruteo.

ADSL

El ADSL (Asymetric Digital Subscriber Line, o lo que es lo mismo, Línea de usuario digital asimétrica), es una tecnología de acceso a Internet de banda ancha, lo que implica una mayor velocidad en la transferencia de datos. Esto se consigue mediante una modulación de las señales de datos en una banda de frecuencias más alta que la utilizada en las conversaciones telefónicas convencionales (300-3800 Hz), función que realiza el Router ADSL. Para evitar distorsiones en las señales transmitidas, es necesaria la instalación de un filtro (llamado *splitter* o discriminador) que se encarga de separar la señal telefónica convencional de las señales moduladas de la conexión mediante ADSL.

Fig. Nº 6.6.1 Conexión ADSL

Esta tecnología se denomina *asimétrica* debido a que la capacidad de descarga (desde la Red hasta el usuario) y de subida de datos (en sentido inverso) no coinciden. Normalmente, la capacidad de bajada (descarga) es mayor que la de subida.

En una línea ADSL se establecen tres canales de comunicación, que son el de envío de datos, el de recepción de datos y el de servicio telefónico normal.

UDP

El protocolo UDP (*Protocolo de datagrama de usuario*) es un protocolo no orientado a conexión de la capa de transporte del modelo TCP/IP. Este protocolo es muy simple ya que no proporciona detección de errores (no es un protocolo orientado a conexión).

Por lo tanto, el encabezado del segmento UDP es muy simple:

puerto de origen (16 bits);	puerto de destino (16 bits);
longitud total (16 bits);	suma de comprobación del encabezado (16 bits);
datos (longitud variable).	

Significado de los diferentes campos

- **Puerto de origen**: es el número de puerto relacionado con la aplicación del remitente del segmento UDP. Este campo representa una dirección de respuesta para el destinatario. Por lo tanto, este campo es opcional. Esto significa que si el puerto de origen no está especificado, los 16 bits de este campo se pondrán en cero. En este caso, el destinatario no podrá responder (lo cual no es estrictamente necesario, en particular para mensajes unidireccionales).

- **Puerto de destino**: este campo contiene el puerto correspondiente a la aplicación del equipo receptor al que se envía.

- **Longitud**: este campo especifica la longitud total del segmento, con el encabezado incluido. Sin embargo, el encabezado tiene una longitud de 4 x 16 bits (que es 8 x 8 bits), por lo tanto la longitud del campo es necesariamente superior o igual a 8 bytes.

- **Suma de comprobación**: es una suma de comprobación realizada de manera tal que permita controlar la integridad del segmento.

GRE

El **GRE** (Generic Routing Encapsulation) es un protocolo para el establecimiento de túneles a través de Internet.

Características

- Permite emplear protocolos de encaminamiento especializados que obtengan el camino óptimo entre los extremos de la comunicación.
- Soporta la secuencialidad de paquetes y la creación de túneles sobre redes de alta velocidad.
- Permite establecer políticas de encaminamiento y seguridad.

Router

Ruteador o encaminador es un dispositivo de hardware para interconexión de red de ordenadores que opera en la capa tres (nivel de red). Este dispositivo permite asegurar el enrutamiento de paquetes entre redes o determinar la ruta que debe tomar el paquete de datos. Asegurándose de esta manera que la información no va a donde no es necesario. El router unira las redes del emisor y el destinatario de una información determinada, transmitiendo solo la información necesaria.

Fig. Nº 6.6.2 Router

Firewall

Un **firewall** es un sistema que protege a un ordenador o a una red de ordenadores contra intrusiones provenientes de redes de terceros (generalmente desde internet). Un sistema de firewall filtra paquetes de datos que se intercambian a través de internet. Por lo tanto, se trata de una pasarela de filtrado que comprende al menos las siguientes interfaces de red:

- una interfaz para la red protegida (red interna)
- una interfaz para la red externa.

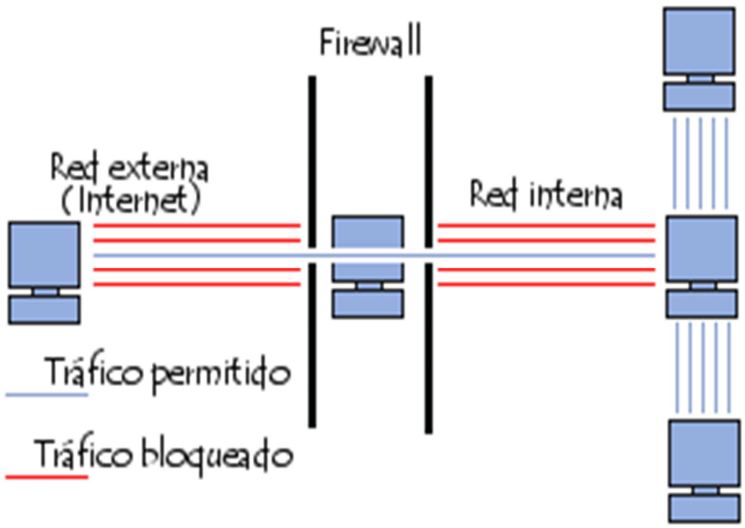


Fig. Nº 6.6.3 Sistema Firewall

El sistema firewall es un sistema de software, a menudo sustentado por un hardware de red dedicada, que actúa como intermediario entre la red local (u ordenador local) y una o más redes externas. Un sistema de firewall puede instalarse en ordenadores que utilicen cualquier sistema siempre y cuando:

- La máquina tenga capacidad suficiente como para procesar el tráfico
- El sistema sea seguro
- No se ejecute ningún otro servicio más que el servicio de filtrado de paquetes en el servidor

Cómo funciona un sistema Firewall

Un sistema firewall contiene un conjunto de reglas predeterminadas que le permiten al sistema:

- Autorizar la conexión (*permitir*)
- Bloquear la conexión (*denegar*)
- Rechazar el pedido de conexión sin informar al que lo envió (*negar*)

Todas estas reglas implementan un método de filtrado que depende de la **política de seguridad** adoptada por la organización. Las políticas de seguridad se dividen generalmente en dos tipos que permiten:

- la autorización de sólo aquellas comunicaciones que se autorizaron explícitamente:

  "Todo lo que no se ha autorizado explícitamente está prohibido"

- el rechazo de intercambios que fueron prohibidos explícitamente

El primer método es sin duda el más seguro. Sin embargo, impone una definición precisa y restrictiva de las necesidades de comunicación.

6.7. Modelo operativo

Configuración básica de una VPN en Windows XP Profesional

Explicaremos el procedimiento para configurar una VPN en Windows XP, tanto en modo cliente como en modo servidor.

Básicamente consiste en realizar una conexión a una red externa creando un túnel a través de internet, permitiendo la creación de una red privada dentro de una red pública.

La VPN utiliza el Protocolo de túnel punto a punto (PPTP, Point-to-Point Tunneling Protocol) o el Protocolo de túnel de nivel dos (L2TP, Layer Two Tunneling Protocol), mediante los cuales se puede tener acceso de forma segura a los recursos de una red al conectar con un servidor de acceso remoto a través de Internet u otra red. El uso de redes privadas y públicas para crear una conexión de red se denomina red privada virtual, Virtual Private Network

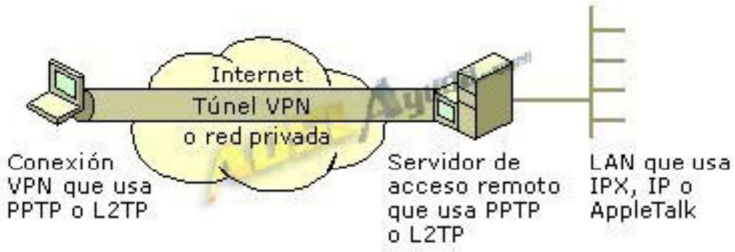


Fig. Nº 6.7.1 Túnel VPN

Un usuario que ya está conectado a Internet utiliza una conexión VPN para marcar el número del servidor de acceso remoto. Entre los ejemplos de este tipo de usuarios se incluyen las personas cuyos equipos están conectados a una red de área local, los usuarios de cables de conexión directa o los suscriptores de servicios como ADSL, en los que la conectividad IP se establece inmediatamente después de que el usuario

inicie el equipo. El controlador PPTP o L2TP establece un túnel a través de Internet y conecta con el servidor de acceso remoto habilitado para PPTP o L2TP. Después de la autenticación, el usuario puede tener acceso a la red corporativa con total funcionalidad.

El procedimiento para la configuración constaría de 3 pasos.

- Configuración del servidor VPN
- Configuración del cliente VPN
- Gestión de puertos o configuración del software de seguridad.

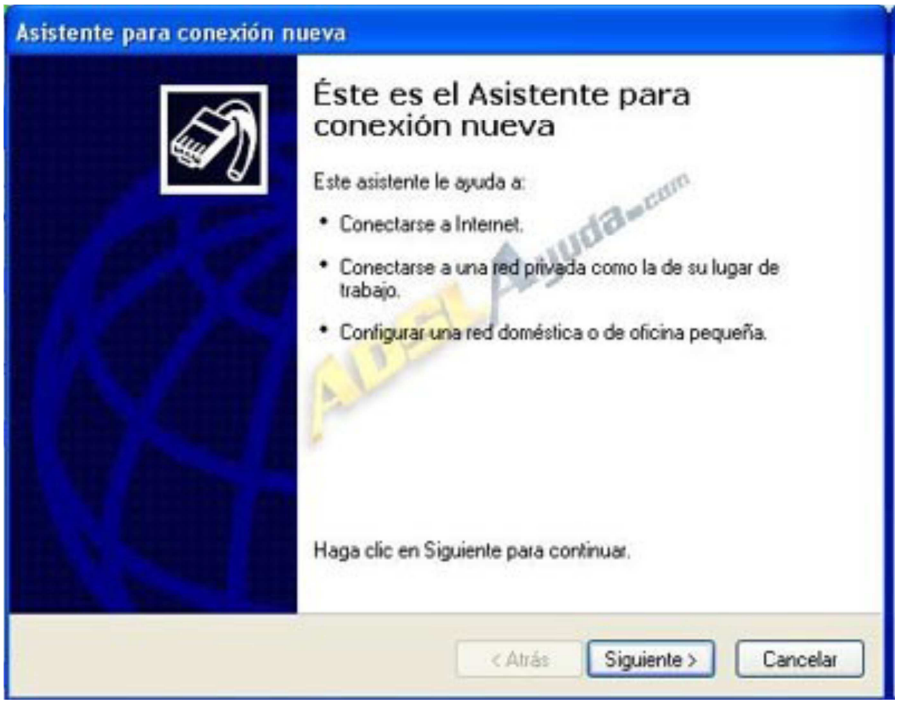
Configuración del Servidor

El procedimiento sería el siguiente:

1. Iremos a **Inicio**
2. **Mis sitios de red**

Dentro de Mis sitios de red, seleccionamos **Ver conexiones de red**, y a continuación, **Crear una conexión nueva**.

Se abrirá el asistente para conexión nueva e iremos siguiendo las indicaciones, pulsamos en **Siguiente**:



Seleccionamos la opción **Configurar una conexión avanzada** y pulsamos en **Siguiente**, para después elegir la opción **Aceptar conexiones entrantes**.

En esta pantalla que aparece a continuación, **Dispositivos de conexiones entrantes**, no debemos marcar ninguno y pulsar directamente en el botón **Siguiente**.

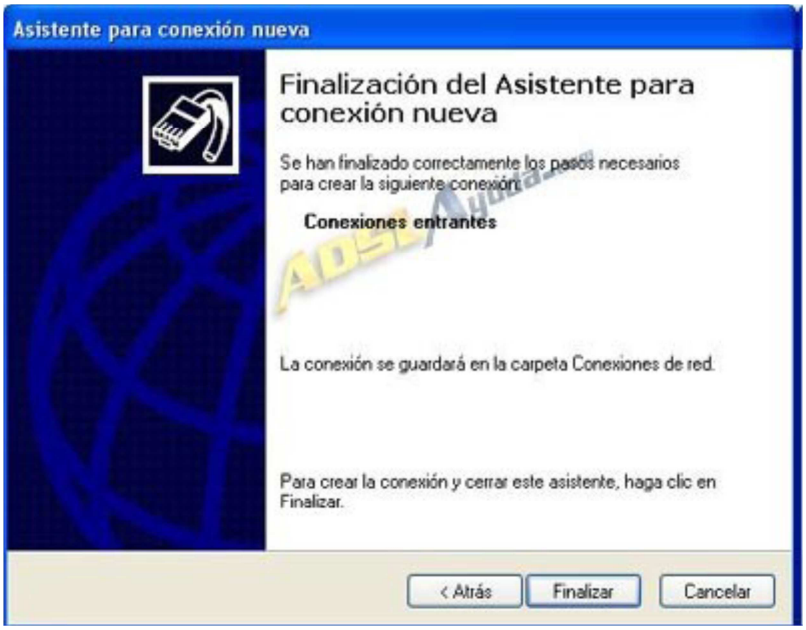
Al hacerlo de este modo, aparecerá la pantalla para empezar a definir **Conexión de red privada virtual (VPN) entrante**. La verdad es que no es fácil llegar hasta aquí. Volvemos a pulsar **Siguiente**.

Debemos ahora definir un usuario que tenga permisos de acceso a través de la VPN. Podemos elegir uno de los que ya tenemos configurado en el PC o bien crear otro exclusivo.

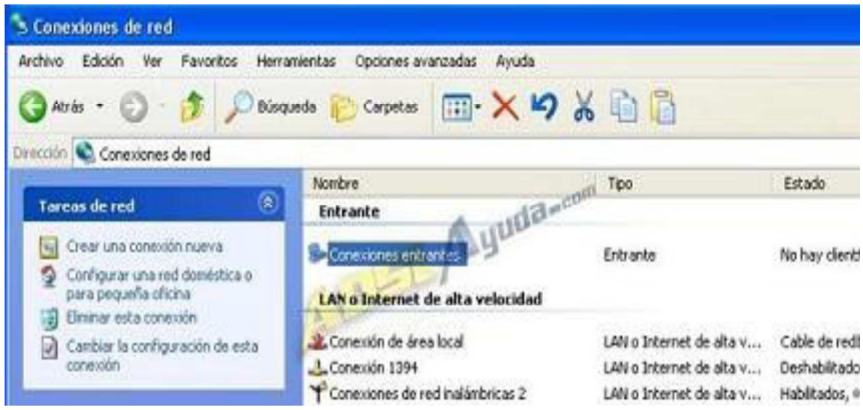
Al crear uno nuevo (pulsar el botón **Agregar...**), nos pedirá que introduzcamos un nombre de usuario y le proporcionemos una contraseña. Esta contraseña será la que posteriormente nos solicite al realizar la conexión remota.

Una vez creado el usuario nuevo, lo seleccionamos para permitirle la conexión, pulsamos en **Siguiente** y pasamos a otra pantalla en la que nos muestra los protocolos que usará la conexión para permitir el acceso al cliente remoto. Lo dejamos como está y pulsamos en **Siguiente** para finalizar esta parte del proceso.

Con esto habremos creado la conexión nueva y habremos creado también un usuario con acceso a la VPN. Pulsamos en **Finalizar**.



Ahora volvemos a Conexiones de red para verificar que se ha creado la conexión. Aparecerá una nueva llamada **Conexiones entrantes**.



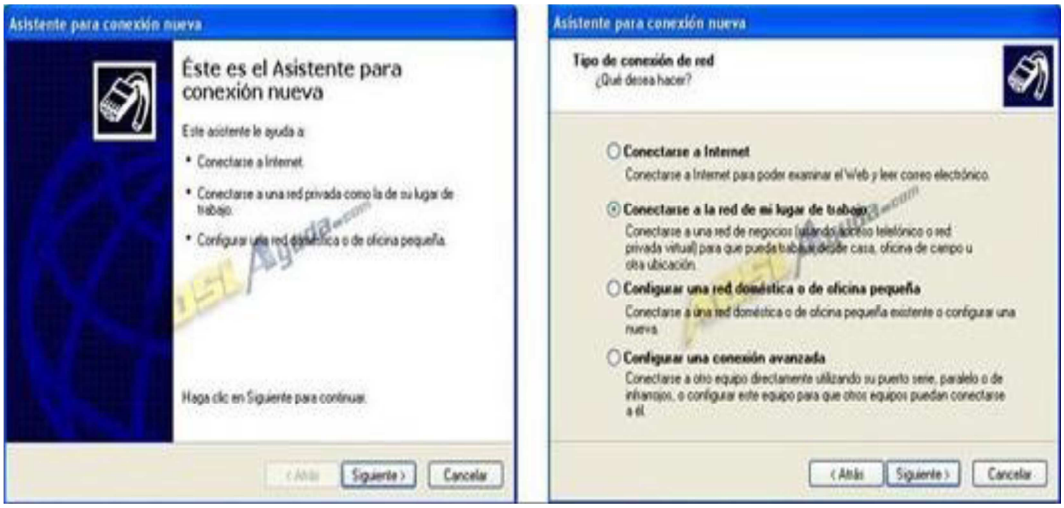
Configuración del Cliente

Una vez que tengamos configurado el servidor de VPN en, por ejemplo, la oficina, debemos configurar el cliente en el lugar desde donde queramos acceder. Para ello debemos crear en el PC del sitio remoto una nueva conexión de red.

Vamos a:

1. **Mis sitios de red**
2. **Ver conexiones de red**
3. Elegimos la opción **Crear una conexión nueva**.

Volverá a abrirse el Asistente para nuevas conexiones. Pulsamos en **Siguiente**. Ahora elegimos **Conectarse a la red de mi lugar de trabajo**.

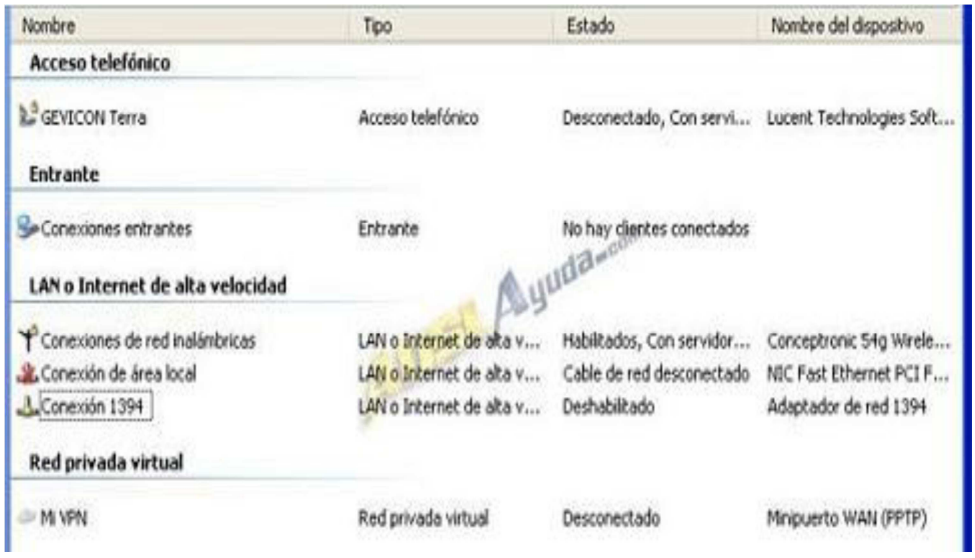


Dentro de las 2 opciones que aparecen, elegimos **Conexión de red privada virtual** y en la pantalla siguiente especificamos un nombre para que la identifique dentro de las conexiones de red que tengamos definidas. Pulsamos en **Siguiente**.

En el siguiente paso nos pedirá que introduzcamos el nombre de host o la dirección IP del servidor remoto. Que será la dirección del servidor que configuramos en la primera parte. Pulsamos en **Siguiente** y en **Finalizar**.

La nueva conexión aparecerá ahora en **Conexiones de Red**, dentro del un nuevo grupo que se llama **Red privada virtual**. Para establecer la conexión, pulsamos 2 veces sobre ella con el botón izquierdo del ratón

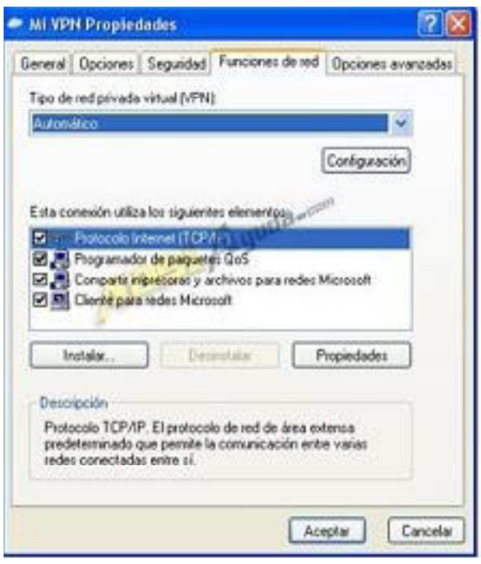
.



Se abrirá el diálogo de conexión, introduciremos nombre de usuario y contraseña.

Antes de realizar la primera conexión hay que hacer un pequeño ajuste en la configuración para que se pueda seguir navegando con normalidad mientras estemos conectados a la VPN. Para ello pulsamos en **Propiedades**.

En la pestaña **Funciones de red**, seleccionamos el **Protocolo Internet (TCP/IP)** y pulsamos de nuevo en **Propiedades**.



Ahora vamos al apartado **Opciones avanzadas** y llegaremos a otra pantalla. Ahí debemos quitar la marca de la casilla **Usar la puerta de enlace predeterminada en la red remota**.

Gestión de puertos o configuración del Software de seguridad.

Para establecer la comunicación VPN necesitamos que el ordenador servidor sea accesible por los puertos **1723 TCP** y el protocolo **GRE** (o en su defecto el puerto **47 UDP**).

Por tanto debemos configurar tanto el router como los servidores de seguridad o firewall que podamos tener instalados en el servidor para permitirlo. Una vez configurados debería ser posible la conexión al equipo remoto. Al menos este equipo debería ser accesible.

Se pretende describir cómo se configura la comunicación entre el PC cliente de la VPN y la red remota a través del servidor de VPN.
Supongamos que la red a la que queremos acceder (parte del servidor) trabaja en el rango de IPs 10.0.0.xxx. y que el PC servidor tiene en su red local la dirección IP 10.0.0.90. Esta dirección debe establecerse como estática para realizar los mapeos de los puertos y protocolos correspondientes en el router.

Ejemplo de una posible red del servidor:

Router: 10.0.0.1

PC servidor de VPN: 10.0.0.90.

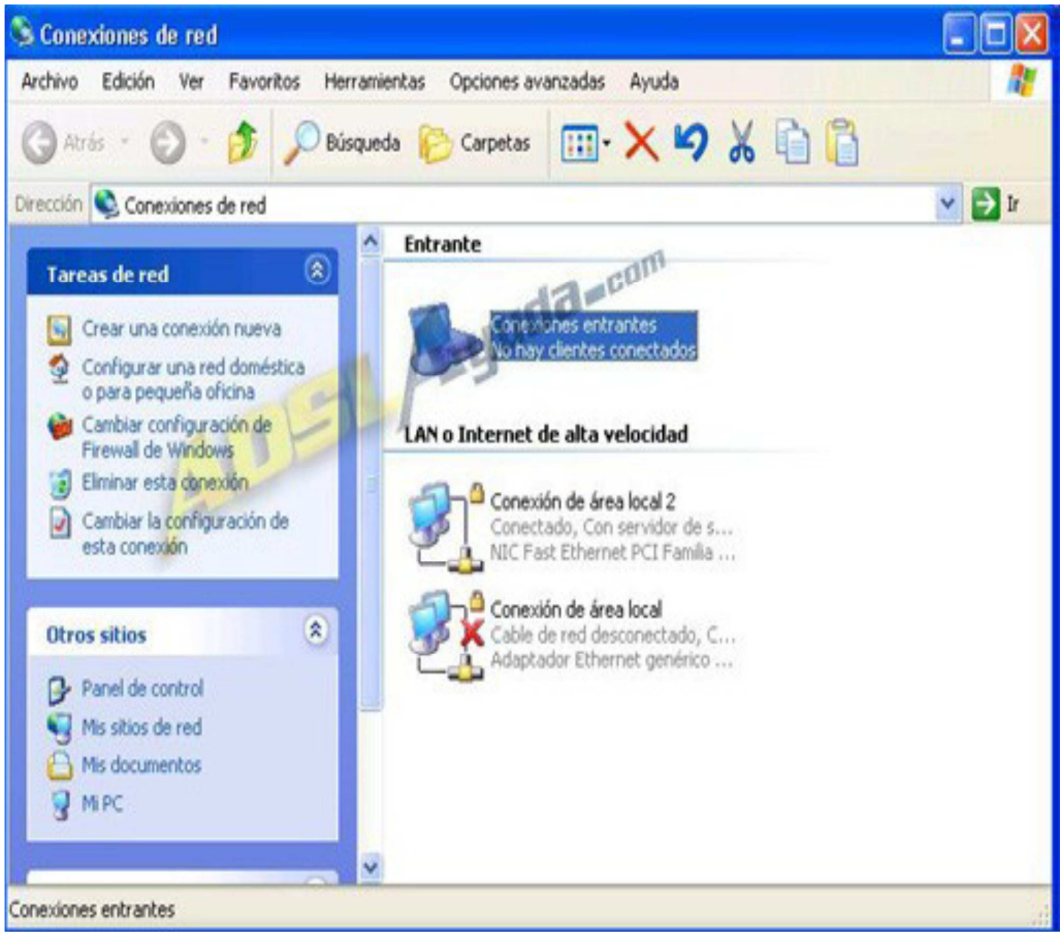
El router asigna direcciones dinámicas a los ordenadores de la red a partir de 10.0.0.100. Hay aparatos como impresoras de red o puntos de acceso inalámbricos configurados en direcciones estáticas de la 10.0.0.40 a la 10.0.0.45.

La finalidad es dar acceso al PC remoto a todos los elementos de esa red local.

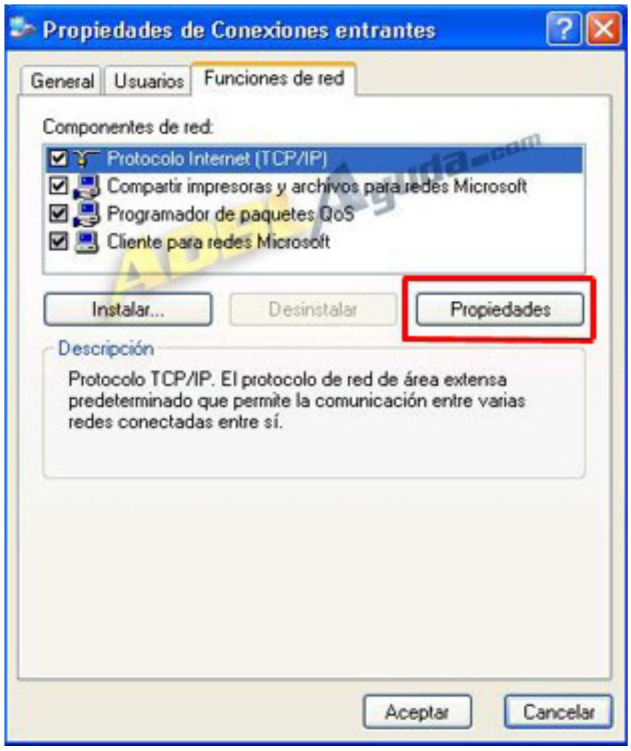
Configuración adicional del Servidor:

Iremos a:

1. **Mis sitios de red**
2. **Ver conexiones de red.**



En la conexión entrante correspondiente a la VPN haremos click con el botón derecho y abriremos el diálogo **Propiedades**.



Iremos a la pestaña **Funciones de red** y, habiendo seleccionado el **Protocolo Internet (TCP/IP)**, pulsaremos el botón **Propiedades**.

Marcaremos la casilla **Permitir a quienes llaman tener acceso a mi red de área local**. En el recuadro "Asignación de direcciones TCP/IP", seleccionaremos la opción **Especificar direcciones TCP/IP**.

En el recuadro **De:** introduciremos una dirección IP que no coincida con ninguna existente en nuestra red local, procurando que quede fuera también del rango de asignación por DHCP del router. Esta dirección IP será la que tenga el servidor VPN con respecto al cliente cuando se conecte.

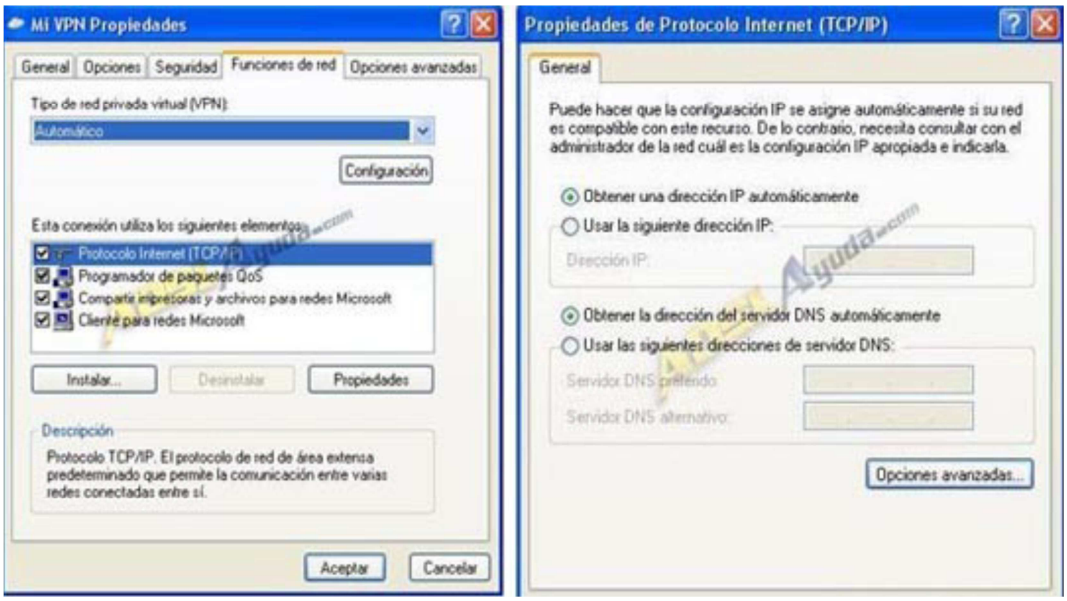
En el recuadro **Para:** pondremos una cercana a la primera ya que Windows XP sólo permite un cliente VPN conectado simultáneamente. La IP del ordenador cliente va a estar dentro de ese intervalo.
Pulsamos en **Aceptar** y terminamos de esta manera la configuración del servidor.

Configuración del cliente de VPN.

Vamos a comprobar que nuestro ordenador cliente está configurado para recibir la dirección IP del servidor.

Abriremos la conexión que tenemos creada.

Pulsaremos el botón **Propiedades** y en el diálogo que se abrirá seleccionaremos la pestaña **Funciones de red**.

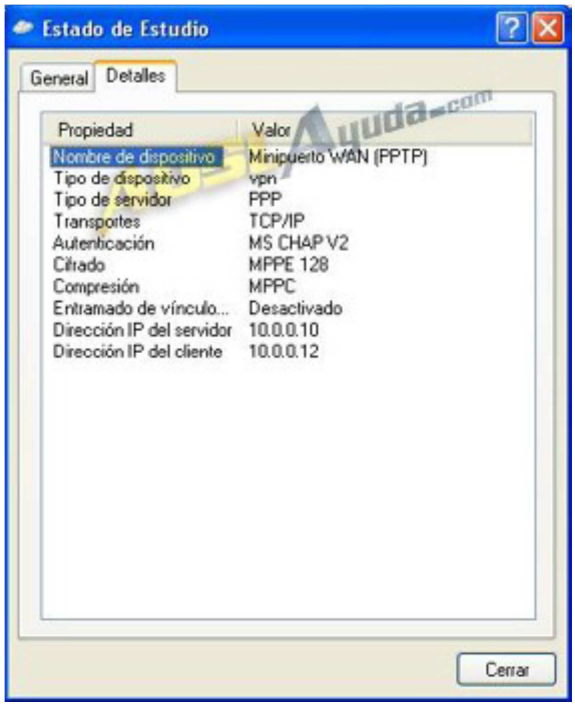


Con el **Protocolo Internet (TC/IP)** seleccionado pulsaremos en el botón **Propiedades** para comprobar que está seleccionada la opción **Obtener una dirección IP automáticamente**.

Ahora tendremos todo preparado para que el ordenador forme parte como uno más de la red remota. Iniciamos la conexión.

Nos aparecerá en la parte inferior derecha un nuevo icono que indica la conexión a la VPN.

Pulsamos con el botón derecho sobre el icono y se abrirá el diálogo de **Estado** de la conexión.



Efectivamente comprobamos que la dirección IP del servidor es 10.0.0.10 y la de nuestro PC cliente es 10.0.0.12. Estamos dentro de la red remota y todos los ordenadores, dispositivos e incluso el router serán accesibles.

Aunque hay que hacer una precisión importante. Los equipos remotos no serán accesibles mediante sus nombres, ya que Windows XP no actúa como servidor para traducir los nombres de los equipos en direcciones de red. Únicamente serán accesibles por IP.

Para ello introduciremos en **Inicio -> Ejecutar** la IP de cada equipo del siguiente modo: **\\Dirección_ IP**. Por ejemplo, para acceder a los recursos compartidos del servidor pondremos \\10.0.0.10.

6.8 Administración

Para la administración de esta red se debe tomar en cuenta algunos objetivos que nos permitan 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.

Para la administración de esta red se debe tener en cuenta 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.

6.9. Previsión de la evaluación

La seguridad informática, hoy en día es parte esencial en los procesos diarios que se generan en un computadora: navegación en Internet, recibir y enviar correo electrónico, operaciones bancarias y administrativas. Por tal motivo es conveniente contar con aplicaciones o herramientas adicionales para la protección de nuestro equipo de cómputo todo con el fin de proteger lo más valioso: **nuestra información.**

Por lo general un 65% de los ataques son realizados mediante el descuido en la seguridad en las computadoras o redes de computadoras, lo que puede provocar: ataques de virus, hackers o el pishing mejor conocido como “la pesca de información” El 35% restante puede venir desde la misma red o intranet ocasionada por lo usuarios y el mal uso de los recursos de Internet tales como: música en línea, paginas con contenido pornográfico, descargas de software malicioso, uso del correo electrónico interno lo que provoca un porcentaje elevado de generación de spam o “correo basura”.

Dichas perdidas de dinero, recursos y materiales pueden ser prevenidos con el uso de equipos de seguridad sofisticados como: Antivirus Perimetrales, Antispam, AntiHackers, Filtrado de Paginas Maliciosas,

Firewall o Bloqueo de Intrusos así como mantener un monitoreo constante en todos los sucesos de la red.

Existen diferentes productos que han sido diseñados para ofrecer las soluciones multifunción contra amenazas más escalables, con mayor rendimiento, fiables y asequibles, que están disponibles para su implementación en empresas, ofreciendo de esta manera una plataforma de seguridad y de conectividad altamente redundante diseñado específicamente para implementaciones de redes internas y externas de alta velocidad y de redes privadas virtuales (VPN), a la vez que proporciona una amplia flexibilidad para implementaciones en línea, en sedes centrales, en redes distribuidas y en campus.

Integrar un antivirus, antispyware y algunas funciones de prevención de intrusiones en pasarela y en tiempo real permitiría que las redes y las VPN sean seguras frente a una extensa gama de amenazas dinámicas.
El cortafuegos de aplicación dota a los administradores de redes de las herramientas para el control de acceso a nivel de aplicación, la prevención contra filtrados de datos y el control del ancho de banda a nivel de aplicación.

Bibliografía:

- http://tecnologicodominicano.blogspot.com/2006/11/tutorial-administracion-de-redes.html
- http://www.emagister.com/manual/manual-administracion-redes-tematica-561.htm
- http://www.tutorial-enlace.net/listado-largo-de-tutoriales-Administracion%20de%20redes.html
- http://www.mundomanuales.com/redes-y-servidores/varios/introduccion-a-la-administracion-de-redes-136.html
- http://tutorialesvenezuela.com/web/manual-de-administracion-de-redes
- http://www.dric.com.mx/opmanager/administraci-n-de-redes-wan.html
- http://es.tldp.org/Manuales-LuCAS/IAR/intro-admon-redes-v1.1.html
- http://www.tutorialesenlared.com/manual5559.html
- http://www.rediris.es/difusion/publicaciones/boletin/35/enfoque2.html
- http://www.datacyl.com/seguridad.php
- http://www.monografias.com/trabajos10/auap/auap.shtml
- http://www.monografias.com/trabajos/seguinfo/seguinfo.shtml
- http://www.monografias.com/trabajos16/seguridad-informatica/seguridad-informatica.shtml
- http://www.seguridadenlared.org/es/index25esp.html
- http://www.emagister.com/manual/seguridad-redes-sistemas-tps-2486092.htm
- http://www.cisco.com/web/ES/about/press/2008/cisco-noticias-08-04-17.html
- http://www.advanzer.com/index.php?option=com_content&task=view&id=58&Itemid=82

- http://es.wikipedia.org/wiki/Red_de_computadoras
- http://revista-redes.rediris.es/webredes/
- http://www.solociencia.com/informatica/computador-historia-redes-concepto-internet.htm
- http://www.mastermagazine.info/termino/6496.php
- http://www.monografias.com/trabajos40/redes-informaticas/redes-informaticas.shtml
- http://www.gobiernodecanarias.org/educacion/conocernos_mejor/paginas/redes.htm
- http://www.bricopage.com/como_se_hace/informatica/redes.htm
- http://es.wikibooks.org/wiki/Redes_inform%C3%A1ticas
- http://antivirus.interbusca.com/glosario/RED.html
- http://www.masadelante.com/faq-lan.htm
- http://www.angelfire.com/mi2/Redes/componentes.html
- http://teleenfermeria.iespana.es/teleenfermeria/componentes_de_red.htm
- http://tutoriales.igluppiweb.com.ar/tutorial_redes/html/Componentes%20de%20la%20red.htm
- http://www.ordenadores-y-portatiles.com/lan.html
- http://www.mitecnologico.com/Main/ComponentesDeUnaRed
- http://www.angelfire.com/mi2/Redes/ventajas.html
- http://es.kioskea.net/contents/initiation/concept.php3
- http://es.wikibooks.org/wiki/Imagen:Osi.png
- http://www.monografias.com/trabajos40/redes-informaticas/redes-informaticas2.shtml
- http://www.iec.csic.es/CRIPTonOMICon/seguridad/mecanism.html
- http://www.seguridaddigital.info/index.php?option=com_content&task=view&id=83&Itemid=26
- http://www3.uji.es/~mmarques/f47/apun/node98.html
- http://www.monografias.com/trabajos/seguinfo/seguinfo.shtml

Anexos

Firewall

Especificaciones:

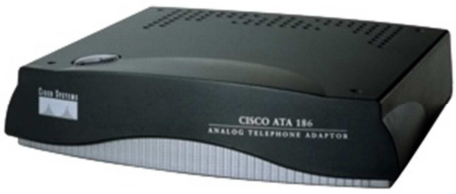
Descripción del producto	D-Link NetDefend DFL-210 - aparato de seguridad
Tipo de dispositivo	Aparato de seguridad
Protocolo de interconexión de datos	Ethernet, Fast Ethernet
Red / Protocolo de transporte	PPTP, L2TP, PPPoE
Protocolo de gestión remota	SNMP 1, SNMP 2c, HTTP, HTTPS
Características	Protección firewall, puerto DMZ, soporte de DHCP, soporte de NAT, asistencia técnica VPN, soporte para PAT, equilibrio de carga, soporte VLAN, snooping IGMP, soporte para Syslog, Stateful Packet Inspection (SPI), filtrado de contenido, soporte ALG, Intrusion Detection System (IDS), actualizable por firmware

Gateway

Especificaciones:

Descripción del producto	Linksys Wireless-N ADSL2+ Gateway WAG160N - enrutador inalámbrico
Tipo de dispositivo	Enrutador inalámbrico + conmutador de 4 puertos (integrado)
Protocolo de direccionamiento	RIP-1, RIP-2, direccionamiento IP estático
Protocolo de interconexión de datos	Ethernet, Fast Ethernet, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n (draft 2.0)
Red / Protocolo de transporte	PPTP, L2TP, IPSec, PPPoE, PPPoA
Protocolo de señalización digital	ADSL Lite, ADSL, ADSL2, ADSL2+, ADSL2+M
Características	Soporte de NAT, señal ascendente automática (MDI/MDI-X automático), Stateful Packet Inspection (SPI), prevención contra ataque de DoS (denegación de servicio), filtrado de dirección MAC, pasarela VPN, filtrado de direcciones IP, cifrado de 256 bits, tecnologÃa MIMO, Wi-Fi Protected Setup (WPS), Servidor DHCP

Modem



Especificaciones:

Descripción del producto	Cisco ATA 186 - adaptador para teléfono VoIP
Tipo de dispositivo	Adaptador para teléfono VoIP
Protocolo de direccionamiento	RIP-1, RIP-2, direccionamiento IP estático
Protocolo de interconexión de datos	Ethernet
Red / Protocolo de transporte	TCP/IP
Protocolo de gestión remota	HTTP
Protocolos VoIP	MGCP, SCCP, SIP
Características	Soporte de DHCP

Adaptador de Red

Especificaciones:

Descripción del producto	Cisco Aironet 802.11a/b/g Wireless PCI Adapter - adaptador de red
Tipo de dispositivo	Adaptador de red
Factor de forma	Tarjeta de inserción
Tipo de interfaz (bus)	PCI
Protocolo de interconexión de datos	IEEE 802.11b, IEEE 802.11a, IEEE 802.11g
Velocidad de transferencia de datos	54 Mbps

Punto de acceso inalámbrico

Especificaciones:

Descripción del producto	Cisco Aironet 1231 - punto de acceso inalámbrico
Tipo de dispositivo	Punto de acceso inalámbrico
Tipo incluido	Externo
Procesador	1 x IBM PowerPC 405 200 MHz
RAM instalada (máx.)	16 MB
Protocolo de gestión remota	SNMP, Telnet, HTTP
Características	Auto-sensor por dispositivo, soporte de DHCP, soporte BOOTP, soporte ARP, soporte VLAN, activable

Router inalámbrico

Especificaciones:

Descripción del producto	Cisco 876W Integrated Services Router - enrutador inalámbrico
Tipo de dispositivo	Enrutador inalámbrico + conmutador de 4 puertos (integrado)
Factor de forma	Externo
Memoria RAM	128 MB (instalados) / 256 MB (máx.)
Velocidad de transferencia de datos	54 Mbps
Banda de frecuencia	2.4 GHz
Protocolo de direccionamiento	RIP-1, RIP-2
Protocolo de interconexión de datos	Ethernet, Fast Ethernet, IEEE 802.11b, IEEE 802.11g
Red / Protocolo de transporte	PPTP, L2TP, IPSec, PPPoE, PPPoA
Protocolo de gestión remota	SNMP, Telnet, HTTP
Protocolo de señalización digital	ADSL over ISDN
Características	Protección firewall, soporte de DHCP, asistencia técnica VPN, soporte VLAN, señal ascendente automática (MDI/MDI-X automático), activable, soporte IPv6, Sistema de prevención de intrusiones (IPS)