

Mantenimiento de equipo de cómputo e instalación de redes



Cuarto Semestre

GOBIERNO DEL ESTADO DE GUANAJUATO

Lic. Diego Sinhue Rodríguez Vallejo
Gobernador del Estado de Guanajuato

Mtro. Jorge Enrique Hernández
Secretario de Educación de Guanajuato

SISTEMA AVANZADO DE BACHILLERATO Y EDUCACIÓN SUPERIOR

Mtro. Alberto de la Luz Socorro Diosdado
Dirección General SABES

Mtra. Georgina Calderón Sierra
Dirección Académica

ELABORÓ

ONTIVEROS GUERRERO ERIC
RIVERA REYES MIREYA
SALAS VÁZQUEZ JUAN ANTONIO
VALTIERRA FRANCO GERARDO

REVISIÓN INTERNA

Juan Roberto Prado Reynoso

COLABORACIÓN

Diseño de Portada
Dirección de Vinculación
Supervisión y Coordinación
Dirección Académica

Taller de Capacitación para el Trabajo: Diseñador de Procesos Digitales

Semestre: 4º

Prohibida la reproducción o transmisión, total o parcial de esta obra mediante cualquier medio o sistema electrónico o mecánico, incluyendo el fotocopiado, la grabación o cualquier sistema de recuperación y almacenamiento de información, sin autorización escrita del SABES.

Derechos Reservados en Trámite
© 2014

Primera Edición: 2018

Redes de Equipo de Cómputo

QUINTO SEMESTRE – Redes de Equipo de Cómputo

TEMA 01: INTERNET.	8
1.1 ¿Qué es el internet?	
1.2 ¿Cómo funciona el internet?	
1.3 Navegadores y aplicaciones de internet	
1.4 Configuración de los navegadores de internet	
TEMA 02: ACCESOS Y PERMISOS.	14
2.1 Cuentas de usuario	
2.2 Uso de cuentas de administrador y usuario limitado	
2.3 Configuración de una cuenta de usuario limitado	
2.4 Cambio de usuario	
2.5 Generar cuentas de usuario	
TEMA 03: REDES: DEFINICIÓN, USOS, TIPOS Y COMPONENTES.	19
3.1 ¿Qué es una red?	
3.2 Tipos de redes	
3.3 Protocolos de red	
3.4 Componentes de una red	
3.5 Topología de red	
TEMA 04: ARMADO DE CABLE DE RED.	47
4.1 Tipos de cable de red	
4.2 Protocolos de cable de red	
4.3 Armado de un cable de red	
TEMA 05: ESTRUCTURADO DE UNA RED.	57
5.1 Topología de una red de área local (LAN)	
5.2 Cableado e instalación de equipos en la red	
5.3 Configuración lógica de la red (Protocolos y Direcciones IP)	
5.4 Pruebas de comunicación (IPConfig, Ping, etc.)	
TEMA 06: RECURSOS COMPARTIDOS.	77
6.1 Archivos y carpetas compartidas	
6.2 Niveles de acceso en archivos y carpetas compartidas	
TEMA 07: PERIFÉRICOS COMPARTIDOS.	90
7.1 Recursos y periféricos compartidos	
7.2 Impresoras compartidas en Windows 7 y Windows XP	
TEMA 08: REDES INALÁMBRICAS.	98
8.1 Rede inalámbricas Wireless (WI-FI)	
8.2 ¿Cómo conectarse a una red inalámbrica?	
Glosario	122

PRESENTACIÓN DEL TALLER DE SOPORTE Y MANTENIMIENTO DE EQUIPO DE CÓMPUTO

Saludos a todos, bienvenidos a la segunda parte de su capacitación para el trabajo, ahora iniciamos con una nueva experiencia dentro de tu formación en el bachillerato, en esta parte de la capacitación tendrás la oportunidad de aplicar de forma práctica mucho de lo que has aprendido en el semestre anterior, además durante el desarrollo del trabajo con tu asesor de capacitación, seguirás desarrollando habilidades, principalmente las relacionadas con el saber hacer.

En lo que se refiere al programa de capacitación, este al igual que el anterior se ha estructurado a partir de la experiencia y vivencias de un grupo de asesores de formación para el trabajo en la especialidad, en su proceso como asesor y en la evaluación y certificación de este perfil, enfocando principalmente lo que se requiere para encarar favorablemente el proceso de evaluación para acreditarse y alcanzar la certificación. En el planteamiento del curso se tiene como propósito general que seas capaz de instalar, configurar, dar mantenimiento y eventualmente reparar cualquier tipo de computadoras personales, en la primera parte que corresponde al cuarto semestre y lo relacionado con la internet y la instalación de redes en el cuarto semestre.

En la parte que corresponde a este semestre se trabajan ocho temas entre los cuales destacan los relacionados con el internet, su acceso y los permisos correspondientes, de manera que esta se convierta en una herramienta que apoye en las actividades que realices, además revisarás lo que tiene que ver con el diseño, instalación, mantenimiento e instalación de redes, las cuales son cada vez más comunes en todas partes, de manera que al terminar cuentas con las competencias necesarias para trabajar con redes, darles mantenimiento y mantenerlas en funcionamiento óptimo.

Es de suma importancia que durante el tiempo que estés en el bachillerato tomes en cuenta las competencias, las genéricas y disciplinares que deberás ir desarrollando durante todo el bachillerato y de manera muy particular las del perfil ocupacional de tu especialidad de capacitación, por lo que encontrarás al inicio de la guía tanto las competencias como los desempeños que componen el perfil ocupacional, para que hagas el esfuerzo por lograr cada uno de ellos de manera efectiva. Encontraras también como apoyo para el logro de las competencias genéricas al menos un ejercicio de comprensión lectora el cuál espero sea de tu agrado y te deje interesado en el tema, por último, pero no menos importante encontraras algunas reflexiones valorales las cuales te pido analices y proyectes a tu vida cotidiana, tratando de vivir estos y los demás valores que trabajen los profesores contigo, sin más preámbulos comencemos con la capacitación.

Esperando que el curso que ahora inicias sea muy provechoso y te ayude en el logro de tus expectativas y metas actuales o futuras, te doy una muy cordial bienvenida nuevamente.

COMPETENCIA GENERAL

El alumno será capaz de crear un ambiente favorable para el equipo de cómputo, realizando actividades de prevención en fallas eléctricas, así como de datos; prolongando la vida útil de los periféricos y del sistema; Auxiliar en el diseño e instalación de redes de área local.



TEMA Inicial

Competencias Genéricas

Las competencias genéricas son las que todos los bachilleres deben estar en capacidad de desempeñar; las que les permiten comprender el mundo e influir en él; les capacitan para continuar aprendiendo de forma autónoma a lo largo de sus vidas, y para desarrollar relaciones armónicas con quienes les rodean, así como participar eficazmente en los ámbitos social, profesional y político. Dada su importancia, dichas competencias se identifican también como competencias clave y constituyen el perfil del egresado del Sistema Nacional de Bachillerato (Acuerdo Secretarial 444 de Sistema Nacional de Bachillerato)

Competencias genéricas del MCC

Atributos de las competencias genéricas

1.6 Administra los recursos disponibles teniendo en cuenta las restricciones para el logro de sus metas.

4.1 Expresa ideas y conceptos mediante representaciones lingüísticas, matemáticas o gráficas.

5.1 Sigue instrucciones y procedimientos de manera reflexiva, comprendiendo como cada uno de sus pasos contribuye al alcance de un objetivo.

5.3 Identifica los sistemas y reglas o principios medulares que subyacen a una serie de fenómenos.

6.1 Elige las fuentes de información más relevantes para un propósito específico y discrimina entre ellas de acuerdo a su relevancia y confiabilidad.

7.3 Articula saberes de diversos campos y establece relaciones entre ellos y su vida cotidiana.

8.1 Propone maneras de solucionar un problema o desarrollar un proyecto en equipo, definiendo un curso de acción con pasos específicos.

11.1 Asume una actitud que favorece la solución de problemas ambientales en los ámbitos local, nacional e internacional.

Competencias ocupacionales

Competencia específica:

Diseña e instala redes de cómputo y periféricos de área local.

Tarea 1: Detecta el equipo requerido para la instalación de la red, elabora cable UTP según la topología indicada y elabora tablas de ruteo según el diseño de la red.

Desempeños esperados

- Detecta los componentes necesarios para la topología indicada y el número de computadoras a conectar.
- Elabora los cables necesarios comprobando que cumpla con la función de conectar periféricos.
- Evita desperdicio de material en la elaboración, en las pruebas y en los tamaños indicados.
- Realiza un adecuado manejo de las herramientas y equipo de red, evitando daños hacia el equipo y su persona.
- Se asegura que las direcciones IP no se repitieran.
- Comprueba que existan puertos de enlace necesarias en la red.

Tarea 2: Configura equipo de la red identificándolos con direcciones IP, dominios o grupos de trabajo.

Desempeños esperados

- Se asegura que las direcciones IP y nombres de los equipos correspondan a un mismo dominio o grupo de trabajo y no se repitieran.
- Utiliza los comandos del Sistema Operativo, para corroborar la conexión entre equipos.
- Comparte exclusivamente la información y recursos requeridos por los usuarios.
- Se asegura, si es necesario de introducir contraseñas en equipos.
- Utiliza las herramientas del Sistema Operativo para verificar el funcionamiento o el conflicto de dispositivos.

- Detecta posibles fallas en los dispositivos para su corrección.
- Utiliza el driver correspondiente para el dispositivo en conflicto de acuerdo al Sistema Operativo.
- Verifica la ubicación de la instalación del software en el Disco Duro (carpetas, partición o unidades de disco).
- Cuida el no saturar la pantalla principal de accesos directos durante la instalación del software.
- Verifica la necesidad del software a instalar.

Tarea 3: Verifica la conexión entre equipos y comparte información y recursos de los equipos de la red.

Desempeños esperados

- Detecta componentes necesarios para la topología indicada y el número de computadoras a conectar.
- Elabora los cables comprobando que cumpla con la función de conectar periféricos.
- Evita el desperdicio de material en la elaboración de los cables para las pruebas.
- Realiza un manejo adecuado de las herramientas y equipo de red, evitando daños hacia el equipo y su persona.
- Obtiene todos los caminos para la comunicación de subredes.
- Se asegura que las direcciones IP no se repitieran.
- Comprueba la existencia de puertas de enlace necesarias en la red.
- Se asegura que las direcciones IP y nombres de los equipos en un mismo dominio o grupo de trabajo, no se repitieran.
- Utiliza los comandos del Sistema Operativo, para corroborar la conexión entre equipos.
- Comparte exclusivamente la información y recursos requeridos por los usuarios.
- Se asegura, si es necesario de introducir contraseñas en equipos.

TEMA 01: INTERNET

- ✓ 1.1 ¿Qué es el internet?
- ✓ 1.2 ¿Cómo funciona el internet?
- ✓ 1.3 Navegadores y aplicaciones de internet.
- ✓ 1.4 Configuración de los navegadores de internet



1.1 ¿QUÉ ES EL INTERNET?

Internet es un conjunto de redes de comunicación interconectadas que utilizan protocolos, garantizando que las redes físicas que la componen funcionen como una sola red mundial.

Un protocolo es un conjunto de reglas usadas por computadoras para comunicarse unas con otras a través de una red.

Sus orígenes se remontan a 1969, cuando se estableció la primera conexión de computadoras, conocida como ARPANET, entre tres universidades en California y una en Utah, Estados Unidos.

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

Existen, por tanto, muchos otros servicios y protocolos en Internet, aparte de la Web: el envío de correo electrónico, la transmisión de archivos, las conversaciones en línea, la mensajería instantánea, la transmisión de contenido y comunicación multimedia, y los juegos en línea.



1.2 ¿COMO FUNCIONA EL INTERNET?

Uno de los aspectos más importantes de Internet es que utiliza una base tecnológica y protocolos de comunicación que son abiertos (no tiene un propietario exclusivo), permitiendo la comunicación integrada entre computadores de distintos fabricantes. Sorprendentemente Internet no tiene dueño y ha surgido gracias a la colaboración entre académicos, investigadores, usuarios y empresas de todo el mundo. Internet es una de la red más flexible del mundo de la teleinformática, dándole a las organizaciones acceso a mayor volumen de información, comunicaciones más baratas y una mayor flexibilidad que la que se puede

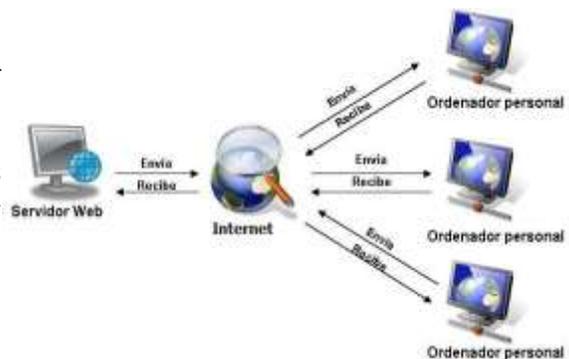
obtener utilizando líneas privadas tradicionales. El tráfico en la web ha crecido de unos cuantos centenares de miles de usuarios.

Se realiza una conexión física conectando una tarjeta adaptadora, tal como un módem o una NIC, desde un PC a una red. La conexión física se utiliza para transferir las señales entre los distintos PC dentro de la red de área local (LAN) y hacia los dispositivos remotos que se encuentran en Internet.

La conexión lógica aplica estándares denominados protocolos. El protocolo Internet (TCP/IP) es el principal conjunto de protocolos que se utiliza en Internet. Los protocolos del conjunto TCP/IP trabajan juntos para transmitir o recibir datos e información. Un navegador Web muestra el código HTML como una página Web. Ejemplos de navegadores Web incluyen Internet Explorer y Netscape. El Protocolo de transferencia de archivos (FTP) se utiliza para descargar archivos y programas de Internet. Los navegadores de Web también utilizan aplicaciones plug-in propietarias para mostrar tipos de datos especiales como, por ejemplo, películas o animaciones flash.

La computadora se conecta al Internet por medio del proveedor de servicios de Internet (ISP). Un ISP es igual que cualquier otro servicio que usted se suscribe tal como: el teléfono, la televisión por cable, la televisión, el gas, la electricidad, y el agua. Todos que quieran conectarse al Internet debe conectarse por medio de un ISP.

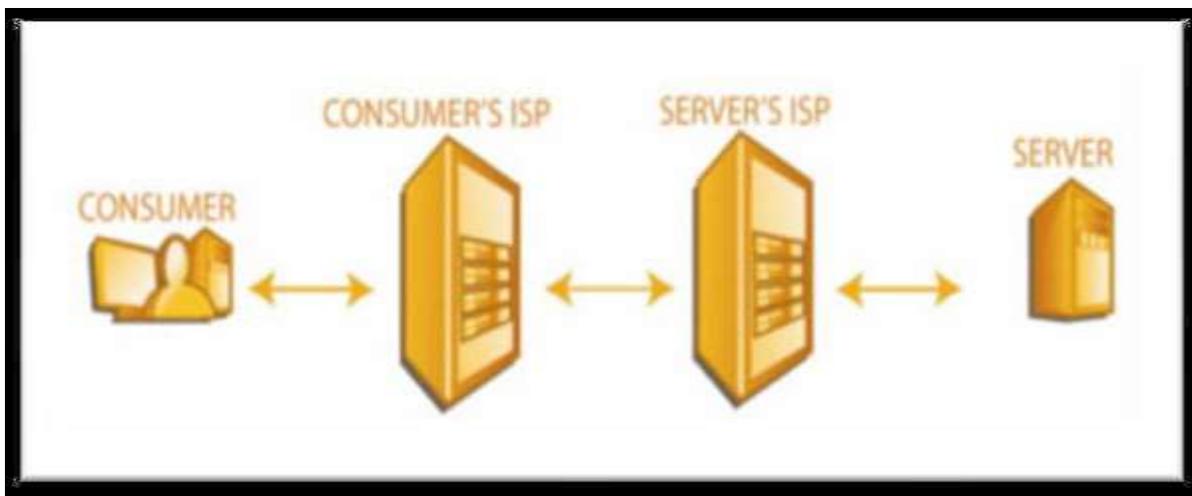
Un ISP provee a cada computadora una identidad única (dirección IP). Una dirección IP es un número único conocido por el ISP que identifica la computadora específica al Internet.



Al navegar o buscar en el Internet, su computadora solicita datos específicos que existen en otra computadora que está conectada al Internet también. Los datos pueden ser una página de la Red, un video, una descarga u otra información.

Procesos de Navegación en Internet.

1. Se inicia una solicitud (al ingresar una dirección de Red, e oprima la conexión).
2. La Dirección de La Red (o conexión) es convertido en una dirección IP.
3. Su computadora manda una solicitud al servidor ubicado en la dirección IP.
4. El servidor recibe la solicitud y responde retornando los datos.
5. Se observan los datos cargados en la computadora.



1º Paso: Iniciando una Solicitud.

Antes de poder ver algún contenido en el Internet o bajar cualquier otro contenido- debe iniciar una solicitud. Cuando teclee una dirección de Red a su navegador u oprima una conexión, está informando su computadora que solicite un documento, dato, o contenido específico localizado en algún lugar en el Internet. Una vez que su solicitud inicial sea cumplida, comenzará un proceso que abarca los cuatro pasos restantes.

2º Paso: La dirección de la Red (o conexión) es convertido en una dirección IP.

Antes que su solicitud pueda ser enviada a su localidad exacta en el Internet, debe tener la dirección IP adecuada para el servidor con los datos que ha solicitado. La dirección Red que ha incluido o la conexión que oprimió no es una dirección IP, pero es un URL (Universal Resource Locutor) que incluye un nombre dominio, cómo redes.org. Su computadora se pone en contacto con servidores especiales en el Internet llamados Servidores de nombre dominios (DNS) para ayudar convertir el Domain Name a una dirección IP. Cada servidor de DNS contiene cuadros de información que convierte un nombre dominio, tal como redes.org a una dirección IP. DNS: Son las siglas en ingles de Domain Name Server. Es el nombre del servidor que actúa como base de datos para interpretar una dirección IP de un sitio web.

3º Paso: La computadora envía una solicitud.

Ahora que su computadora tiene la dirección IP convertida, finalmente se puede enviar la solicitud. La solicitud incluye los datos que el servidor necesitará, incluyendo su dirección IP de retorno, el nombre del documento solicitado, un puerto, y otra información.

¿Qué es un Puerto? Un puerto es un punto de conexión virtual que una computadora usa para enviar y recibir transmisiones para un protocolo específico. Además, usando los puertos permite la computadora comunicarse usando varios protocolos simultáneamente.

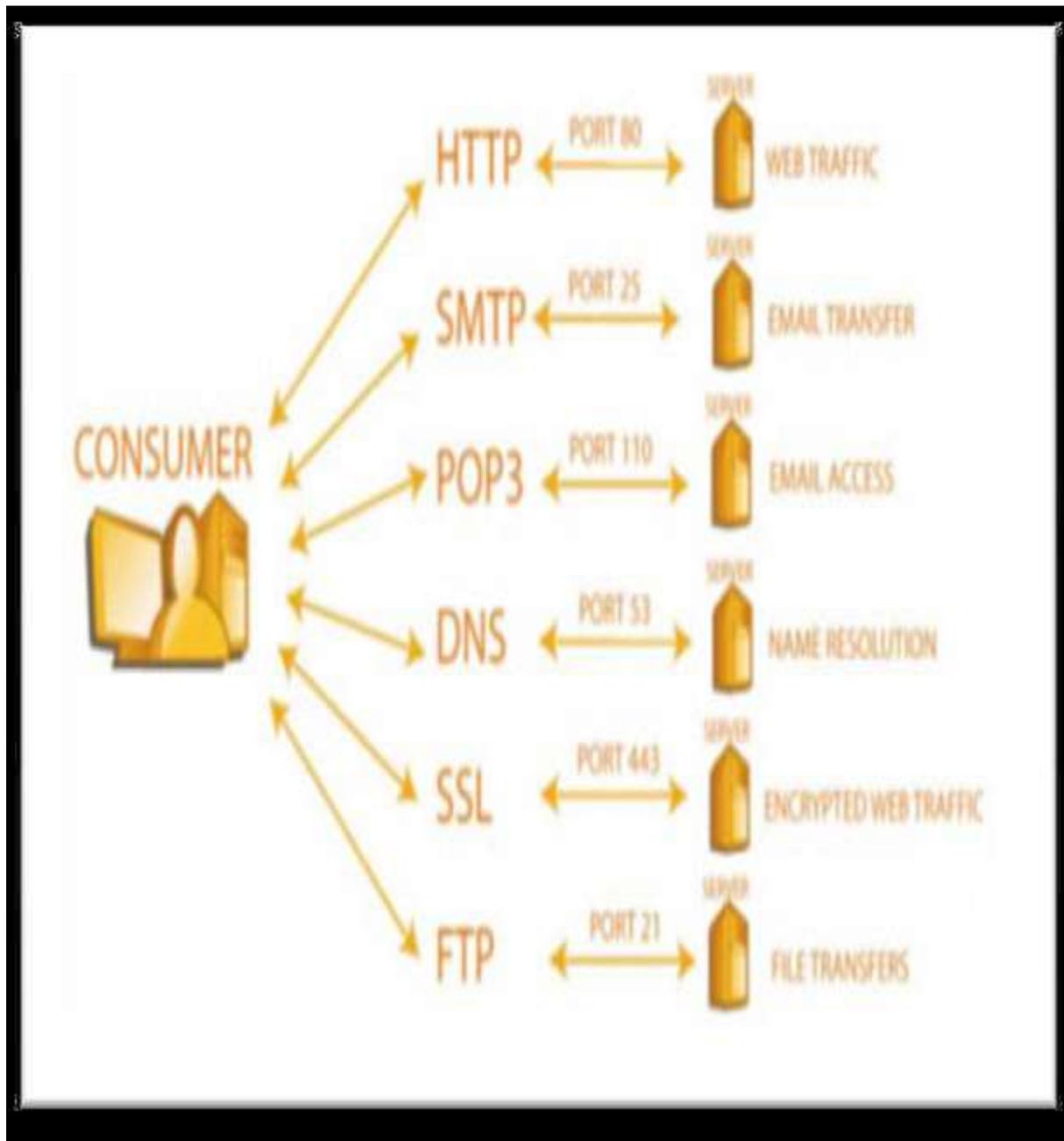
¿Cuántos Puertos existen? Piense de un puerto como un canal del Internet, parecido a un canal de televisión por cable. Hay más de 65,000 canales del Internet disponible en la Red hoy, pero únicamente un canal (puerto 80) es usado para todo el tráfico http estandarte del Internet.

¿Qué es un Protocolo de internet? Un protocolo es un lenguaje entre dos computadoras: Cliente y Servidor, intercambiando datos exitosamente. Sin un protocolo, no hay comunicación. Por ejemplo, si dos personas necesiten hablar, pero hablan diferentes idiomas, ellos serían incapaces de comunicarse. Las dos personas necesitarían hablar el mismo idioma.

Tipos de Protocolos Hoy, en el Internet hay miles de protocolos que son utilizados; sin embargo, la mayoría de individuos usan pocos solamente. Unos de los Protocolos comunes son: HTTP, SMTP, POP3, FTP, SSL, DNS, IMAP, y NEWS. El Hyper Text Transfer Protocolo (HTTP) define las reglas para comunicarse entre un navegador de red y un servidor de red. El Simple Mail Transfer Protocolo (SMTP) define las reglas para transferir mensajes de correo electrónico entre el servidor del correo a través del Internet.

El Secure Sockets Layer (SSL) define las reglas para la transferencia de datos seguros. Este protocolo ayuda proteger información personal, y es usada comúnmente con compras adquiridas en-línea.





4° Paso: El servidor recibe la solicitud y responde regresando los datos. El servidor tomará acción una vez que llegue la solicitud. Dependiendo en el puerto que se usó para hacer la solicitud, el servidor comprende cual protocolo debe usar y como formatear y enviar una respuesta. El servidor usa la dirección IP que identifica su computadora y manda una respuesta. Si la solicitud contiene los datos incorrectos, el solicitante sería mandado a una página de error o recibirá totalmente nada.

5° Paso: Se observa el contenido en su computadora. Cuando la respuesta es contestada su computadora puede presentar los datos en la manera apropiada para que usted la vea. Al

añadir una nueva dirección de red, o al oprimir una nueva conexión, el proceso entero comienza nuevamente.

1.3 NAVEGADORES Y APLICACIONES DE INTERNET.

Un navegador de Web realiza las siguientes funciones:

- Inicia el contacto con un servidor de Web.
- Solicita información.
- Recibe información.
- Muestra los resultados en pantalla.



Un navegador de Web es un software que interpreta el lenguaje de etiquetas por hipertexto (HTML), que es uno de los lenguajes que se utiliza para codificar el contenido de una página Web. Otros lenguajes de etiqueta con funciones más avanzadas son parte de la tecnología emergente. HTML el lenguaje de etiquetas más común, puede mostrar gráficos en pantalla, ejecutar sonidos, películas y otros archivos multimediales. Los hipervínculos están integrados en una página web y permiten establecer un vínculo rápido con otra ubicación en la misma página web o en una totalmente distinta.

Navegadores de Web de mayor popularidad son Safari, Mozilla Fierox, Opera e Internet Explorer. Aunque son idénticos en el tipo de tareas que realizan, existen algunas diferencias entre estos navegadores. Algunos sitios Web no admiten el uso de uno u otro y puede resultar útil tener algunos programas instalados en el computador. También existen algunos tipos de archivos especiales, o propietarios, que no se pueden visualizar con los navegadores de Web estándar. Para ver estos archivos, el navegador debe configurarse para utilizar aplicaciones

denominadas plug-in. Estas aplicaciones trabajan en conjunto con el navegador para iniciar el programa que se necesita para ver los archivos



- Flash
- QuickTime
- Java
- Shockwave
- Silverlight
- ActiveX
- DirectX

Para instalar un plug-in, siga estos pasos:

1. Vaya al sitio Web del proveedor.
2. Baje (descargue) la última versión del instalador.
3. Ejecute e instale el plug-in.
4. Verifique la instalación y la correcta operación accediendo algún sitio web que lo solicite.

1.4 CONFIGURACIÓN DE NAVEGADORES DE INTERNET.

Los navegadores presentan características similares en su funcionamiento y configuración. La elección depende de las necesidades y requerimientos del usuario:

1. Página de inicio: Cada navegador ofrece una página de inicio diferente, la cual a su vez puede ser personalizada a conveniencia del usuario, accediendo al menú herramientas / opciones de internet / página de inicio.

2. Personalización: Una característica principal es modificar el estilo y visualización del navegador, como el color, texto y barras de visualización.

3. Favoritos: Esta opción permite crear atajos de páginas web usadas frecuentemente por el usuario.

4. Seguridad: Este recurso nos permite generar el nivel de seguridad y restricciones a páginas web.

5. Actualizaciones: Esta acción se realiza cuando el navegador presenta problemas o errores al navegar por sitios web que solicitan la actualización requerida.

TEMA 02: USUARIOS

- ✓ 2.1 Cuentas de usuario
- ✓ 2.2 Uso de cuentas de administrador y usuario limitado.
- ✓ 2.3 Configuración de una cuenta de usuario limitado
- ✓ 2.4 Cambio de usuario.



2.1 CUENTAS DE USUARIO.

Es un entorno virtual dentro del mismo sistema operativo otorgado a cada usuario, que le permite tener su propio espacio privatizando su información y generar su propia configuración y personalización, dependiendo el tipo de cuenta. ¿Sabe si ahora mismo está utilizando una cuenta de usuario limitada o de administrador?

Si trabaja con una cuenta de usuario limitada, quizás pueda limitar los efectos de un virus o de cualquier otro tipo de software malintencionado. Pero si el ataque se produce mientras se utiliza una cuenta de administrador, el intruso podrá obtener un acceso sin restricciones al equipo y los resultados pueden ser desde molestos hasta catastróficos.

Elegir la cuenta adecuada en cada momento es uno de los mejores métodos para proteger un equipo. Y configurar cuentas es sencillo. Si utiliza Microsoft Windows XP, mueva el cursor sobre el reloj situado en la parte inferior derecha de la pantalla. Da clic con el botón secundario y, a continuación, Da clic en Ajustar fecha y hora.

- Si está utilizando una cuenta de usuario limitada, se mostrará un mensaje con el texto "No tiene el nivel de privilegio adecuado para cambiar la hora del sistema".
- Si utiliza una cuenta de administrador, se abrirá una ventana pequeña con controles que permiten cambiar la fecha y la hora del equipo.

2.2 USO DE CUENTAS DE ADMINISTRADOR Y USUARIO LIMITADO.

Cuenta de administrador: Es el tipo de cuenta predeterminado de Microsoft Windows XP. Esta cuenta está diseñada para que pueda:

- Configurar el equipo e instalar el software y el hardware iniciales.
- Establecer preferencias y realizar reparaciones.
- Agregar nuevos programas y componentes de hardware (por ejemplo, software para compartir música o una impresora).

Cuenta de usuario limitada: Permite el acceso a las funcionalidades de software del equipo que posibilitan el desarrollo de las actividades cotidianas. Por ejemplo, con una cuenta de usuario limitada, puede utilizar:

- Programas de acceso a Internet y de correo electrónico.
- Programas de productividad tales como Microsoft Word, Microsoft Excel y Microsoft PowerPoint.
- Programas de ocio y entretenimiento que permiten reproducir música y vídeo o editar fotografías, entre otras muchas posibilidades.

Nota: también hay disponible una cuenta de invitado, con acceso a la mayoría de las funciones propias una cuenta de usuario limitada pero que, a diferencia de ésta, no está protegida con contraseña, de modo que un invitado puede iniciar y cerrar sesión rápidamente para realizar operaciones simples, como comprobar el correo electrónico o explorar Internet.



2.3 CONFIGURACIÓN DE UNA CUENTA DE USUARIO LIMITADO.

Las cuentas de Administrador no están diseñadas para un uso ocasional: para todos los usuarios del equipo debe configurar una cuenta de usuario Limitada con la que puedan desempeñar sus actividades usuales, como procesamiento de textos o exploración Web. Si sufre un ataque por software malintencionado, el atacante puede obtener acceso al equipo por medio de la cuenta que se esté utilizando. Una cuenta de usuario limitada proporcionará al atacante un acceso parcial, mientras que, si se trata de una cuenta de administrador, le permitirá actuar como un administrador.

Tiene la posibilidad de configurar tantas cuentas de usuario limitadas como necesite para uso propio, de su familia e incluso de sus amigos.

1. Para configurar una cuenta de usuario limitada:

Asegúrese de que ha iniciado sesión como administrador.

2. Da clic en **Inicio** y, a continuación, en **Panel de control**.

3. Da clic en **Cuentas de usuario** y, a continuación, en **Elija una tarea**, Da clic en **Crear una cuenta nueva**.

4. En el menú **Acción**, Da clic en **Nuevo usuario**.

5. Escriba el nombre del usuario y Da clic en **Siguiente**.

6. En **Elija un tipo de cuenta**, Da clic en **Limitada** y, a continuación, Da clic en **Crear cuenta**.

2.4 CAMBIO DE USUARIO.

Windows XP ofrece una función denominada Cambio rápido de usuario, que le permite **pasar de un usuario a otro sin cerrar ningún programa** ni apagar el equipo.

Con la función de cambio rápido de usuario, puede cambiar a la cuenta de administrador durante un cierto tiempo si desea realizar modificaciones o tiene que **instalar nuevo software**, para después volver nuevamente a la cuenta limitada sin interrumpir ningún proceso.

El equipo debe ejecutar Windows XP, tener como mínimo una cuenta limitada configurada y no pertenecer a un dominio de red. A continuación:

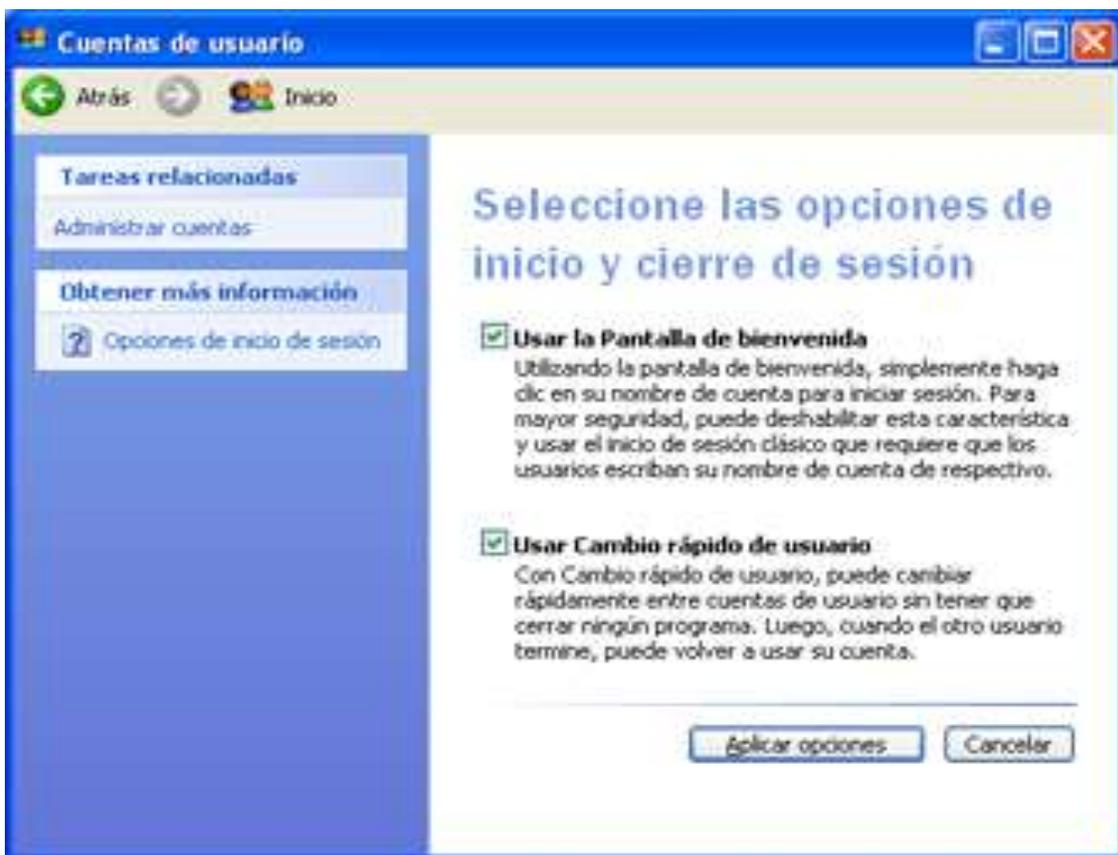
1. Da clic en **Inicio**, después en **Panel de control** y, a continuación, en **Cuentas de usuario**.

2. Da clic en **Cambiar la forma en la que los usuarios inician o cierran sesión**.

3. Active la casilla de verificación **Usar Cambio rápido de usuario**.

(Nota: es posible que necesite activar la casilla de verificación **Usar la Pantalla de bienvenida** para que se habilite **Usar Cambio rápido de usuario**.)

4. Da clic en **Aplicar opciones**.



Uso de la función de cambio rápido de usuario.

Después de la configuración, puede cambiar de cuenta de usuario con la frecuencia que desee mediante las operaciones siguientes:

1. Da clic en **Inicio** y, a continuación, en **Cerrar sesión** (o presione la **tecla Windows + L**).
2. Da clic en **Cambiar de usuario**.
3. **Da clic en la cuenta de usuario** que desea activar.

Nota: algunos juegos no se inician correctamente cuando se usa la función de cambio rápido de usuario; el juego pide que se introduzca el disco original en la unidad, aunque ya esté insertado.

2.5 GENERAR CUENTAS DE USUARIO

Para crear una cuenta de usuario.

1. Da clic en **Inicio**, **Panel de control**, y después **Cuentas de usuario**.
2. En el apartado de "Usuarios", Da clic en **Agregar**.
3. Escriba un nombre para su cuenta de usuario, su nombre completo y una descripción para su cuenta.
4. Escriba el nombre de dominio, y después **Siguiente**, si su ordenador está establecido en una red cliente/servidor. Si establece su ordenador como individual (sin una red) o en una red peer-to-peer, no necesita proporcionar un nombre de dominio.
5. Escriba una contraseña, y después escríbala de nuevo para confirmar.

En las contraseñas se toman en cuenta tanto letras mayúsculas como minúsculas. "MiClave" y "miclave" son consideradas dos contraseñas diferentes.

6. Da clic en **Siguiente**.

7. Seleccione el nivel de acceso para su cuenta de usuario, y después Da clic en **Finalizar**.



Reporte de resultados de la práctica			
Nombre de la práctica			
Competencia que a desarrollar según el programa			
La práctica la realicé de manera:	Grupal	Individual	Fecha de realización
Desempeños que debo mostrar			
El producto obtenido en la práctica es:			
Lo que aprendí con la práctica			
Indicadores de la competencia que trabajé			
Dónde puedo aplicar lo aprendido			
Con qué contenidos de otras unidades de aprendizaje se relaciona			
En dónde encontré información complementaria para trabajar la práctica			
Cómo seleccioné la información utilizada			
Criterios con los que me evaluaron			
Qué más me gustaría aprender sobre el tema			

TEMA 03: REDES: DEFINICIÓN, USOS, TIPOS Y COMPONENTES.

- ✓ 3.1 ¿Qué es una red?
- ✓ 3.2 Tipos de redes
- ✓ 3.3 Protocolos de red
- ✓ 3.4 Componentes de una red
- ✓ 3.5 Topología de una red

3.1 ¿QUÉ ES UNA RED?

Una red es un conjunto de computadoras (dos como mínimo), que se unen a través de medios físicos (hardware) y lógicos (software), para compartir información y recursos, con el fin de llevar a cabo una actividad o labor de forma eficiente y eficaz. La conexión física entre los computadores puede efectuarse por alambre de cobre, fibra óptica, cableado UTP, satélites de comunicaciones, microondas, entre otros. Una empresa puede poseer varios computadores en diferentes ciudades y en cada uno de ellos llevar un control de inventarios, activos fijos, cartera, control de producción y nómina.

Cuando surge la necesidad de extraer y consolidar información de toda la empresa, se vuelve un trabajo muy complejo. Ahora, si la misma empresa requiere que todos los programas y computadores estén disponibles para cualquier usuario, adicionalmente tener control de la información, y a su vez consolidar sin importar su localización geográfica, la mejor opción es una Red.

Redes de datos. Las redes de datos se desarrollaron como consecuencia de aplicaciones comerciales diseñadas para microcomputadores. Por aquel entonces, los microcomputadores no estaban conectados entre sí como sí lo estaban las terminales de computadores



mainframe, por lo cual no había una manera eficaz de compartir datos entre varios computadores. Se tornó evidente que el uso de disquetes para compartir datos no era un método eficaz ni económico para desarrollar la actividad empresarial. La red a pie creaba copias múltiples de los datos. Cada vez que se modificaba un archivo, había que volver a compartirlo con el resto de sus usuarios. Si dos usuarios modificaban el archivo, y luego intentaban compartirlo, se perdía alguno de los dos conjuntos de modificaciones. Las empresas necesitaban una solución que resolviera con éxito los tres problemas siguientes:

- Cómo evitar la duplicación de equipos informáticos y de otros recursos
- Cómo comunicarse con eficiencia
- Cómo configurar y administrar una red

Las empresas se dieron cuenta de que la tecnología de networking podía aumentar la productividad y ahorrar gastos. Las redes se agrandaron y extendieron casi con la misma rapidez con la que se lanzaban nuevas tecnologías y productos de red. A principios de la década de 1980 networking se expandió enormemente, aun cuando en sus inicios su desarrollo fue desorganizado.

A mediados de la década de 1980, las tecnologías de red que habían emergido se habían creado con implementaciones de hardware y software distintas. Cada empresa dedicada a crear hardware y software para redes utilizaba sus propios estándares corporativos. Estos estándares individuales se desarrollaron como consecuencia de la competencia con otras empresas.

Por lo tanto, muchas de las nuevas tecnologías no eran compatibles entre sí. Se tornó cada vez más difícil la comunicación entre redes que usaban distintas especificaciones. Esto a menudo obligaba a deshacerse de los equipos de la antigua red al implementar equipos de red nuevos.

Una de las primeras soluciones fue la creación de los estándares de Red de área local (LAN - Local Area Network, en inglés). Como los estándares LAN proporcionaban un conjunto abierto de pautas para la creación de hardware y software de red, se podrían compatibilizar los equipos provenientes de diferentes empresas. Esto permitía la estabilidad en la implementación de las LAN. En un sistema LAN, cada departamento de la empresa era una especie de isla electrónica. A medida que el uso de los computadores en las empresas aumentaba, pronto resultó obvio que incluso las LAN no eran suficientes.

Lo que se necesitaba era una forma de que la información se pudiera transferir rápidamente y con eficiencia, no solamente dentro de una misma empresa sino también de una empresa a otra. La solución fue la creación de redes de área metropolitana (MAN) y redes de área amplia (WAN). Como las WAN podían conectar redes de usuarios dentro de áreas geográficas extensas, permitieron que las empresas se comunicaran entre sí a través de grandes distancias.

La historia de networking informática es compleja.

Participaron en ella muchas personas de todo el mundo a lo largo de los últimos 35 años. Presentamos aquí una versión simplificada de la evolución de la Internet. Los procesos de creación y comercialización son mucho más complicados, pero es útil analizar el desarrollo fundamental. A mediados de la década de 1980 los usuarios con computadores autónomos comenzaron a usar módems para conectarse con otros computadores y compartir archivos. Estas comunicaciones se denominaban comunicaciones punto a punto o de acceso telefónico. El concepto se expandió a través del uso de computadores que funcionaban como punto central de comunicación en una conexión de acceso telefónico. Estos computadores se denominaron tableros de boletín. Los usuarios se conectaban a los tableros de boletín, donde depositaban y levantaban mensajes, además de cargar y descargar archivos. La desventaja de este tipo de sistema era que había poca comunicación directa, y únicamente con quienes conocían el tablero de boletín. Otra limitación era la necesidad de un módem por cada conexión al computador del tablero de boletín.

Si cinco personas se conectaban simultáneamente, hacían falta cinco módems conectados a cinco líneas telefónicas diferentes. A medida que crecía el número de usuarios interesados, el sistema no pudo soportar la demanda. Imagine, por ejemplo, que 500 personas quisieran conectarse de forma simultánea. A partir de la década de 1960 y durante las décadas de 1970, 1980 y 1990, el Departamento de Defensa de Estados Unidos (DoD) desarrolló redes de área amplia (WAN) de gran extensión y alta confiabilidad, para uso militar y científico. Esta tecnología era diferente de la comunicación punto-a-punto usada por los tableros de boletín. Permitía la internetworking de varios computadores mediante diferentes rutas. La red en sí determinaba la forma de transferir datos de un computador a otro. En lugar de poder comunicarse con un solo computador a la vez, se podía acceder a varios computadores mediante la misma conexión. La WAN del DoD finalmente se convirtió en la Internet.

Las LAN constan de los siguientes componentes:

- Computadores
- Tarjetas de interfaz de red
- Dispositivos periféricos
- Medios de networking
- Dispositivos de networking

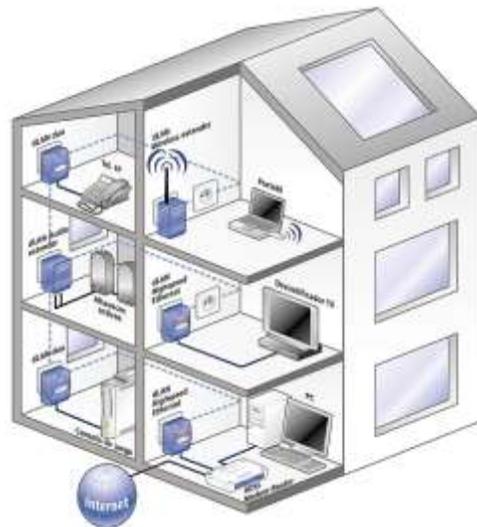
3.2 Tipos de Redes.

LAN. Permiten a las empresas aplicar tecnología informática para compartir localmente archivos e impresoras de manera eficiente, y posibilitar las comunicaciones internas. Un buen ejemplo de esta tecnología es el correo electrónico.

Los que hacen es conectar los datos, las comunicaciones locales y los equipos informáticos.

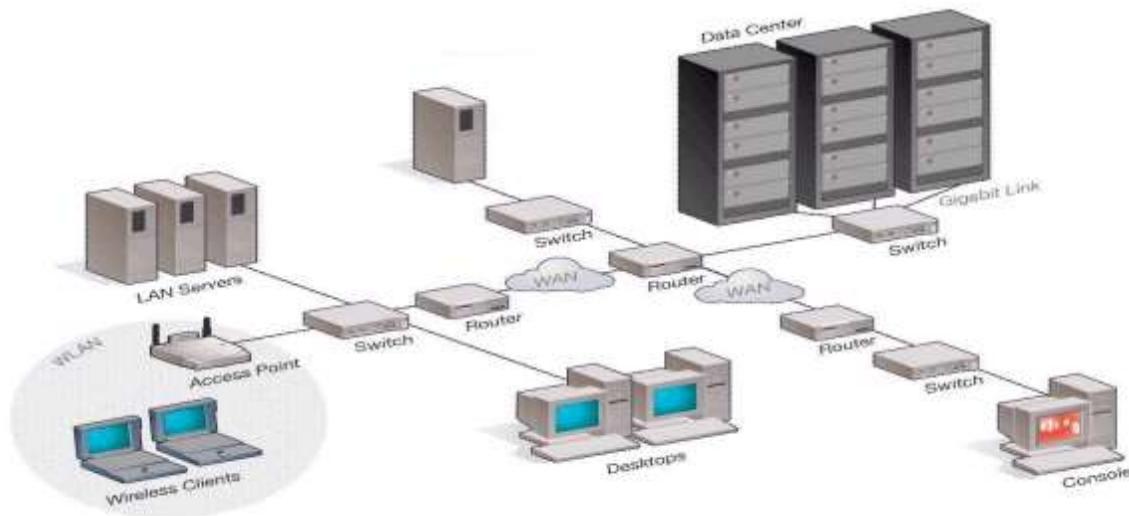
Algunas de las tecnologías comunes de LAN son:

- Ethernet
- Token Ring
- FDDI



WAN.

Interconectan las LAN, que a su vez proporcionan acceso a los computadores o a los servidores de archivos ubicados en otros lugares. Como las WAN conectan redes de usuarios dentro de un área geográfica extensa, permiten que las empresas se comuniquen entre sí a través de grandes distancias. Las WAN permiten que los computadores, impresoras y otros dispositivos de una LAN compartan y sean compartidos por redes en sitios distantes. Las WAN proporcionan comunicaciones instantáneas a través de zonas geográficas extensas. El software de colaboración brinda acceso a información en tiempo real y recursos que permiten realizar reuniones entre personas separadas por largas distancias, en lugar de hacerlas en persona. Networking de área amplia también dio lugar a una nueva clase de trabajadores, los empleados a distancia, que no tienen que salir de sus hogares para ir a trabajar.



Las WAN están diseñadas para realizar lo siguiente:

- Operar entre áreas geográficas extensas y distantes
- Posibilitar capacidades de comunicación en tiempo real entre usuarios
- Brindar recursos remotos de tiempo completo, conectados a los servicios locales
- Brindar servicios de correo electrónico, World Wide Web, transferencia de archivos y comercio electrónico

Algunas de las tecnologías comunes de WAN son:

- Módems
- Red digital de servicios integrados (RDSI)
- Línea de suscripción digital (DSL - Digital Subscriber Line)
- Frame Relay
- Series de portadoras para EE.UU. (T) y Europa (E): T1, E1, T3, E3
- Red óptica síncrona (SONET)

MAN. Es una red que abarca un área metropolitana, como, por ejemplo, una ciudad o una zona suburbana. Una MAN generalmente consta de una o más LAN dentro de un área geográfica común. Por ejemplo, un banco con varias sucursales puede utilizar una MAN. Normalmente, se utiliza un proveedor de servicios para conectar dos o más sitios LAN utilizando líneas privadas de comunicación o servicios ópticos. También se puede crear una MAN usando tecnologías de puente inalámbrico enviando haces de luz a través de áreas públicas.

VPN. Es una red privada que se construye dentro de una infraestructura de red pública, como la Internet global. Con una VPN, un empleado a distancia puede acceder a la red de la sede de la empresa a través de Internet, formando un túnel seguro entre el PC del empleado y un router VPN en la sede. La VPN es un servicio que ofrece conectividad segura y confiable en una infraestructura de red pública compartida, como la Internet. Las VPN conservan las mismas políticas de seguridad y administración que una red privada. Son la forma más económica de establecer una conexión punto-a-punto entre usuarios remotos y la red de un cliente de la empresa.

A continuación, se describen los tres principales tipos de VPN:

- **VPN de acceso:** Las VPN de acceso brindan acceso remoto a un trabajador móvil y una oficina pequeña/oficina hogareña (SOHO), a la sede de la red interna o externa, mediante una infraestructura compartida. Las VPN de acceso usan tecnologías analógicas, de acceso telefónico, RDSI, línea de suscripción digital (DSL), IP móvil y de cable para brindar conexiones seguras a usuarios móviles, empleados a distancia y sucursales.
- **Redes internas VPN:** Las redes internas VPN conectan a las oficinas regionales y remotas a la sede de la red interna mediante una infraestructura compartida, utilizando conexiones dedicadas. Las redes internas VPN difieren de las redes externas VPN, ya que sólo permiten el acceso a empleados de la empresa.
- **Redes externas VPN:** Las redes externas VPN conectan a socios comerciales a la sede de la red mediante una infraestructura compartida, utilizando conexiones dedicadas. Las redes externas VPN difieren de las redes internas VPN, ya que permiten el acceso a usuarios que no pertenecen a la empresa.

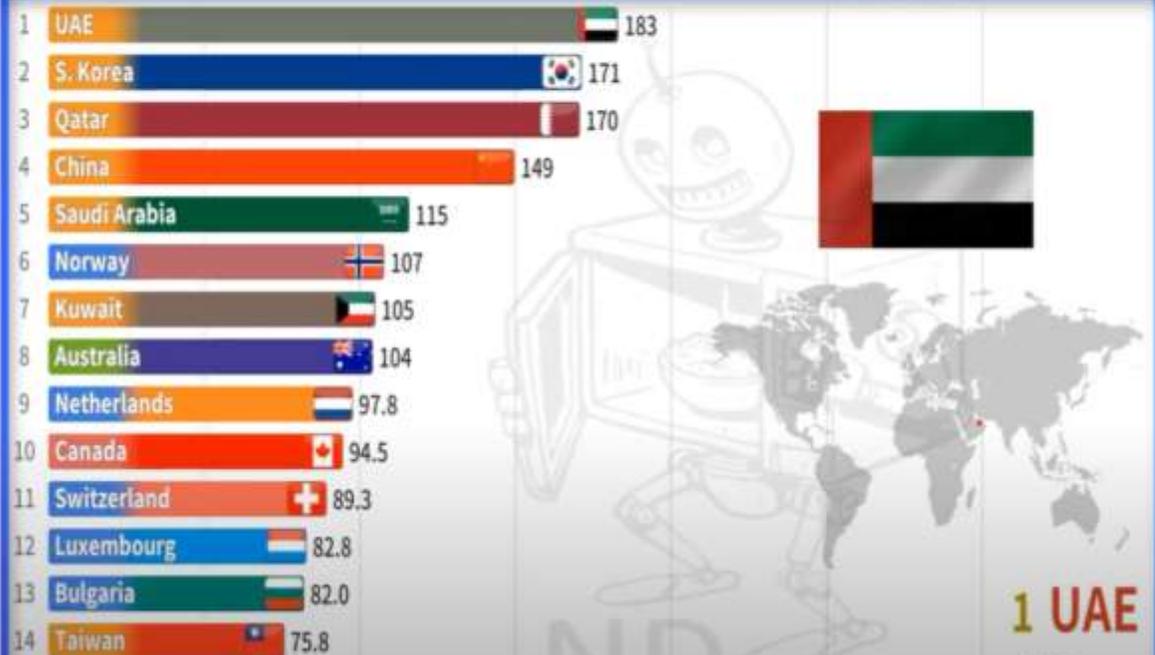
Redes internas y externas. Una de las configuraciones comunes de una LAN es una red interna, a veces denominada "intranet". Los servidores de Web de red interna son distintos de los servidores de Web públicos, ya que es necesario que un usuario público cuente con los correspondientes permisos y contraseñas para acceder a la red interna de una organización. Las redes internas están diseñadas para permitir el acceso por usuarios con privilegios de acceso a la LAN interna de la organización.

Dentro de una red interna, los servidores de Web se instalan en la red. La tecnología de navegador se utiliza como interfaz común para acceder a la información, por ejemplo, datos financieros o datos basados en texto y gráficos que se guardan en esos servidores.

Las redes externas hacen referencia a aplicaciones y servicios basados en la red interna, y utilizan un acceso extendido y seguro a usuarios o empresas externas. Este acceso generalmente se logra mediante contraseñas, identificaciones de usuarios, y seguridad a nivel de las aplicaciones. Por lo tanto, una red externa es la extensión de dos o más estrategias de red interna, con una interacción segura entre empresas participantes y sus respectivas redes internas.

El ancho de banda. Se define como la cantidad de información que puede fluir a través de una conexión de red en un período dado. Es esencial comprender el concepto de ancho de banda al estudiar networking, por las siguientes cuatro razones:

Ranking Mundial de Velocidad de Internet Móvil de 2021



Ranking Mundial de Velocidad de Internet Móvil de 2021



El ancho de banda es finito. Independientemente del medio que se utilice para construir la red, existen límites para la capacidad de la red para transportar información. El ancho de banda está limitado por las leyes de la física y por las tecnologías empleadas para colocar la información en los medios. Por ejemplo, el ancho de banda de un módem convencional está limitado a alrededor de 56 kbps por las propiedades físicas de los cables telefónicos de par trenzado y por la tecnología de módems. No obstante, las tecnologías empleadas por DSL utilizan los mismos cables telefónicos de par trenzado, y sin embargo DSL ofrece un ancho de banda mucho mayor que los módems convencionales. Esto demuestra que a veces es difícil definir los límites impuestos por las mismas leyes de la física. La fibra óptica posee el potencial físico para proporcionar un ancho de banda prácticamente ilimitado. Aun así, el ancho de banda de la fibra óptica no se puede aprovechar en su totalidad, hasta se desarrollen tecnologías que aprovechen todo su potencial.

El ancho de banda no es gratuito. Es posible adquirir equipos para una red de área local (LAN) capaz de brindar un ancho de banda casi ilimitado durante un período extendido de tiempo. Para conexiones de red de área amplia (WAN), casi siempre hace falta comprar el ancho de banda de un proveedor de servicios. En ambos casos, comprender el significado del ancho de banda, y los cambios en su demanda a través del tiempo, pueden ahorrarle importantes sumas de dinero a un individuo o a una empresa. Un administrador de red necesita tomar las decisiones correctas con respecto al tipo de equipo y servicios que debe adquirir.

El ancho de banda es un factor clave a la hora de analizar el rendimiento de una red, diseñar nuevas redes y comprender la Internet. Un profesional de networking debe comprender el fuerte impacto del ancho de banda y la tasa de transferencia en el rendimiento y el diseño de la red. La información fluye en una cadena de bits de un computador a otro en todo el mundo. Estos bits representan enormes cantidades de información que fluyen de ida y de vuelta a través del planeta en segundos, o menos. En cierto sentido, puede ser correcto afirmar que la Internet es puro ancho de banda.

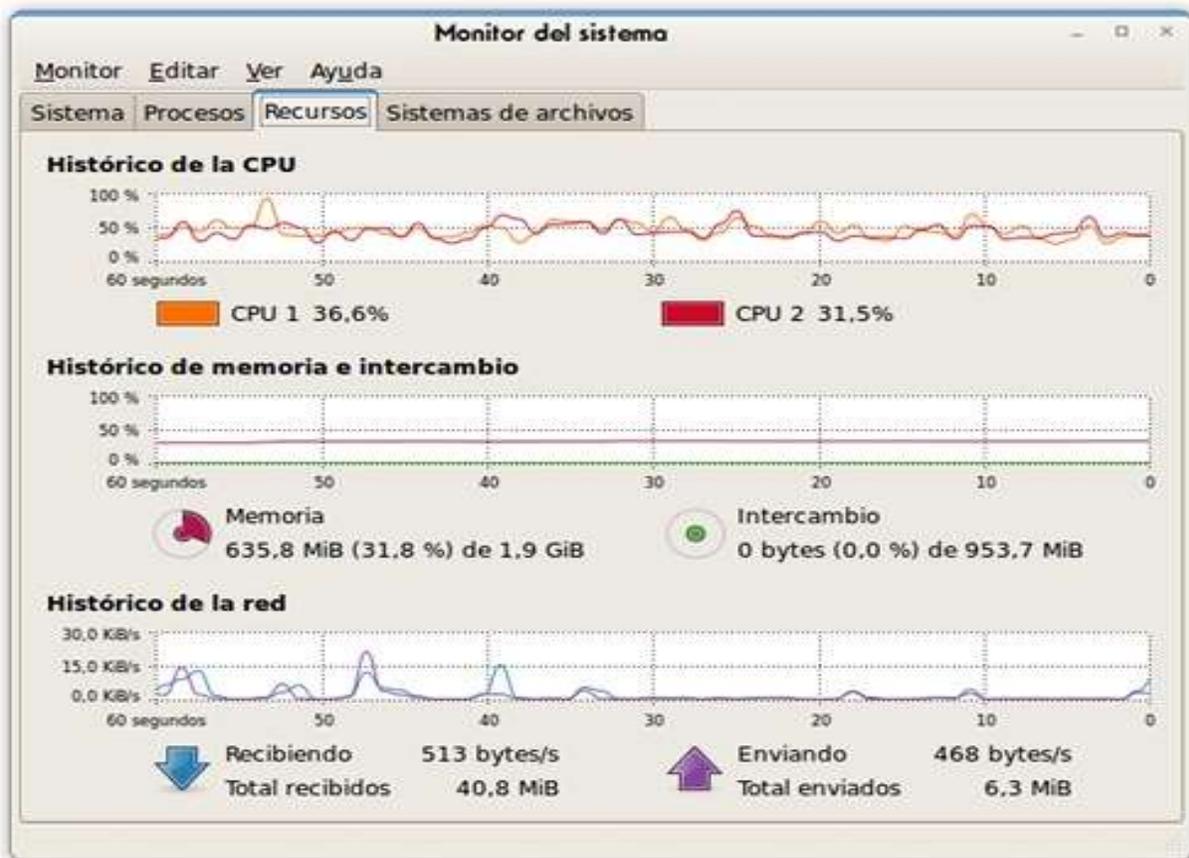
La demanda de ancho de banda no para de crecer. No bien se construyen nuevas tecnologías e infraestructuras de red para brindar mayor ancho de banda, se crean nuevas aplicaciones que aprovechan esa mayor capacidad. La entrega de contenidos de medios enriquecidos a través de la red, incluyendo video y audio fluido, requiere muchísima cantidad de ancho de banda. Hoy se instalan comúnmente sistemas telefónicos IP en lugar de los tradicionales sistemas de voz, lo que contribuye a una mayor necesidad de ancho de banda. Un profesional de networking exitoso debe anticiparse a la necesidad de mayor ancho de banda y actuar en función de eso.

Medición. En los sistemas digitales, la unidad básica del ancho de banda es bits por segundo (bps). El ancho de banda es la medición de la cantidad de información, o bits, que puede fluir desde un lugar hacia otro en un período de tiempo determinado, o segundos. Aunque el ancho de banda se puede describir en bits por segundo, se suelen usar múltiplos de bits por segundo. En otras palabras, el ancho de banda de una red generalmente se describe en términos de miles de bits por segundo (kbps), millones de bits por segundo (Mbps), miles de millones de bits por segundo (Gbps) y billones de bits por segundo (Tbps). A pesar de que las expresiones ancho de banda y velocidad a menudo se usan en forma indistinta, no significan exactamente lo mismo. Se puede decir, por ejemplo, que una conexión T3 a 45Mbps opera a una velocidad mayor que una conexión T1 a 1,544Mbps. No obstante, si sólo se utiliza una cantidad pequeña de su capacidad para transportar datos, cada uno de estos tipos de conexión transportará datos a aproximadamente la misma velocidad. Por ejemplo, una cantidad pequeña de agua fluirá a la misma velocidad por una tubería pequeña y por una tubería grande. Por lo tanto, suele ser más exacto decir que una conexión T3 posee un mayor ancho de banda que una

conexión T1. Esto es así porque la conexión T3 posee la capacidad para transportar más información en el mismo período de tiempo, y no porque tenga mayor velocidad.

Limitaciones. El ancho de banda varía según el tipo de medio, además de las tecnologías LAN y WAN utilizadas. La física de los medios fundamenta algunas de las diferencias. Las señales se transmiten a través de cables de cobre de par trenzado, cables coaxiales, fibras ópticas, y por el aire. Las diferencias físicas en las formas en que se transmiten las señales son las que generan las limitaciones fundamentales en la capacidad que posee un medio dado para transportar información. No obstante, el verdadero ancho de banda de una red queda determinado por una combinación de los medios físicos y las tecnologías seleccionadas para señalar y detectar señales de red. Por ejemplo, la actual comprensión de la física de los cables de cobre de par trenzado no blindados (UTP) establece el límite teórico del ancho de banda en más de un gigabit por segundo (Gbps). Sin embargo, en la realidad, el ancho de banda queda determinado por el uso de Ethernet 10BASE-T, 100BASE-TX, o 1000BASE-TX. En otras palabras, el ancho de banda real queda determinado por los métodos de señalización, las tarjetas de interfaz de red (NIC) y los demás equipos de red seleccionados. Por lo tanto, el ancho de banda no sólo queda determinado por las limitaciones de los medios.

Tasa de Transferencia. El ancho de banda es la medida de la cantidad de información que puede atravesar la red en un período dado de tiempo. Por lo tanto, la cantidad de ancho de banda disponible es un punto crítico de la especificación de la red. Una LAN típica se podría construir para brindar 100 Mbps a cada estación de trabajo individual, pero esto no significa que cada usuario pueda realmente mover cien megabits de datos a través de la red por cada segundo de uso. Esto sólo podría suceder bajo las circunstancias más ideales. El concepto de tasa de transferencia nos ayudará a entender el motivo.



La tasa de transferencia se refiere a la medida real del ancho de banda, en un momento dado del día, usando rutas de Internet específicas, y al transmitirse un conjunto específico de datos. Desafortunadamente, por varios motivos, la tasa de transferencia a menudo es mucho menor que el ancho de banda digital máximo posible del medio utilizado. A continuación, se detallan algunos de los factores que determinan la tasa de transferencia:

- Dispositivos de internetworking
- Tipo de datos que se transfieren
- Topología de la red
- Cantidad de usuarios en la red

El ancho de banda teórico de una red es una consideración importante en el diseño de la red, porque el ancho de banda de la red jamás será mayor que los límites impuestos por los medios y las tecnologías de networking escogidos. No obstante, es igual de importante que un diseñador y administrador de redes considere los factores que pueden afectar la tasa de transferencia real. Al medir la tasa de transferencia regularmente, un administrador de red estará al tanto de los cambios en el rendimiento de la red y los cambios en las necesidades de los usuarios de la red. Así la red se podrá ajustar en consecuencia.

Uso de capas para describir la comunicación de datos. Para que los paquetes de datos puedan viajar desde el origen hasta su destino a través de una red, es importante que todos los dispositivos de la red hablen el mismo lenguaje o protocolo. Un protocolo es un conjunto de reglas que hacen que la comunicación en una red sea más eficiente. Por ejemplo, al pilotar un avión, los pilotos obedecen reglas muy específicas para poder comunicarse con otros aviones y con el control de tráfico aéreo.

Un protocolo de comunicaciones de datos es un conjunto de normas, o un acuerdo, que determina el formato y la transmisión de datos.

3.3 PROTOCOLOS DE RED

Podemos definir un protocolo como el conjunto de normas que regulan la comunicación (establecimiento, mantenimiento y cancelación) entre los distintos componentes de una red informática. Existen dos tipos de protocolos: protocolos de bajo nivel y protocolos de red.

Los protocolos de bajo nivel controlan la forma en que las señales se transmiten por el cable o medio físico. En la primera parte del curso se estudiaron los habitualmente utilizados en redes locales (Ethernet y Token Ring). Aquí nos centraremos en los protocolos de red. Los protocolos de red organizan la información (controles y datos) para su transmisión por el medio físico a través de los protocolos de bajo nivel. Veamos algunos de ellos:

IPX/SPX. IPX (*Internetwork Packet Exchange*) es un protocolo de Novell que interconecta redes que usan clientes y servidores Novell Netware. Es un protocolo orientado a paquetes y no orientado a conexión (esto es, no requiere que se establezca una conexión antes de que los paquetes se envíen a su destino). Otro protocolo, el SPX (*Sequenced Packet eXchange*), actúa sobre IPX para asegurar la entrega de los paquetes.

NetBIOS. NetBIOS (*Network Basic Input/Output System*) es un programa que permite que se comuniquen aplicaciones en diferentes ordenadores dentro de una LAN. Desarrollado originalmente para las redes de ordenadores personales IBM, fue adoptado posteriormente por Microsoft. NetBIOS se usa en redes con topologías Ethernet y Token ring.

No permite por sí mismo un mecanismo de enrutamiento por lo que no es adecuado para redes de área extensa (MAN), en las que se deberá usar otro protocolo para el transporte de los datos (por ejemplo, el TCP).

NetBIOS puede actuar como protocolo orientado a conexión o no (en sus modos respectivos *sesión* y *datagrama*). En el modo sesión dos ordenadores establecen una conexión para establecer una conversación entre los mismos, mientras que en el modo datagrama cada mensaje se envía independientemente.

Una de las desventajas de NetBIOS es que no proporciona un marco estándar o formato de datos para la transmisión.

NetBEUI. *NetBIOS Extended User Interface* o *Interfaz de Usuario para NetBIOS* es una versión mejorada de NetBIOS que sí permite el formato o arreglo de la información en una transmisión de datos. También desarrollado por IBM y adoptado después por Microsoft, es actualmente el protocolo predominante en las redes Windows NT, LAN Manager y Windows para Trabajo en Grupo.

Aunque NetBEUI es la mejor elección como protocolo para la comunicación dentro de una LAN, el problema es que no soporta el enrutamiento de mensajes hacia otras redes, que deberá hacerse a través de otros protocolos (por ejemplo, IPX o TCP/IP). Un método usual es instalar tanto NetBEUI como TCP/IP en cada estación de trabajo y configurar el servidor para usar NetBEUI para la comunicación dentro de la LAN y TCP/IP para la comunicación hacia afuera de la LAN.

AppleTalk. Es el protocolo de comunicación para ordenadores Apple Macintosh y viene incluido en su sistema operativo, de tal forma que el usuario no necesita configurarlo. Existen tres variantes de este protocolo:

 **LocalTalk.** La comunicación se realiza a través de los puertos serie de las estaciones. La velocidad de transmisión es pequeña, pero sirve por ejemplo para compartir impresoras.

 **Ethernalk.** Es la versión para Ethernet. Esto aumenta la velocidad y facilita aplicaciones como por ejemplo la transferencia de archivos.

 **Tokentalk.** Es la versión de Appletalk para redes Tokenring.

TCP/IP. Es realmente un conjunto de protocolos, donde los más conocidos son TCP (*Transmission Control Protocol* o protocolo de control de transmisión) e IP (*Internet Protocol* o protocolo Internet). Dicha conjunto o familia de protocolos es el que se utiliza en Internet. Lo estudiaremos con detalle en el apartado siguiente.

Internet es un conglomerado muy amplio y extenso en el que se encuentran ordenadores con sistemas operativos incompatibles, redes más pequeñas y distintos servicios con su propio conjunto de protocolos para la comunicación. Ante tanta diversidad resulta necesario establecer un conjunto de reglas comunes para la comunicación entre estos diferentes elementos y que además optimice la utilización de recursos tan distantes.

Este papel lo tiene el protocolo TCP/IP. TCP/IP también puede usarse como protocolo de comunicación en las redes privadas intranet y extranet. Las siglas TCP/IP se refieren a dos protocolos de red, que son *Transmission Control Protocol* (Protocolo de Control de Transmisión) e *Internet Protocol* (Protocolo de Internet) respectivamente. Estos protocolos pertenecen a un conjunto mayor de protocolos. Dicho conjunto se denomina *suite TCP/IP*.

Los diferentes protocolos de la suite TCP/IP trabajan conjuntamente para proporcionar el transporte de datos dentro de Internet (o Intranet). En otras palabras, hacen posible que accedamos a los distintos servicios de la Red. Estos servicios incluyen, como se comentó en el capítulo 1: transmisión de correo electrónico, transferencia de ficheros, grupos de noticias, acceso a la World Wide Web, etc.

Hay dos clases de protocolos dentro de la suite TCP/IP que son: *protocolos a nivel de red* y *protocolos a nivel de aplicación*.

Protocolos a Nivel de Red. Estos protocolos se encargan de controlar los mecanismos de transferencia de datos. Normalmente son invisibles para el usuario y operan por debajo de la superficie del sistema. Dentro de estos protocolos tenemos:

 **TCP.** Controla la división de la información en unidades individuales de datos (llamadas paquetes) para que estos paquetes sean encaminados de la forma más eficiente hacia su punto de destino. En dicho punto, TCP se encargará de re ensamblar dichos paquetes para reconstruir el fichero o mensaje que se envió. Por ejemplo, cuando se nos envía un fichero HTML desde un servidor Web, el protocolo de control de transmisión en ese servidor divide el fichero en uno o más paquetes, numera dichos paquetes y se los pasa al protocolo IP. Aunque cada paquete tenga la misma dirección IP de destino, puede seguir una ruta diferente a través de la red. Del otro lado (el programa cliente en nuestro ordenador), TCP reconstruye los paquetes individuales y espera hasta que hayan llegado todos para presentárnoslos como un solo fichero.

 **IP.** Se encarga de repartir los paquetes de información enviados entre el ordenador local y los ordenadores remotos. Esto lo hace etiquetando los paquetes con una serie de información, entre la que cabe destacar las direcciones IP de los dos ordenadores. Basándose en esta información, IP garantiza que los datos se encaminarán al destino correcto. Los paquetes recorrerán la red hasta su destino (que puede estar en el otro extremo del planeta) por el camino más corto posible gracias a unos dispositivos denominados *encaminadores* o *routers*.

Protocolos a Nivel de Aplicación. Aquí tenemos los protocolos asociados a los distintos servicios de Internet, como FTP, Telnet, Gopher, HTTP, etc. Estos protocolos son visibles para el usuario en alguna medida. Por ejemplo, el protocolo FTP (File Transfer Protocol) es visible para el usuario. El usuario solicita una conexión a otro ordenador para transferir un fichero, la conexión se establece, y comienza la transferencia. Durante dicha transferencia, es visible parte del intercambio entre la máquina del usuario y la máquina remota (mensajes de error y de estado de la transferencia, como por ejemplo cuantos bytes del fichero se han transferido en un momento dado).

Breve Historia del Protocolo TCP/IP. A principios de los años 60, varios investigadores intentaban encontrar una forma de compartir recursos informáticos de una forma más eficiente. En 1961, Leonard Klienrock introduce el concepto de *Conmutación de Paquetes* (*Packet Switching*, en inglés). La idea era que la comunicación entre ordenadores fuese dividida en *paquetes*. Cada paquete debería contener la dirección de destino y podría encontrar su propio camino a través de la red.

Como ya comentamos en el capítulo anterior, en 1969 la Agencia de Proyectos de Investigación Avanzada (Defense Advanced Research Projects Agency o DARPA) del Ejército de los EEUU desarrolla la ARPAnet. La finalidad principal de esta red era la capacidad de resistir un ataque nuclear de la URSS para lo que se pensó en una administración descentralizada. De este modo, si algunos ordenadores eran destruidos, la red seguiría funcionando. Aunque dicha

red funcionaba bien, estaba sujeta a algunas caídas periódicas del sistema. De este modo, la expansión a largo plazo de esta red podría resultar difícil y costosa. Se inició entonces una búsqueda de un conjunto de protocolos más fiables para la misma. Dicha búsqueda finalizó, a mediados de los 70, con el desarrollo de TCP/IP.

TCP/IP tenía (y tiene) ventajas significativas respecto a otros protocolos. Por ejemplo, consume pocos recursos de red. Además, podía ser implementado a un coste mucho menor que otras opciones disponibles entonces. Gracias a estos aspectos, TCP/IP comenzó a hacerse popular. En 1983, TCP/IP se integró en la versión 4.2 del sistema operativo UNIX de Berkeley y la integración en versiones comerciales de UNIX vino pronto.

Así es como TCP/IP se convirtió en el estándar de Internet. En la actualidad, TCP/IP se usa para muchos propósitos, no solo en Internet. Por ejemplo, a menudo se diseñan *intranets* usando TCP/IP. En tales entornos, TCP/IP ofrece ventajas significativas sobre otros protocolos de red. Una de tales ventajas es que trabaja sobre una gran variedad de hardware y sistemas operativos. De este modo puede crearse fácilmente una red heterogénea usando este protocolo.

Dicha red puede contener estaciones Mac, PC compatibles, estaciones Sun, servidores Novell, etc. Todos estos elementos pueden comunicarse usando la misma suite de protocolos TCP/IP.

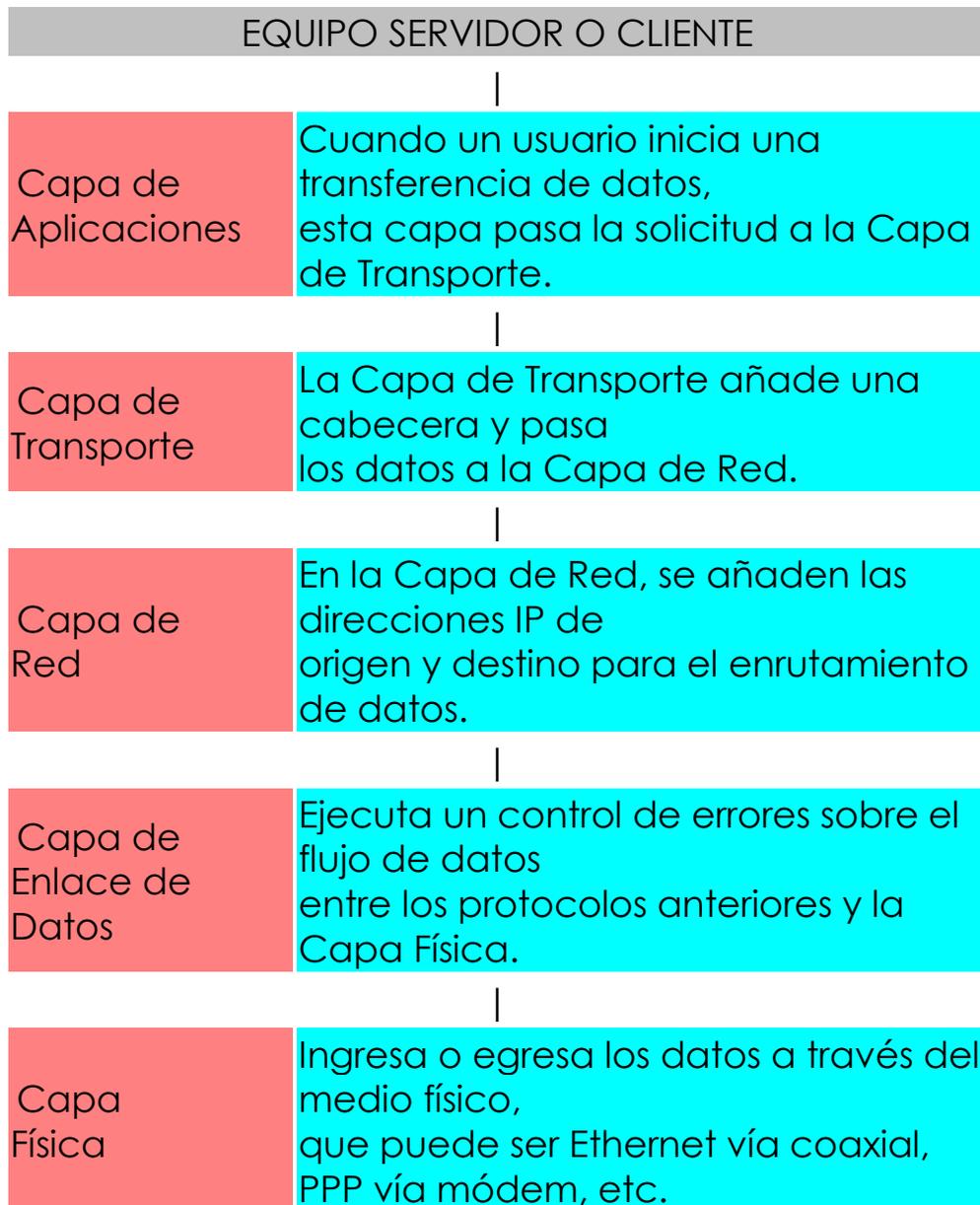
La siguiente tabla muestra una lista de plataformas que soportan TCP/IP:

<i>Plataforma</i>	<i>Soporte de TCP/IP</i>
UNIX	Nativo
DOS	Piper/IP por Ipswitch
Windows	TCPMAN por Trumpet Software
Windows 95	Nativo
Windows NT	Nativo
Macintosh	MacTCP u OpenTransport (Sys 7.5+)
OS/2	Nativo
AS/400 OS/400	Nativo

Las plataformas que no soportan TCP/IP nativamente lo implementan usando programas TCP/IP de terceras partes, como puede apreciarse en la tabla anterior.

Cómo Trabaja TCP/IP.

TCP/IP opera a través del uso de una pila. Dicha pila es la suma total de todos los protocolos necesarios para completar una transferencia de datos entre dos máquinas (así como el camino que siguen los datos para dejar una máquina o entrar en la otra). La pila está dividida en capas, como se ilustra en la figura siguiente:



Después de que los datos han pasado a través del proceso ilustrado en la figura anterior, viajan a su destino en otra máquina de la red. Allí, el proceso se ejecuta al revés (los datos entran por la capa física y recorren la pila hacia arriba). Cada capa de la pila puede enviar y recibir datos

desde la capa adyacente. Cada capa está también asociada con múltiples protocolos que trabajan sobre los datos.

Cada vez que una máquina solicita una conexión a otra, especifica una dirección particular. En general, esta dirección será la dirección IP Internet de dicha máquina. Pero hablando con más detalle, la máquina solicitante especificará también la aplicación que está intentando alcanzar dicho destino. Esto involucra a dos elementos: un programa llamado *inetd* y un sistema basado en *puertos*.

Inetd. Inetd pertenece a un grupo de programas llamados TSR (*Terminate and stay resident*). Dichos programas siempre están en ejecución, a la espera de que se produzca algún suceso determinado en el sistema. Cuando dicho suceso ocurre, el TSR lleva a cabo la tarea para la que está programado.

En el caso de *inetd*, su finalidad es estar a la espera de que se produzca alguna solicitud de conexión del exterior. Cuando esto ocurre, *inetd* evalúa dicha solicitud determinando que servicio está solicitando la máquina remota y le pasa el control a dicho servicio. Por ejemplo, si la máquina remota solicita una página web, le pasará la solicitud al proceso del servidor Web.

En general, *inetd* es iniciado al arrancar el sistema y permanece residente (a la escucha) hasta que apagamos el equipo o hasta que el operador del sistema finaliza expresamente dicho proceso.

Puertos. La mayoría de las aplicaciones TCP/IP tienen una filosofía de cliente-servidor. Cuando se recibe una solicitud de conexión, *inetd* inicia un programa servidor que se encargará de comunicarse con la máquina cliente. Para facilitar este proceso, a cada aplicación (FTP o Telnet, por ejemplo) se le asigna una única dirección. Dicha dirección se llama *puerto*. Cuando se produce una solicitud de conexión a dicho puerto, se ejecutará la aplicación correspondiente. Aunque la asignación de puertos a los diferentes servicios es de libre elección para los administradores de sistema, existe un estándar en este sentido que es conveniente seguir. La tabla que se muestra a continuación presenta un listado de algunas asignaciones estándar:

<i>Servicio o Aplicación</i>	<i>Puerto</i>
File Transfer Protocol (FTP)	21
Telnet	23
Simple Mail Transfer Protocol (SMTP)	25
Gopher	70
Finger	79
Hypertext Transfer Protocol (HTTP)	80
Network News Transfer Protocol (NNTP)	119

Números IP. En el capítulo anterior vimos que una dirección IP consistía en cuatro números separados por puntos, estando cada uno de ellos en el rango de 0 a 254. Por ejemplo, una dirección IP válida sería 193.146.85.34. Cada uno de los números decimales representa una cadena de ocho dígitos binarios. De este modo, la dirección anterior sería realmente la cadena de ceros y unos:

11000001.10010010.01010101.00100010

NOTA: Podemos usar la Calculadora de Windows 95 para realizar las conversiones de binario-decimal y viceversa.

La versión actual del protocolo IP (la versión 4 o IPv4) define de esta forma direcciones de 32 bits, lo que quiere decir que hay 2^{32} (4.294.967.296) direcciones IPv4 disponibles. Esto parece un gran número, pero la apertura de nuevos mercados y el hecho de que un porcentaje significativo de la población mundial sea candidato a tener una dirección IP, hacen que el número finito de direcciones pueda agotarse eventualmente. Este problema se ve agravado por el hecho de que parte del espacio de direccionamiento está mal asignado y no puede usarse a su máximo potencial.

Por otra parte, el gran crecimiento de Internet en los últimos años ha creado también dificultades para encaminar el tráfico entre el número cada vez mayor de redes que la componen. Esto ha creado un crecimiento exponencial del tamaño de las tablas de encaminamiento que se hacen cada vez más difíciles de sostener. Los problemas comentados se han solucionado en parte hasta la fecha introduciendo progresivos niveles de jerarquía en el espacio de direcciones IP, que pasamos a comentar en los siguientes apartados. No obstante, la solución a largo plazo de estos problemas pasa por desarrollar la próxima generación del protocolo IP (IPng o IPv6) que puede alterar algunos de nuestros conceptos fundamentales acerca de Internet.

Clasificación del Espacio de Direcciones

Cuando el protocolo IP se estandarizó en 1981, la especificación requería que a cada sistema conectado a Internet se le asignase una única dirección IP de 32 bits. A algunos sistemas, como los routers, que tienen interfaces a más de una red se les debía asignar una única dirección IP para cada interfaz de red. La primera parte de una dirección IP identifica la red a la que pertenece el host, mientras que la segunda identifica al propio host. Por ejemplo, en la dirección 135.146.91.26 tendríamos:

Prefijo de Red	Número de Host
135.146	91.26

Esto crea una jerarquía del direccionamiento a dos niveles. Recordemos que la dirección es realmente una cadena de 32 dígitos binarios, en la que en el ejemplo anterior hemos usado los 24 primeros para identificar la red y los 8 últimos para identificar el host.

Clases Primarias de Direcciones.

Con la finalidad de proveer la flexibilidad necesaria para soportar redes de distinto tamaño, los diseñadores decidieron que el espacio de direcciones debería ser dividido en tres clases diferentes: Clase A, Clase B y Clase C. Cada clase fija el lugar que separa la dirección de red de la de host en la cadena de 32 bits. Una de las características fundamentales de este sistema

de clasificación es que cada dirección contiene una clave que identifica el punto de división entre el prefijo de red y el número de host. Por ejemplo, si los dos primeros bits de la dirección son 1-0 el punto estará entre los bits 15 y 16.

Redes Clase A (/8).

Cada dirección IP en una red de clase A posee un prefijo de red de 8 bits (con el primer bit puesto a 0 y un número de red de 7 bits), seguido por un número de host de 24 bits.

El posible definir un máximo de 126 (2^7-2) redes de este tipo y cada red /8 soporta un máximo de 16.777.214 ($2^{24}-2$) hosts. Obsérvese que hemos restado dos números de red y dos números de host. Estos números no pueden ser asignados ni a ninguna red ni a ningún host y son usados para propósitos especiales. Por ejemplo, el número de host "todos 0" identifica a la propia red a la que "pertenece".

Traduciendo los números binarios a notación decimal, tendríamos el siguiente rango de direcciones para las redes /8 o clase A:

1.xxx.xxx.xxx hasta 126.xxx.xxx.xxx

Redes Clase B (/16). Tienen un prefijo de red de 16 bits (con los dos primeros puestos a 1-0 y un número de red de 14 bits), seguidos por un número de host de 16 bits. Esto nos da un máximo de 16.384 (2^{14}) redes de este tipo, pudiéndose definir en cada una de ellas hasta 65.534 ($2^{16}-2$) hosts.

Traduciendo los números binarios a notación decimal, tendríamos el siguiente rango de direcciones para las redes /16 o clase B:

128.0.xxx.xxx hasta 191.255.xxx.xxx

Redes Clase C (/24). Cada dirección de red clase C tiene un prefijo de red de 24 bits (siendo los tres primeros 1-1-0 con un número de red de 21 bits), seguidos por un número de host de 8 bits. Tenemos así 2.097.152 (2^{21}) redes posibles con un máximo de 254 (2^8-2) host por red.

El rango de direcciones en notación decimal para las redes clase C sería:

192.0.0.xxx hasta 223.255.255.xxx

Subredes. En 1985 se define el concepto de subred, o división de un número de red Clase A, B o C, en partes más pequeñas. Dicho concepto es introducido para subsanar algunos de los problemas que estaban empezando a producirse con la clasificación del direccionamiento de dos niveles jerárquicos.



Las tablas de enrutamiento de Internet estaban empezando a crecer.



Los administradores locales necesitaban solicitar otro número de red de Internet antes de que una nueva red se pudiese instalar en su empresa.

Ambos problemas fueron abordados añadiendo otro nivel de jerarquía, creándose una jerarquía a tres niveles en la estructura del direccionamiento IP. La idea consistió en dividir la

parte dedicada al número de host en dos partes: el número de subred y el número de host en esa subred:

Jerarquía a dos Niveles

Prefijo de Red	Número de Host
135.146	91.26

Jerarquía a tres Niveles

Prefijo de Red	Número de Subred	Número de Host
135.146	91	26

Este sistema aborda el problema del crecimiento de las tablas de enrutamiento, asegurando que la división de una red en subredes nunca es visible fuera de la red privada de una organización. Los routers dentro de la organización privada necesitan diferenciar entre las subredes individuales, pero en lo que se refiere a los routers de Internet, todas las subredes de una organización están agrupadas en una sola entrada de la tabla de rutas.

Esto permite al administrador local introducir la complejidad que desee en la red privada, sin afectar al tamaño de las tablas de rutas de Internet.

Por otra parte, sólo hará falta asignar a la organización un único número de red (de las clases A, B o C) o como mucho unos pocos. La propia organización se encargará entonces de asignar distintos números de subred para cada una de sus redes internas. Esto evita en la medida de lo posible el agotamiento de los números IP disponibles.

Máscara de Subred.

Prefijo de Red extendido. Los routers de Internet usan solamente el prefijo de red de la dirección de destino para encaminar el tráfico hacia un entorno con subredes. Los routers dentro del entorno con subredes usan el prefijo de red extendido para encaminar el tráfico entre las subredes. El prefijo de red extendido está compuesto por el prefijo de red y el número de subred:

Prefijo de Red Extendido		
Prefijo de Red	Número de Subred	Número de Host

El prefijo de red extendido se identifica a través de la *máscara de subred*. Por ejemplo, si consideramos la red clase B 135.146.0.0 y queremos usar el tercer octeto completo para representar el número de subred, deberemos especificar la máscara de subred 255.255.255.0

Entre los bits en la máscara de subred y la dirección de Internet existe una correspondencia uno a uno. Los bits de la máscara de subred están a 1 si el sistema que examina la dirección debe tratar los bits correspondientes en la dirección IP como parte del prefijo de red extendido. Los bits de la máscara están a 0 si el sistema debe considerar los bits como parte del número de host. Esto se ilustra en la siguiente figura:

		prefijo de red		nº subred	nº host
Dirección IP	135.146.91.26	10000111	10010010	01011011	00011010
Máscara de Subred	255.255.255.0	11111111	11111111	11111111	00000000
		prefijo de red extendido			

En lo que sigue nos referiremos a la *longitud del prefijo de red extendido* más que a la máscara de subred, aunque indican lo mismo. La longitud del prefijo es igual al número de bits a 1 contiguos en la máscara de subred.

De este modo, la dirección 135.146.91.26 con una máscara de subred 255.255.255.0 podrá expresarse también de la forma 135.146.91.26/24, lo que resulta más compacto y fácil de entender.

Caso práctico.

Pero veamos un caso práctico para comprender mejor esta clasificación con tres niveles jerárquicos. A una organización se le ha asignado el número de red 193.1.1.0/24 (esto es, una clase C) y dicha organización necesita definir seis subredes. La subred más grande puede contener un máximo de 25 hosts.

Primer paso (definir la máscara de subred).

Lo primero que debemos hacer es determinar el número de bits necesarios para definir las 6 subredes. Dada la naturaleza del sistema de numeración binario esto sólo puede hacerse tomando múltiplos de 2. Así que cogemos $2^3=8$ y podemos dejar las 2 subredes restantes previendo un eventual crecimiento de nuestra red.

Como $8=2^3$, se necesitan 3 bits para numerar las 8 subredes. Como estamos hablando de una clase C (/24), sumamos 3 y nuestro prefijo de red extendido será /27 que en decimal nos daría la máscara 255.255.255.224. Esto se ilustra en la figura siguiente:

	prefijo de red			bits nº subr	bits nº host
193.1.1.0/24=	11000001	00000001	00000001	000	00000
		prefijo de red extendido			

255.255.255.224=	11111111	11111111	11111111	111	00000
27 bits					

NOTA: Para no desanimarse, podemos coger la calculadora y hacer la conversión de 11100000 a decimal, que dará justamente 224.

Segundo paso (definir los números de subred). Las ocho subredes se numerarán de 0 a 7. Lo único que tenemos que hacer es colocar la representación binaria de dichos números en el campo *bits n° subred* de la primera fila de la figura anterior, y luego traducir las direcciones binarias a decimal.

Quedaría lo siguiente:

- Red Base: 11000001.00000001.00000001.00000000=193.1.1.0/24
- Subred 0: 11000001.00000001.00000001.**000**00000=193.1.1.0/27
- Subred 1: 11000001.00000001.00000001.**001**00000=193.1.1.32/27
- Subred 2: 11000001.00000001.00000001.**010**00000=193.1.1.64/27
- Subred 3: 11000001.00000001.00000001.**011**00000=193.1.1.96/27
- Subred 4: 11000001.00000001.00000001.**100**00000=193.1.1.128/27
- Subred 5: 11000001.00000001.00000001.**101**00000=193.1.1.160/27
- Subred 6: 11000001.00000001.00000001.**110**00000=193.1.1.192/27
- Subred 7: 11000001.00000001.00000001.**111**00000=193.1.1.224/27

Tercer paso (definir los números de host).

En nuestro ejemplo, disponemos de 5 bits en el campo *bits n° host* de cada dirección de subred. Esto nos da un bloque de 30 ($=2^5-2$) direcciones de host posibles, que cubre los 25 que se prevén como máximo. Obsérvese que restamos 2 pues las direcciones de host todos 0 (esta subred) o todos 1 (broadcast) no pueden usarse.

- Subred 2: 11000001.00000001.00000001.010**00000**=193.1.1.64/24
- Host 1: 11000001.00000001.00000001.010**00001**=193.1.1.64/27
- Host 2: 11000001.00000001.00000001.010**00010**=193.1.1.65/27
- Host 3: 11000001.00000001.00000001.010**00011**=193.1.1.66/27

Host 29: 11000001.00000001.00000001.01011101=193.1.1.93/27

Host 30: 11000001.00000001.00000001.01011110=193.1.1.94/27

DNS.

Como ya comentamos en el capítulo dedicado a Internet, el DNS (Domain Name System, o Sistema de Nombres de Dominio) es un sistema que hace corresponder a la dirección IP de cada host de Internet un único nombre de dominio, para que podamos acceder a dicho host con mayor facilidad. Además, veíamos que la estructura de dichos nombres es jerárquica, algo similar a *Nombre_del_host.Subsubdominio.Subdominio.Dominio*. Estudiaremos ahora con más detalle este tema. Comenzamos explicando algunos conceptos previos que nos servirán para comprender mejor el tema.

En las redes TCP/IP, los ordenadores se identifican a través de su dirección IP. Sin embargo, a los usuarios les resulta más fácil usar nombres para los ordenadores en vez de números, por lo que se hace necesario establecer un mecanismo que resuelva nombres en direcciones IP cuando se soliciten conexiones dando los nombres de los ordenadores remotos.

Esto se conoce como un sistema de resolución de nombres. En las redes Windows existen diversos sistemas de resolución de nombres disponibles:

Resolución de nombres por difusión.

Cuando un equipo se conecta a la red, realizará difusiones a nivel IP para registrar su nombre NetBIOS anunciándolo en la red. Cada equipo en el área de difusión es responsable de cancelar cualquier intento de registrar un nombre duplicado.

Uno de los problemas existentes en este sistema es que, si la red es grande, se sobrecargará de difusiones. No obstante, resultará el adecuado en nuestra Intranet para las conexiones internas.

Servicio de nombres Internet de Windows (WINS, Windows Internet Naming Service).

Utiliza una base de datos dinámica que hace corresponder nombres de equipos NetBIOS con direcciones IP. Dicha base de datos reside en un servidor WINS (que será una máquina con Windows NT server). WINS reduce el uso de la resolución por difusión y permite a los usuarios localizar fácilmente sistemas en redes remotas.

Resolución de nombres usando el Sistema de nombres de dominio (DNS).

DNS permite resolver nombres DNS a direcciones IP cuando un ordenador se conecta a ordenadores remotos fuera de la red local (por ejemplo, a nodos de Internet). Necesita un servidor de nombres DNS. En nuestro caso dicho servidor será el de Red Canaria, al cual accederemos a través de nuestro router que actuará como puerta de enlace o gateway para cada estación de nuestra red local. Para más detalles sobre DNS ver el apartado siguiente.

Ficheros LMHOSTS y HOSTS.

Ambos ficheros se utilizan en ordenadores locales para enumerar direcciones IP conocidas de ordenadores remotos junto con sus nombres de equipo. El fichero LMHOSTS especifica el nombre NetBIOS del ordenador remoto y su dirección IP. El fichero HOST especifica el nombre DNS y la dirección IP.

Pueden considerarse como equivalentes locales a los servicios WINS y DNS y pueden usarse para resolver nombres de ordenadores remotos a direcciones IP cuando los servicios anteriores no están disponibles. En nuestro caso, usaremos un fichero HOSTS en cada una de nuestras estaciones para indicar el nombre y la dirección IP de nuestro servidor web interno (Servweb), ya que al tener el DNS activado en dichas estaciones (para acceder a Internet), cuando no estemos conectados dicho DNS no estará operativo con la consiguiente ralentización en la resolución del nombre del servidor web interno.

El DNS es una base de datos distribuida que proporciona un sistema de nomenclatura jerárquico para indentificar hosts en Internet.

Espacio de nombres de dominio.

La base de datos DNS tiene una estructura en árbol que se llama *espacio de nombres de dominio*. Cada dominio (o nodo en el árbol) tiene un nombre y puede contener subdominios. El *nombre de dominio* identifica la posición del dominio en el árbol respecto a su dominio principal, utilizándose puntos para separar los nombres de los nodos. Por ejemplo, el nombre de dominio *rcanaria.es* se refiere al subdominio *rcanaria* perteneciente al dominio principal *es*. **Dominios de primer nivel.** Los dominios del nivel superior en la base de datos DNS pueden ser genéricos (*com*, *org*, *edu*, etc.) o territoriales (*uk*, *es*, etc.). Para obtener un listado completo, consultar el capítulo 1. La administración de dichos dominios se lleva a cabo por un organismo llamado InterNIC.

Dominios de niveles inferiores y zonas.

Por debajo del primer nivel, InterNIC delega en otras organizaciones la administración del espacio de nombres de dominio. El árbol DNS queda dividido en zonas, donde cada zona es una unidad administrativa independiente. Las zonas pueden ser un único dominio o un dominio dividido en subdominios. Por ejemplo, el dominio *rcanaria* sería una zona administrativa del árbol DNS.

Nombres de dominio completos.

Un nombre de dominio completo (FQDN o Fully Qualified Domain Name) se forma siguiendo la ruta desde la parte inferior del árbol DNS (nombre de host) hasta la raíz de dicho árbol. En el FQDN el nombre de cada nodo es separado por un punto. Un ejemplo de FQDN sería *www.educa.rcanaria.es*.

Servidores de nombres y resolvers.

Los servidores DNS o servidores de nombre contienen información de una parte de la base de datos DNS (zona) para satisfacer las demandas de los clientes DNS. Cuando un ordenador cliente (*resolver*) solicita una conexión a un ordenador remoto de Internet a través de su FQDN, el servidor de nombres buscará el FQDN en su porción de la base de datos DNS. Si está ahí, satisfará de inmediato la demanda del resolver. En caso contrario, consultará a otros servidores de nombres para intentar responder a la consulta.

3.4 COMPONENTES DE UNA RED.

Una red de computadoras consta tanto de hardware como de software. En el hardware se incluyen: estaciones de trabajo, servidores, tarjeta de interfaz de red, cableado y equipo de conectividad. En el software se encuentra el sistema operativo de red (Network Operating System, NOS).

Estaciones de trabajo.

Cada computadora conectada a la red conserva la capacidad de funcionar de manera independiente, realizando sus propios procesos. Asimismo, las computadoras se convierten en estaciones de trabajo en red, con acceso a la información y recursos contenidos en el servidor de archivos de la misma. Una estación de trabajo no comparte sus propios recursos con otras computadoras. Esta puede ser desde una PC XT hasta una Pentium, equipada según las necesidades del usuario; o también de otra arquitectura diferente como Macintosh, Silicon Graphics, Sun, etc.

Servidores. Son aquellas computadoras capaces de compartir sus recursos con otras. Los recursos compartidos pueden incluir impresoras, unidades de disco, CD-ROM, directorios en disco duro e incluso archivos individuales. Los tipos de servidores obtienen el nombre dependiendo del recurso que comparten. Algunos de ellos son: servidor de discos, servidor de archivos, servidor de archivos distribuido, servidores de archivos dedicados y no dedicados, servidor de terminales, servidor de impresoras, servidor de discos compactos, servidor web y servidor de correo.

Tarjeta de Interfaz de Red. Para comunicarse con el resto de la red, cada computadora debe tener instalada una tarjeta de interfaz de red (Network Interface Card, NIC). Se les llama también adaptadores de red o sólo tarjetas de red. En la mayoría de los casos, la tarjeta se adapta en la ranura de expansión de la computadora, aunque algunas son unidades externas que se conectan a ésta a través de un puerto serial o paralelo. Las tarjetas internas casi siempre se utilizan para las PC's, PS/2 y estaciones de trabajo como las SUN's. Las tarjetas de interfaz también pueden utilizarse en minicomputadoras y mainframes. A menudo se usan cajas externas para Mac's y para algunas computadoras portátiles. La tarjeta de interfaz obtiene la información de la PC, la convierte al formato adecuado y la envía a través del cable a otra tarjeta de interfaz de la red local. Esta tarjeta recibe la información, la traduce para que la PC pueda entender y la envía a la PC.

Son ocho las funciones de la NIC:

1. Comunicaciones de host a tarjeta
2. Buffering
3. Formación de paquetes
4. Conversión serial a paralelo
5. Codificación y decodificación
6. Acceso al cable
7. Saludo



8. Transmisión y recepción.

Estos pasos hacen que los datos de la memoria de una computadora pasen a la memoria de otra.

Cableado. *La LAN debe tener un sistema de cableado que conecte las estaciones de trabajo individuales con los servidores de archivos y otros periféricos. Si sólo hubiera un tipo de cableado disponible, la decisión sería sencilla. Lo cierto es que hay muchos tipos de cableado, cada uno con sus propios defensores y como existe una gran variedad en cuanto al costo y capacidad, la selección no debe ser un asunto trivial.*

Cable de par trenzado: Es con mucho, el tipo menos caro y más común de medio de red.

Cable coaxial: Es tan fácil de instalar y mantener como el cable de par trenzado, y es el medio que se prefiere para las LAN grandes.

Cable de fibra óptica: Tiene mayor velocidad de transmisión que los anteriores, es inmune a la interferencia de frecuencias de radio y capaz de enviar señales a distancias considerables sin perder su fuerza. Tiene un costo mayor.

Equipo de conectividad. *Por lo general, para redes pequeñas, la longitud del cable no es limitante para su desempeño; pero si la red crece, tal vez llegue a necesitarse una mayor extensión de la longitud de cable o exceder la cantidad de nodos especificada. Existen varios dispositivos que extienden la longitud de la red, donde cada uno tiene un propósito específico. Sin embargo, muchos dispositivos incorporan las características de otro tipo de dispositivo para aumentar la flexibilidad y el valor.*



Hubs o concentradores: Son un punto central de conexión para nodos de red que están dispuestos de acuerdo a una topología física de estrella.

Switch. Los conmutadores utilizan la información de la dirección de cada paquete (TCP/IP) para controlar el flujo del tráfico de la red. Por medio de la monitorización de los paquetes que recibe, un conmutador distingue qué dispositivos están conectados a sus puertos, y envía los

paquetes a los puertos adecuados solamente. Un conmutador reduce la cantidad de tráfico innecesario porque la información recibida en un puerto se envía solamente al dispositivo que tiene la dirección de destino correcta.

Repetidores: Un repetidor es un dispositivo que permite extender la longitud de la red; amplifica y retransmite la señal de red. Puentes: Un puente es un dispositivo que conecta dos LAN separadas para crear lo que aparenta ser una sola LAN.

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

Compuertas: Una compuerta permite que los nodos de una red se comuniquen con tipos diferentes de red o con otros dispositivos. Podrá tenerse, por ejemplo, una LAN que consista en computadoras compatibles con IBM y otra con Macintosh.

Sistema operativo de red.

Después de cumplir todos los requerimientos de hardware para instalar una LAN, se necesita instalar un sistema operativo de red (Network Operating System, NOS), que administre y coordine todas las operaciones de dicha red. Los sistemas operativos de red tienen una gran variedad de formas y tamaños, debido a que cada organización que los emplea tiene diferentes necesidades. Algunos sistemas operativos se comportan excelentemente en redes pequeñas, así como otros se especializan en conectar muchas redes pequeñas en áreas bastante amplias.

Los servicios del NOS realiza son:

Soporte para archivos: Esto es, crear, compartir, almacenar y recuperar archivos, actividades esenciales en que el NOS se especializa proporcionando un método rápido y seguro.

Comunicaciones: Se refiere a todo lo que se envía a través del cable. La comunicación se realiza cuando, por ejemplo, alguien entra a la red, copia un archivo, envía correo electrónico, o imprime.

Servicios para el soporte de equipo: Aquí se incluyen todos los servicios especiales como impresiones, respaldos en cinta, detección de virus en la red, etc.

zotero



Zotero: Guía básica

1

I. Características principales

A. ¿Qué es Zotero?

Zotero es un gestor o manejador de referencias bibliográficas, de acceso libre, que trabaja como una extensión del navegador Firefox. Permite a los usuarios crear su propia base de datos (biblioteca) donde puedes: guardar, manejar, buscar, organizar y citar fuentes de todo tipo. Zotero reside en el navegador Firefox, aunque la versión Standalone Alpha (desktop) funciona con los navegadores Safari y Chrome mediante un plugin.

B. Requisitos

OS/Linux/Windows

Es conveniente tener instalado en la computadora los siguientes programas:

- Firefox <http://www.mozilla.com/en-US/products/download.html> (excepto con versión Standalone)*
- Zotero <http://www.zotero.org/>
- Plugin para procesador de palabras (Open Office, MS Word, Word Perfect, etc.)*
http://www.zotero.org/support/word_processor_plugin_installation

*Standalone Alpha funciona como una aplicación independiente en el desktop, por lo que puede utilizarse con Safari y Chrome. Sin embargo, los plugins para esta versión están en desarrollo; no podrá apreciar todas las funciones de inmediato. Con esta versión no necesitará descargar plugins adicionales, pues se incluyen en el paquete. Si tiene ambas versiones instaladas en la computadora, los cambios efectuados en una se registrarán en la otra una vez abra la aplicación. No puede tener ambas versiones abiertas a la vez.

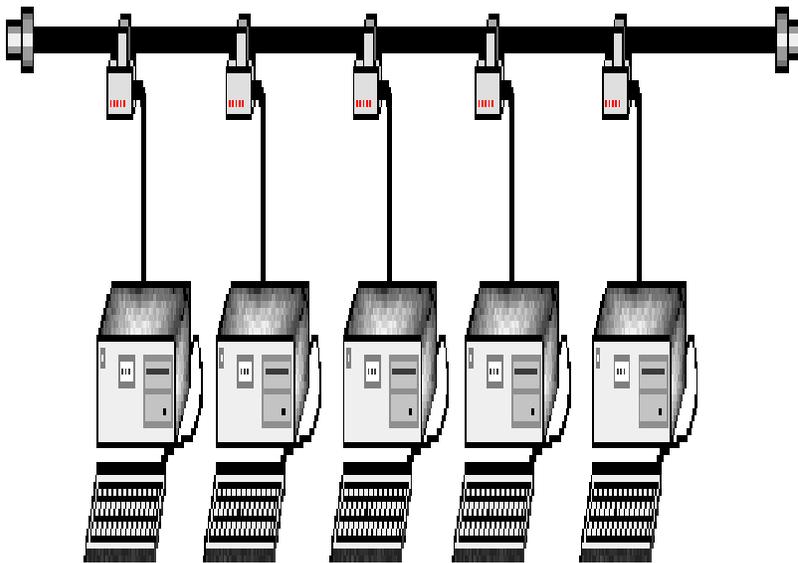
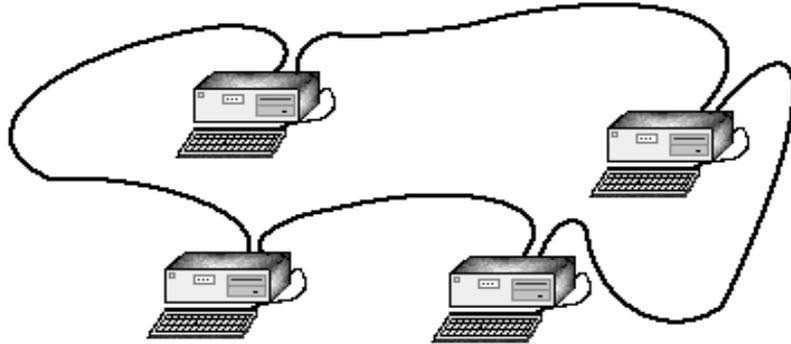
3.5 TOPOLOGÍA DE RED.

La **topología de red** se define como la cadena de comunicación usada por los nodos que conforman una red para comunicarse.

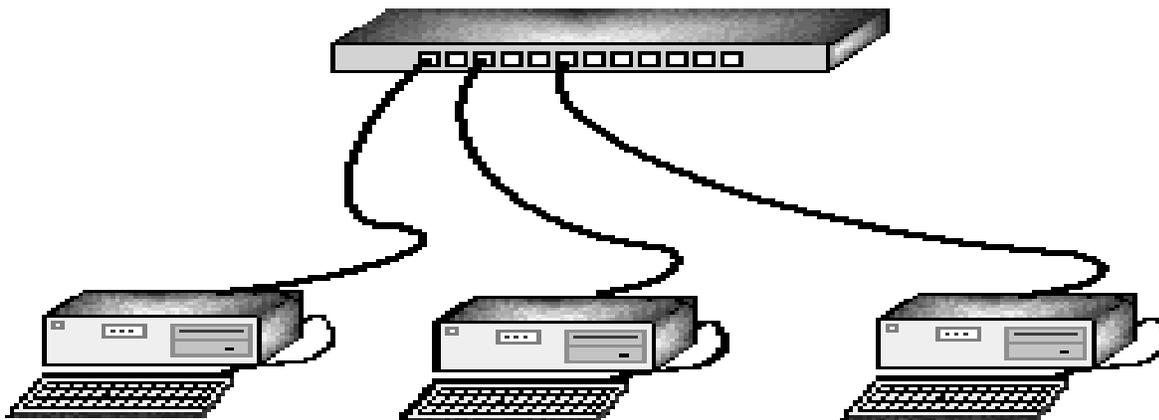
Un ejemplo claro de esto es la topología de árbol, la cual es llamada así por su apariencia estética, por la cual puede comenzar con la inserción del servicio de internet desde el proveedor, pasando por el router, luego por un switch y este deriva a otro switch u otro router o sencillamente a los hosts (estaciones de trabajo), el resultado de esto es una red con apariencia de árbol porque desde el primer router que se tiene se ramifica la distribución de internet dando lugar a la creación de nuevas redes o subredes tanto internas como externas.

Además de la topología estética, se puede dar una topología lógica a la red y eso dependerá de lo que se necesite en el momento. En algunos casos se puede usar la palabra arquitectura en un sentido relajado para hablar a la vez de la disposición física del cableado y de cómo el protocolo considera dicho cableado. Así, en un anillo con una MAU podemos decir que tenemos una topología en anillo, o de que se trata de un anillo con topología en estrella. La topología de red la determina únicamente la configuración de las conexiones entre nodos. La distancia entre los nodos, las interconexiones físicas, las tasas de transmisión y los tipos de señales no pertenecen a la topología de la red, aunque pueden verse afectados por la misma.

Anillo. Tipo de LAN en la que los ordenadores o nodos están enlazados formando un círculo a través de un mismo cable. Las señales circulan en un solo sentido por el círculo, regenerándose en cada nodo. En la práctica, la mayoría de las topologías lógicas en anillo son en realidad una topología física en estrella.

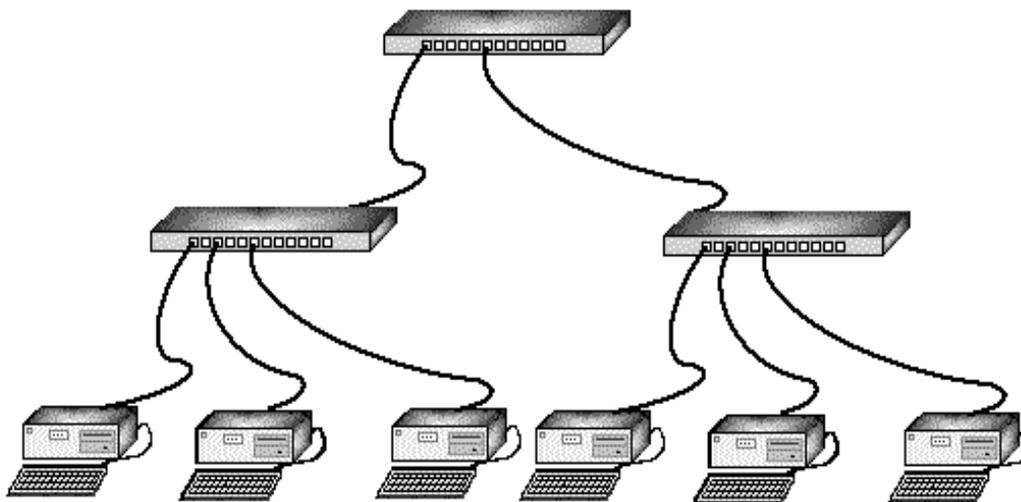


Bus. Una topología de bus consiste en que los nodos se unen en serie con cada nodo conectado a un cable largo o bus, formando un único segmento. A diferencia del anillo, el bus es pasivo, no se produce regeneración de las señales en cada nodo. Una rotura en cualquier parte del cable causará, normalmente, que el segmento entero pase a ser inoperable hasta que la rotura sea reparada. Como ejemplos de topología de bus tenemos 10BASE-2 y 10BASE-5.



Estrella. Lo más usual en ésta topología es que en un extremo del segmento se sitúe un nodo y el otro extremo se termine en una situación central con un concentrador. La principal ventaja de este tipo de red es la fiabilidad, dado que, si uno de los segmentos tiene una rotura, afectará sólo al nodo conectado en él. Otros usuarios de los ordenadores de la red continuarán operando como si ese segmento no existiera. 10BASE-T Ethernet y Fast Ethernet son ejemplos de esta topología.

Árbol. A la interconexión de varias subredes en estrella se le conoce con el nombre de topología en **árbol**.



Reporte de resultados de la práctica	
Nombre de la práctica	

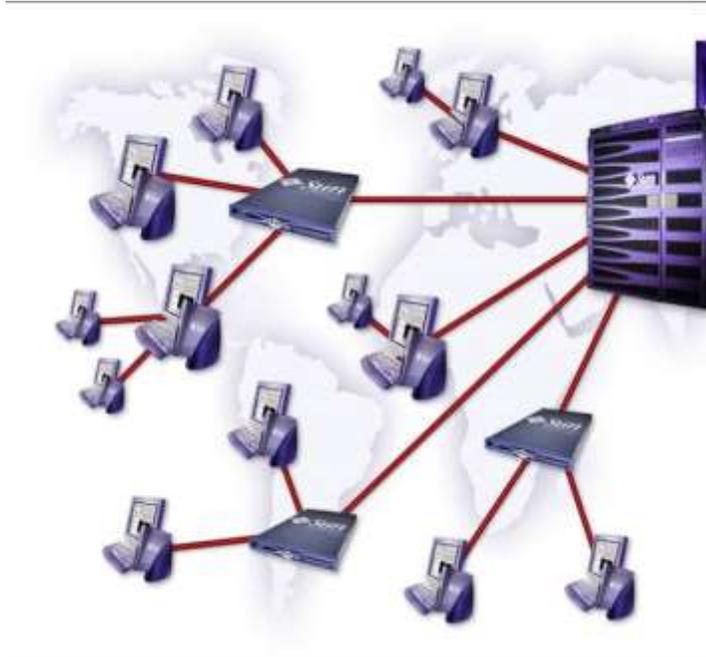
Competencia que a desarrollar según el programa			
La práctica la realicé de manera:	Grupal	Individual	Fecha de realización
Desempeños que debo mostrar			
El producto obtenido en la práctica es:			
Lo que aprendí con la práctica			
Indicadores de la competencia que trabajé			
Dónde puedo aplicar lo aprendido			
Con qué contenidos de otras unidades de aprendizaje se relaciona			
En dónde encontré información complementaria para trabajar la práctica			
Cómo seleccioné la información utilizada			
Criterios con los que me evaluaron			
Qué más me gustaría aprender sobre el tema			

TEMA 4.0: ARMADO DE CABLE DE RED.

- ✓ 4.1 Tipos de cable de red
- ✓ 4.2 Protocolo de cable de red
- ✓ 4.3 Armado de un cable de red

4.1 TIPOS DE CABLE DE RED.

En el mercado existen cables de red de varias medidas ya hechos, pero en ocasiones necesitamos hacerlo nosotros, bien porque no haya la medida que necesitamos o bien porque necesitemos pasarlo a través de paredes y tubos. El UTP, con la especificación 10BaseT, es el tipo más conocido de cable de par trenzado y ha sido el cableado LAN más utilizado en los últimos años. El segmento máximo de longitud de cable es de 100 metros.



El cable UTP tradicional consta de dos hilos de cobre aislados. Las especificaciones UTP dictan el número de entrelazados permitidos por pie de cable; el número de entrelazados depende del objetivo con el que se instale el cable. La especificación 568A Commercial Building Wiring Standard de la Asociación de Industrias Electrónicas e Industrias de la Telecomunicación (EIA/TIA) especifica el tipo de cable UTP que se va a utilizar en una gran variedad de situaciones y construcciones. El objetivo es asegurar la coherencia de los productos para los clientes. Estos estándares definen cinco categorías de UTP:

- **Categoría 1.** Hace referencia al cable telefónico UTP tradicional que resulta adecuado para transmitir voz, pero no datos. La mayoría de cables telefónicos instalados antes de 1983 eran de estos.
- **Categoría 2.** Esta categoría certifica el cable UTP para transmisión de datos de hasta 4 megabits por segundo (mbps), Este cable consta de cuatro pares trenzados de hilo de cobre.
- **Categoría 3.** Esta categoría certifica el cable UTP para transmisión de datos de hasta 16 mbps. Este cable consta de cuatro pares trenzados de hilo de cobre con tres entrelazados por pie.
- **Categoría 4.** Esta categoría certifica el cable UTP para transmisión de datos de hasta 20 mbps. Este cable consta de cuatro pares trenzados de hilo de cobre.
- **Categoría 5.** Esta categoría certifica el cable UTP para transmisión de datos de hasta 100 mbps. Este cable consta de cuatro pares trenzados de hilo de cobre.

- **Categoría 5a.** También conocida como Categoría 5+ o Cat5e. Ofrece mejores prestaciones que el estándar de Categoría 5. Para ello se deben cumplir especificaciones tales como una atenuación a la ratio crosstalk (ARC) de 10 dB a 155 Mhz y 4 pares para la comprobación del Power Sum NEXT. Este estándar todavía no está aprobado.

- **Nivel 7.** Proporciona al menos el doble de ancho de banda que la Categoría 5 y la capacidad de soportar Gigabit Ethernet a 100 m. El ARC mínimo de 10 dB debe alcanzarse a 200 Mhz y el cableado debe soportar pruebas de Power Sum NEXT, más estrictas que las de los cables de Categoría 5 Avanzada.

La mayoría de los sistemas telefónicos utilizan uno de los tipos de UTP. De hecho, una razón por la que UTP es tan conocido es debido a que muchas construcciones están preparadas para sistemas telefónicos de par trenzado. Como parte del proceso previo al cableado, se instala UTP extra para cumplir las necesidades de cableado futuro.

Si el cable de par trenzado preinstalado es de un nivel suficiente para soportar la transmisión de datos, se puede utilizar para una red de equipos. Sin embargo, hay que tener mucho cuidado, porque el hilo telefónico común podría no tener entrelazados y otras características eléctricas necesarias para garantizar la seguridad y nítida transmisión de los datos del equipo.



La intermodulación es un problema posible que puede darse con todos los tipos de cableado (la intermodulación se define como aquellas señales de una línea que interfieren con las señales de otra línea.)

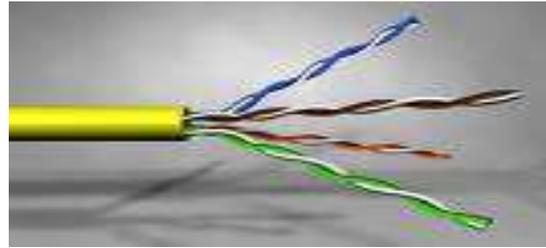
UTP es particularmente susceptible a la intermodulación, pero cuanto mayor sea el número de entrelazados por pie de cable, mayor será la protección contra las interferencias.

4.2 PROTOCOLO DE CABLE DE RED.

CABLE DE RED TRENZADO (CABLE UTP).

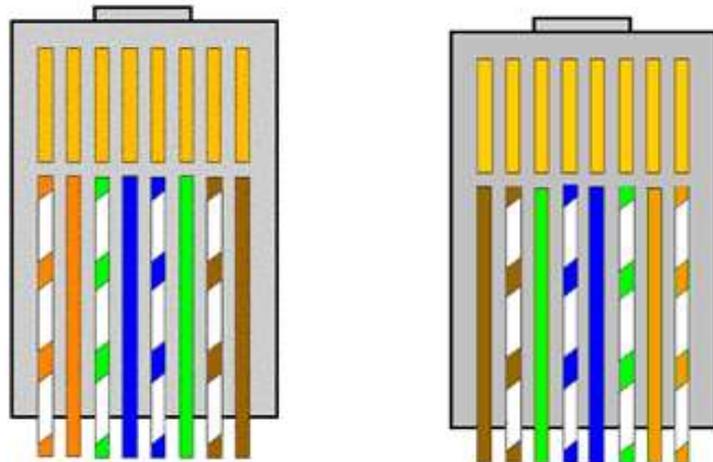
Es el cable que se utiliza para conexiones de red. Puede ser de varios tipos y categorías, siendo el más empleado el de categoría 5 (C5), a ser posible blindado. Tiene en su interior 4 pares de cables trenzados y diferenciados por colores (blanco naranja, naranja, blanco verde, verde, blanco azul, azul y blanco marrón y marrón).

Lo podemos comprar por metros o en bobinas de 100 y 300 metros. Es importante recordar que la longitud máxima de un cable de red no debe exceder de los 90 metros.



Vamos a numerar los hilos:

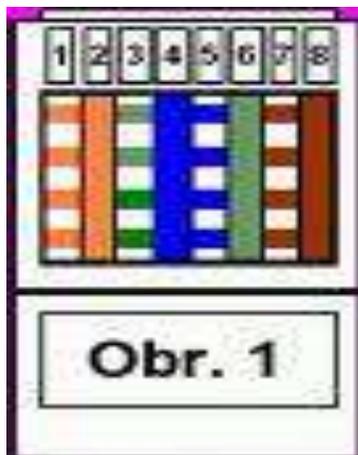
- 1 Blanco – Naranja
- 2 Naranja
- 3 Blanco – verde
- 4 Verde
- 5 Blanco – Azul
- 6 Azul
- 7 Blanco – Marrón
- 8 Marrón



El orden estándar de colocación de los hilos, siempre con la pestaña del conector hacia abajo, sería:

Estándar 568-B: 1-2-3-5-6-4-7-8, correspondiendo estos números al orden indicado en cable de red.

Estándar 568-A: 3-4-1-5-6-2-7-8, correspondiendo estos números al orden indicado en cable de red.



Distribuciones de hijos 568-B (Obr. 1) y 568-A (Obr. 2).

Es importante mantener este orden porque si necesitamos que en uno de los extremos vaya una roseta pared RJ45 en vez de un terminal RJ45, estas rosetas vienen señaladas siguiendo este orden.

TERMINALES RJ45.



Imagen de terminales RJ45. El superior es normal y el inferior es blindado.

Varios tipos de protectores de terminales.

Imagen de roseta de pared para dos salidas RJ45.



Es un terminal similar a los de conexión telefónica (RJ11), pero de 11 mm de longitud por 7 mm de grosor, con 8 hilos en vez de 4 ó 6 de los terminales de teléfono. Aunque tanto los terminales RJ45 como los cables de red tienen 8 hilos, para las funciones de red solo se utilizan los pares 1 - 2 y 3 - 6.

Los terminales RJ45 pueden ser blindados o sin blindar. Para longitudes mayores de 10 metros es aconsejable utilizar los blindados. También venden protectores para los terminales, que darán un mejor aspecto a nuestro trabajo y, además, si tenemos varios cables, nos ayudarán a identificarlos.

También podemos poner en uno de los extremos una roseta RJ45. Estas rosetas pueden ser de muy diferentes tipos (empotrable, de superficie, con un terminal o con varios). Para un correcto funcionamiento, en el caso de que pongamos una roseta con varios conectores deberemos tirar un cable para cada conector.



CRIMPADORA.

Crimpadora mixta (RJ11 y RJ45) metálica de PVC.



Crimpadora mixta (RJ9, RJ11 y RJ45)

Imprescindible para poder hacer un cable de red. Se trata de una especie de tenaza que utilizamos para cerrar los conectores y crisar los cables correspondientes. La que aparece en la foto superior es una crimpadora de tipo profesional, pero las hay más económicas, fabricadas en PVC (foto inferior). Las más recomendables son las que tienen para varios tipos de clavijas (RJ9, RJ11 y RJ45), ya que en una sola herramienta tendremos la posibilidad de crisar tanto cables de red como de teléfono. Una vez que ya tenemos el material que necesitamos, vamos por la fabricación. En primer lugar, y con mucho cuidado para no dañar los cables interiores, cortaremos aproximadamente cuatro centímetros de la funda del cable y dejaremos al descubierto los pares de hilos. A continuación, procederemos a desenlazar los pares y a colocarlos en el orden correspondiente al estándar que necesitemos (568-B o 568-A). Los cortamos a una longitud aproximada de un centímetro manteniendo el orden de los hilos y los introducimos en el terminal RJ45, manteniendo este con la uñeta de sujeción hacia abajo. Una vez introducidos los hilos y comprobado que están en el orden correcto, que llegan hasta el fondo del terminal y que el cuerpo del cable queda en el interior del conector (tal como muestra la fotografía) lo introducimos en la crimpadora y procedemos a crisararlo apretando con fuerza y comprobando que queda perfectamente sujeto.



Repetimos esta operación en el otro extremo del cable y ya tenemos hecho nuestro cable de red.

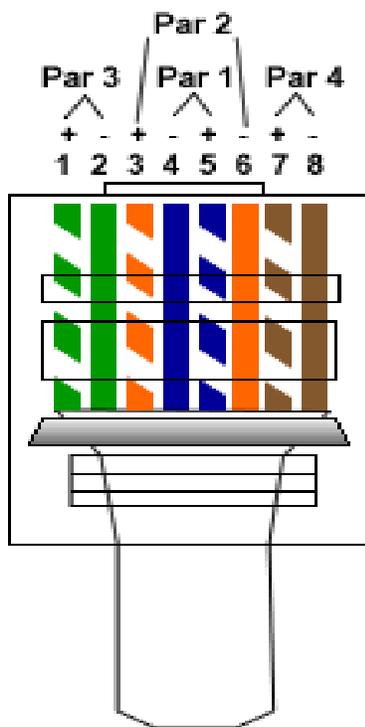
TIPOS DE CABLES DE RED:

Cable Recto: Las dos fichas RJ-45 irán colocadas a los extremos del cable, respetando la siguiente tabla de valores:

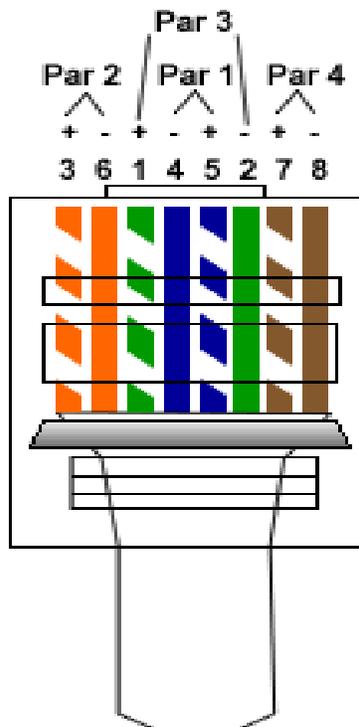
Para usar con un HUB o SWITCH		
Extremo 1	Pin a pin	Extremo 2
1  Naranja y blanco	Pin 1 a Pin 1	1  Naranja y blanco
2  Naranja	Pin 2 a Pin 2	2  Naranja
3  Verde y blanco	Pin 3 a Pin 3	3  Verde y blanco
4  Azul	Pin 4 a Pin 4	4  Azul
5  Azul y blanco	Pin 5 a Pin 5	5  Azul y blanco
6  Verde	Pin 6 a Pin 6	6  Verde
7  Marrón y blanco	Pin 7 a Pin 7	7  Marrón y blanco
8  Marrón	Pin 8 a Pin 8	8  Marrón

- **Cable Cruzado:** si nuestro objetivo es conectar dos PC's, esta es la forma de crear el cable para poder evitar la utilización de un Hub.

Conexión directa PC a Pc o Entre Hubs, switchs, etc.		
Extremo 1	Pin a pin	Extremo 2
1  Naranja y blanco	Pin 1 a Pin 3	1  Verde y Blanco
2  Naranja	Pin 2 a Pin 6	2  Verde
3  Verde y blanco	Pin 3 a Pin 1	3  Naranja y blanco
4  Azul	Pin 4 a Pin 4	4  Azul
5  Azul y blanco	Pin 5 a Pin 5	5  Azul Blanco
6  Verde	Pin 6 a Pin 2	6  Naranja
7  Marrón y blanco	Pin 7 a Pin 7	7  Marrón y blanco
8  Marrón	Pin 8 a Pin 8	8  Marrón



Norma T568A



Norma T568B

- Par 1 + Azul-blanco
- Azul
- Par 2 + Naranja-blanco
- Naranja
- Par 3 + Verde-blanco
- Verde
- Par 4 + Cafe-blanco
- Cafe

En lo que respecta a normas se tienen las siguientes convenciones:

- **Cable Recto:** extremo 1 = Norma A y extremo 2 = Norma A o extremo 1 = Norma B y Extremo 2 = Norma B.
 - **Cable Cruzado:** extremo 1= Norma A y extremo2= Norma B.
- La norma B suele ser la más utilizada.

4.3 ARMADO DE UN CABLE DE RED



Paso 1.



Paso 2.



Paso 3.



Paso 4.



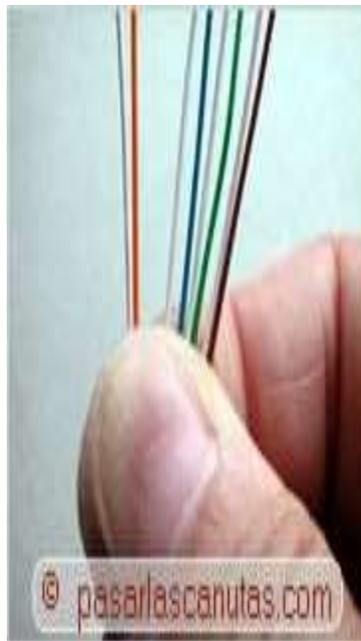
Paso 5.



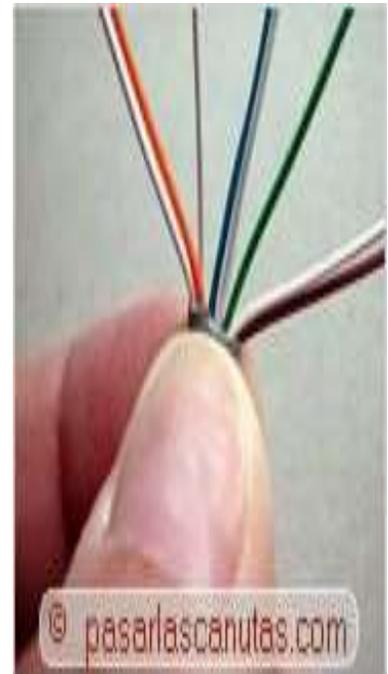
Paso 6.



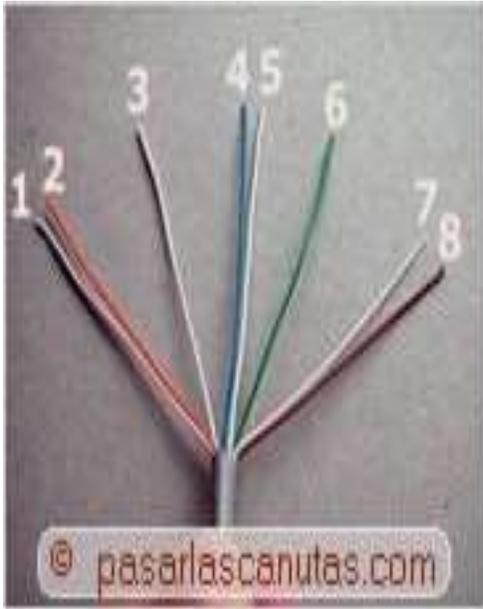
Paso 7.



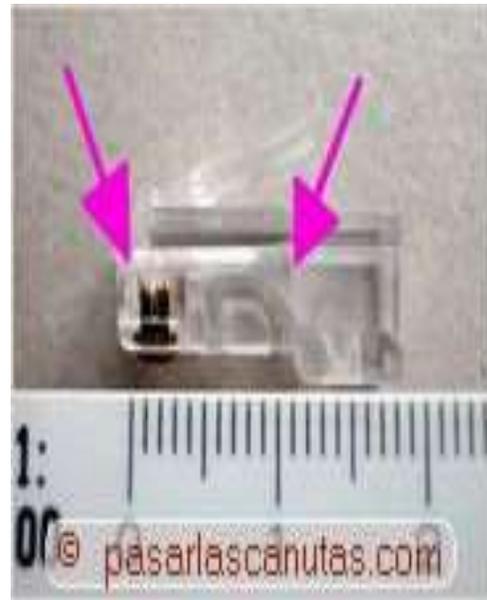
Paso.8



Paso 9.



Paso 10.



Paso 11



Paso12.



Paso 13.



Paso 14.



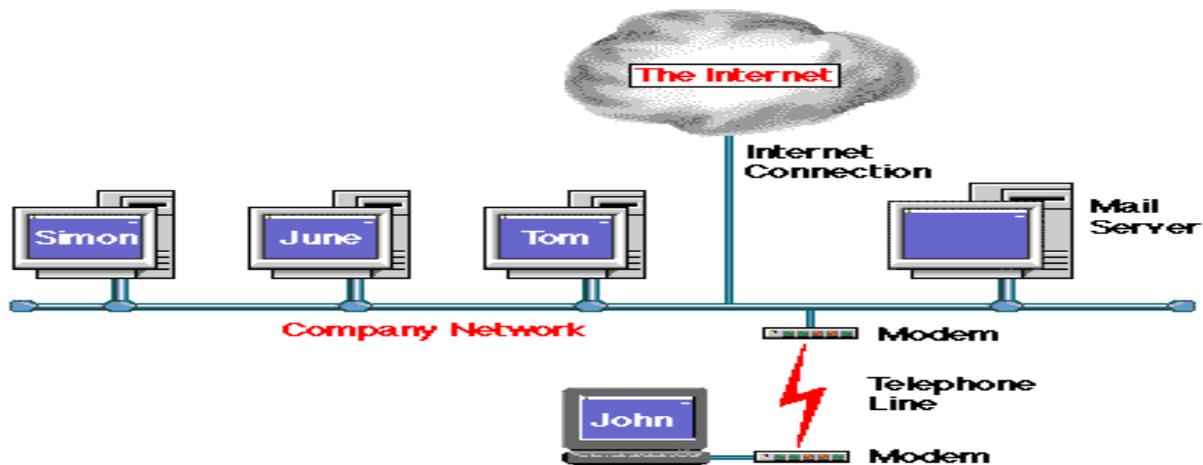
Paso 15.

Reporte de resultados de la práctica			
Nombre de la práctica			
Competencia que a desarrollar según el programa			
La práctica la realicé de manera:	Grupal	Individual	Fecha de realización
Desempeños que debo mostrar			
El producto obtenido en la práctica es:			
Lo que aprendí con la práctica			
Indicadores de la competencia que trabajé			
Dónde puedo aplicar lo aprendido			
Con qué contenidos de otras unidades de aprendizaje se relaciona			
En dónde encontré información complementaria para trabajar la práctica			
Cómo seleccioné la información utilizada			
Criterios con los que me evaluaron			
Qué más me gustaría aprender sobre el tema			

TEMA 05: ESTRUCTURADO DE UNA RED

- ✓ 5.1 Topología de una red de área Local (Lan)
- ✓ 5.2 Cableado e instalación de equipos en la Red
- ✓ 5.3 Configuración lógica (Protocolos y Direcciones IP)
- ✓ 5.4 Pruebas de comunicación (IPConfig y Ping)

5.1 TOPOLOGÍA DE UNA RED DE ÁREA LOCAL (LAN).



Topología:

Es simplemente visualizar el sistema de comunicación en una red es conveniente utilizar el concepto de topología, o estructura física de la red. Las topologías describen la red físicamente y también nos dan información acerca del método de acceso que se usa (Ethernet, Token Ring, etc.).

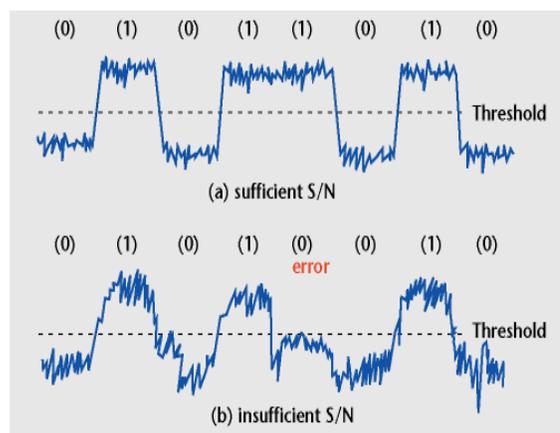
Posibles problemas que presenta una Red a raíz de una mala configuración en los Equipos establecidos:

Perdida de las Datos.

La pérdida de datos es producida por algún virus o por otro tipo de incidencia, los más 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.

Caídas Continuas de la Red.

La caída continua en una Red se debe en la mayoría de los casos a una mala conexión Servidor > Concentrador o la conexión existente con el proveedor de Internet.



En 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.

Alcance.

La norma EIA/TIA 568A especifica los requerimientos mínimos para el cableado de establecimientos comerciales de oficinas. Se hacen recomendaciones para:

- Las topologías
- La distancia máxima de los cables
- El rendimiento de los componentes
- Las tomas y los conectores de telecomunicaciones

Se pretende que el cableado de telecomunicaciones especificado soporte varios tipos de edificios y aplicaciones de usuario. Se asume que los edificios tienen las siguientes características:

- Una distancia entre ellos de hasta 3 Km.
- Un espacio de oficinas de hasta 1,000,000 m²
- Una población de hasta 50,000 usuarios individuales

Las aplicaciones que emplean los sistemas de cableado de telecomunicaciones incluyen, pero no están limitadas a:

Voz, Datos, Texto, Video, Imágenes

La vida útil de los sistemas de cableado de telecomunicaciones especificados por esta norma debe ser mayor de 10 años.

Las normas EIA/TIA es una de las mejores Normas por sus Antecedentes que son: Vos, Dato, video, Control y CCTV

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.

Beneficios.

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

Diseñar la Red.

Dibuje un diagrama de la casa o la oficina donde se encuentra cada equipo e impresora. O bien, puede crear una tabla donde figure el hardware que hay en cada equipo.

Determinar qué tipo de Hardware tiene cada equipo, en caso de usar equipos ya establecidos en la empresa u oficina. Junto a cada equipo, anote el hardware, como módems y adaptadores de red, que tiene cada equipo.

Elegir el servidor o (HOST) determinado para la conexión con las estaciones de trabajo. Elija el equipo HOST para Conexión compartida a Internet.

Determinar el tipo de adaptadores de Red, que necesita para su Red doméstica o de oficina. Determine el tipo de adaptadores de red que necesita para su red doméstica o de pequeña oficina.

Escribe una lista del hardware que necesita comprar. Aquí se incluyen módems, adaptadores de red, concentradores y cables. Haga una lista del hardware que necesita comprar. Aquí se incluyen módems, adaptadores de red, concentradores y cables.

Medición del espacio entre las Estaciones de Trabajo y El servidor. En este espacio se medirá las distancias que existe entre las Estaciones de Trabajo y el Servidor (HOST), con un Metro, esto se hace para evitar excederse en los metros establecidos para dicha construcción.

5.2 Cableado e instalación de equipos en la red.

1. Colocación de las canaletas Plástica. Para la colocación de las canaletas plástica simplemente tomaremos las medidas establecidas, Cortaremos las Canaletas, Colocaremos los Ramplus en la Pared y Atornillaremos las Canaletas Plásticas con los Tornillos Tira fondo.

2. Medición del Cableado. En esta parte haremos el mismo procedimiento que con las Canaletas, Tomaremos las medidas del Cableado para evitar el exceso de Cables entre la Estaciones de Trabajo.

3. Elaboración del cable de red. De acuerdo a la topología planteada se procede a elaborar los cables requeridos.

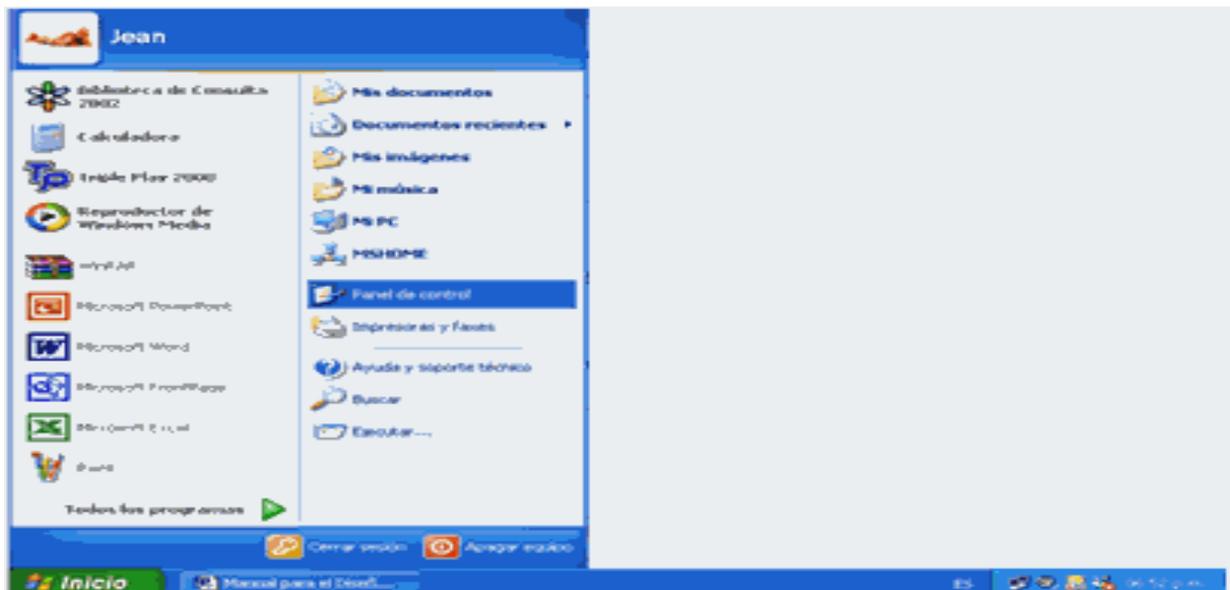
4. Interconexión de equipos y cables de la red. En este paso se procede a conectar los equipos como lo indica la topología elaborada.

5.3 Configuración Lógica (Protocolos y Direcciones IP).

Primero examinaremos las normativas ya que esto es indispensable para el buen funcionamiento de la Red.

Configuración de las Tarjetas de Red:

Para la conexión de la tarjeta de Red comenzaremos con el primer paso, Daremos un clic en la Barra del Menú de **Inicio**. Ubicamos el puntero del Mouse en la solapa de **Panel de Control** y



damos un clic. A Continuación, ubicaremos el Icono de Agregar Nuevo Hardware, Aremos un doble clic para Abrir el Menú Agregar Nuevo Hardware.

De allí en adelante sigue los procedimientos que te indica el Computador.

Nota: Actualmente las nuevas Plataformas de Windows detectan Automáticamente las Tarjetas de Red no hace falta configurarlas a menos que dicha plataforma no contenga el Controlador Requerido para dicha Tarjeta.

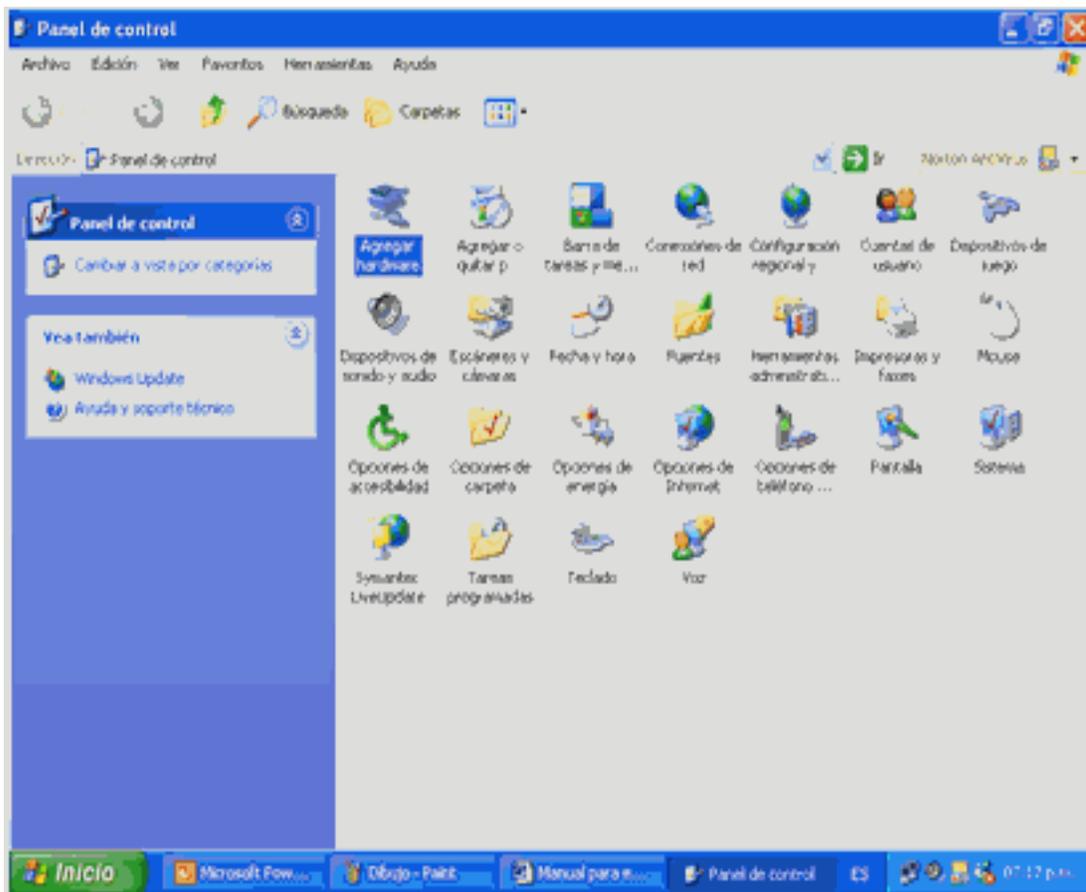
Configuración del HOST a Internet:

Para la conexión del Servidor a la Gran Red (Internet), debemos realizar los siguientes pasos:

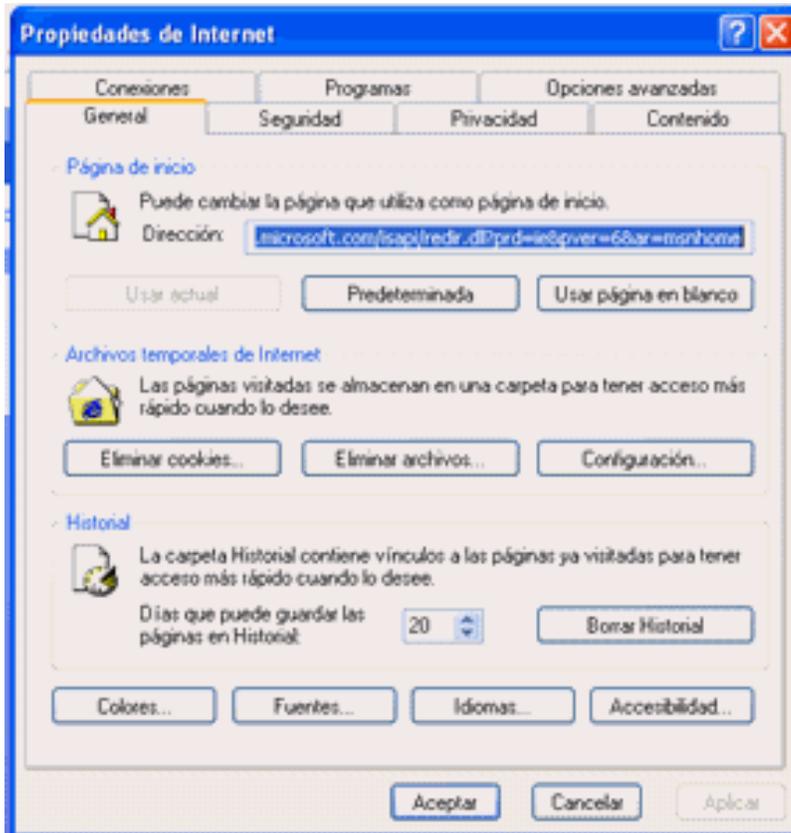
- 1 – Dar un Clic en el Botón Inicio
- 2 – Ubicarnos sobre Panel de Control, daremos doble clic
- 3 – Una vez allí nos posicionaremos sobre el Icono **Opciones de Internet**, daremos doble clic
- 4 – Luego saldrá una pequeña Ventana, ubícate sobre la solapa que dice; **Conexiones**.

Daremos doble clic, Aparecerá otra pantalla que te pedirá la Información de la Ubicación.

□

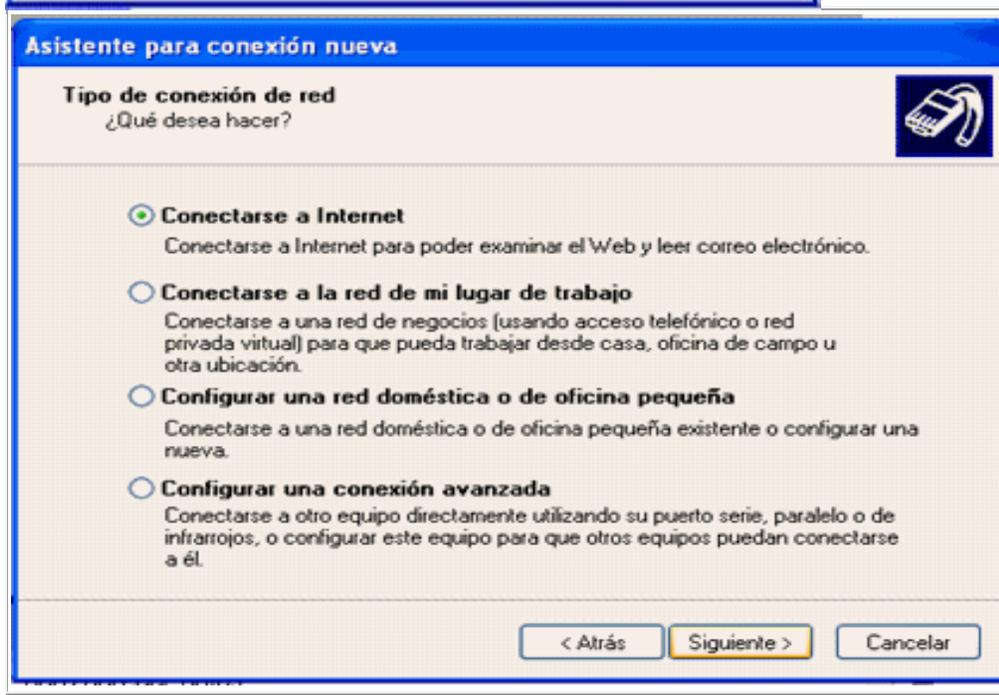


Luego de haber completado el cuadro de dialogo daremos un clip en Aceptar para continuar con la Instalación.





El siguiente cuadro te muestra las diferentes conexiones que puedes utilizar, le daremos un clip en Siguiete.



En este espacio te dará cuatro Opciones que son:

1. Conectarse a Internet
2. Conectarse a la Red de mi lugar de Trabajo
3. Configurar una Red doméstica o de Oficina pequeña

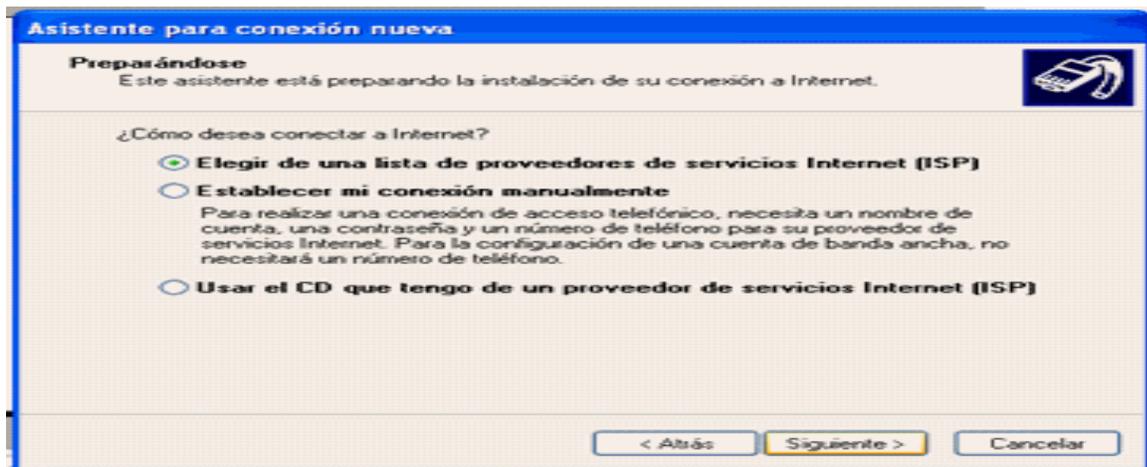
4. Configurar una Conexión Avanzada

Solamente tomaremos la primera Opción que es **Conectarse a Internet**

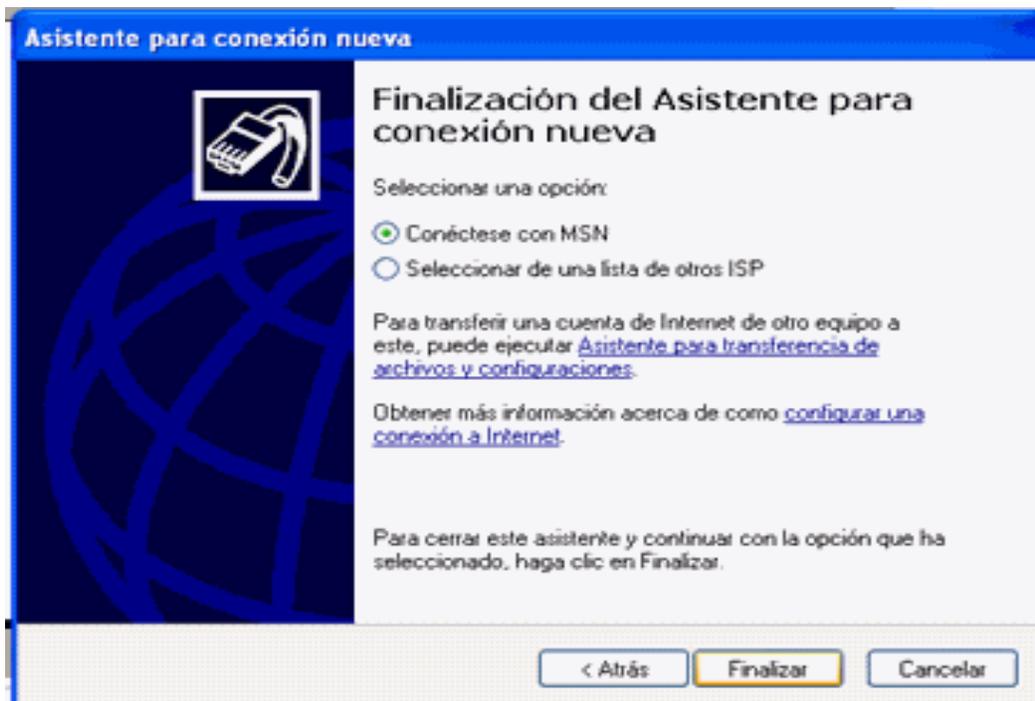
La siguiente parte es fundamental ya que la serie de opciones son de vital importancia, te dará tres opciones que son las siguientes.

1. Elegir una lista de proveedores de Servicios de Internet
2. Establecer mi Conexión Manualmente
3. Usar el CD que tengo de un proveedor de servicios Internet (ISP).

Recordemos que esto es según el servicio que tengas disponible.

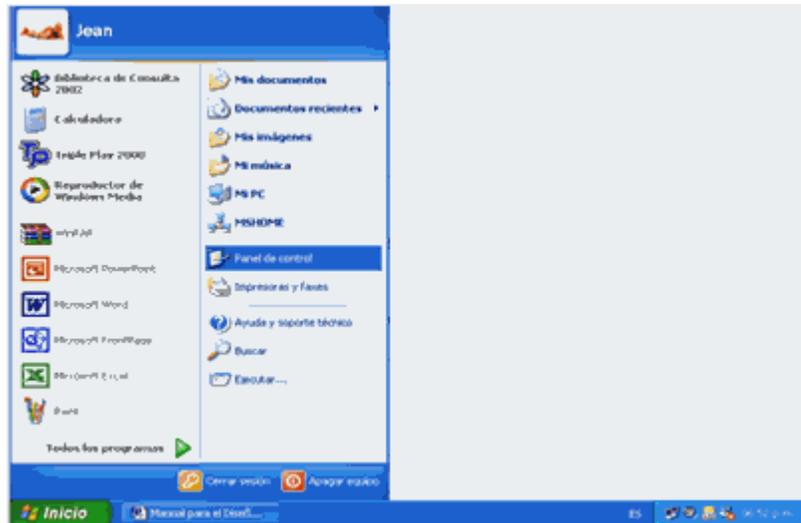


Luego de haber tomado la decisión daremos un Clic en Siguiete para continuar con la conexión.

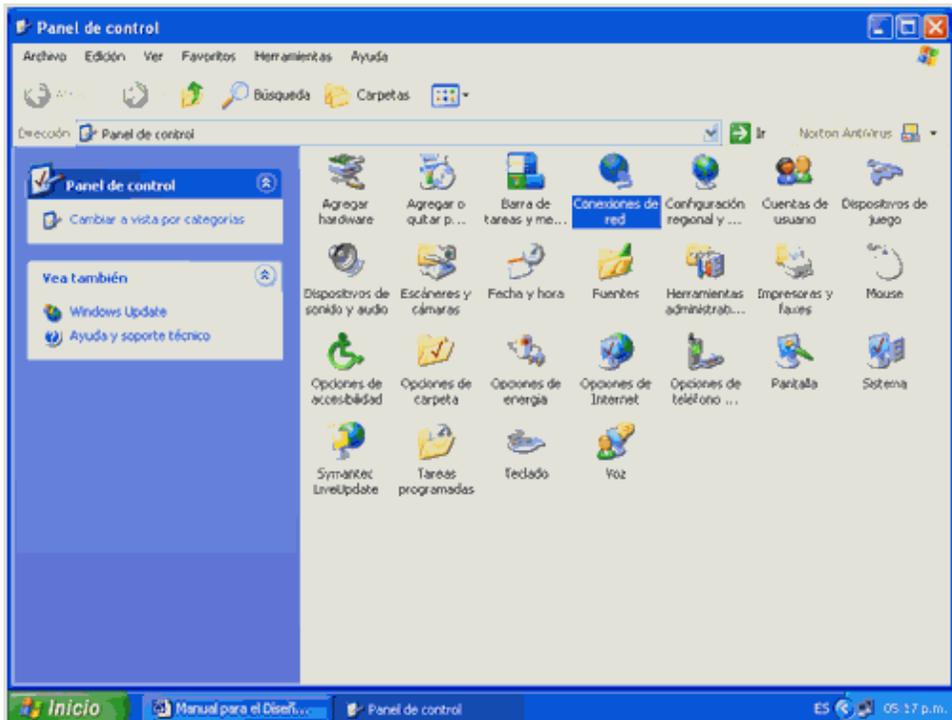


Luego que aparezca el siguiente cuadro daremos un clic en finalizar Instalación para terminar. **Configuración del Servidor (HOST), Dirección IP, Mascara de Subred, Puerta de Enlace e Internet:** La configuración de HOST es muy sencilla solamente de vemos proporcionar algunos códigos o protocolos que nos exige el computador para comenzar a programar nuestro servidor, así como las Estaciones de trabajo. Seamos muy cuidadosos ya que un pequeño error nos costaría mucho tiempo y un mal funcionamiento, podría traer graves consecuencias como un (Colapso). A continuación, abriremos en la barra de menú Inicio daremos un Clic en la Solapa de Panel de Control.

Barra del Menú Inicio

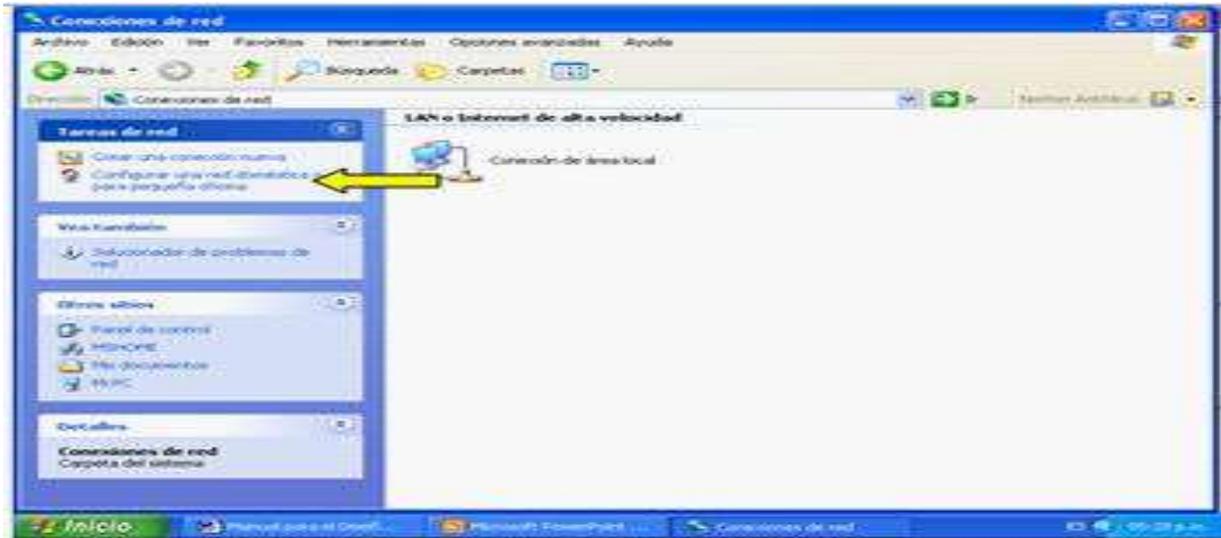


Una vez hecho esto ubicaremos el Icono de Conexiones de Red. Daremos doble clic. **Panel de Control**



Bien, nos enfocaremos en la parte superior izquierda de la pantalla, en un Icono llamado configurar una Red doméstica o para Oficina. Nos posicionaremos sobre este Icono y daremos doble click sobre el mismo.

Ventana Conexión de Red

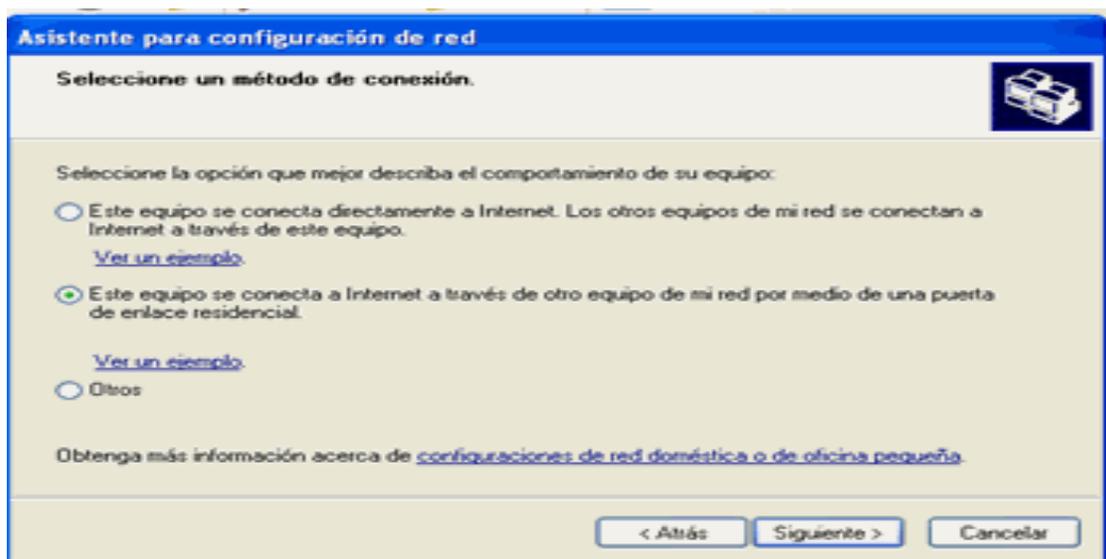


A continuación, seguiremos las instrucciones que nos indique el Ordenador. Luego tendremos una Ventana que nos Preguntara como deseamos conectar el Equipo, tendremos tres opciones.

1. Este equipo se conecta directamente a Internet. Los otros equipos se conectan a Internet a través de mi Equipo.
2. Este Equipo se conecta a Internet a través de otro Equipo de mi Red por medio de una puerta de enlace residencial.
3. Otros

Solo y solamente tomaremos la Primera (1) opción **(Este equipo se conecta directamente a Internet. Los otros equipos se conectan a Internet a través de mi Equipo)**

Ventana para modo de conexión de Red



Hecho esto Continuaremos dando un Clic en el botón siguiente. Aparecerá otra pantalla que dirá que le des Nombre a tu Equipo y lo Describas.

Ventana para la selección de Nombre y Descripción de tu PC

Asistente para configuración de red

Dé a este equipo una descripción y nombre.

Descripción del equipo:
Ejemplos: Equipo de la sala de estar o Equipo de Pablo

Nombre de equipo:
Ejemplos: FAMILIA o PABLO

El nombre actual del equipo es JEAN.

Aprenda más acerca de [Nombres de equipo y descripciones.](#)

< Atrás Siguinte > Cancelar

Hecho esto Continuaremos dando un Clic en el botón siguiente. Aparecerá otra pantalla que te pedirá que le des el Nombre del Grupo de Trabajo o el Nombre que desees como se llame tu Red.

Ventana para el Acceso a Nombre de la Red

□

Asistente para configuración de red

Dé nombre a su red.

Especifique un nombre de grupo de trabajo para su red. Todos los equipos en su red deben tener el mismo nombre de grupo de trabajo.

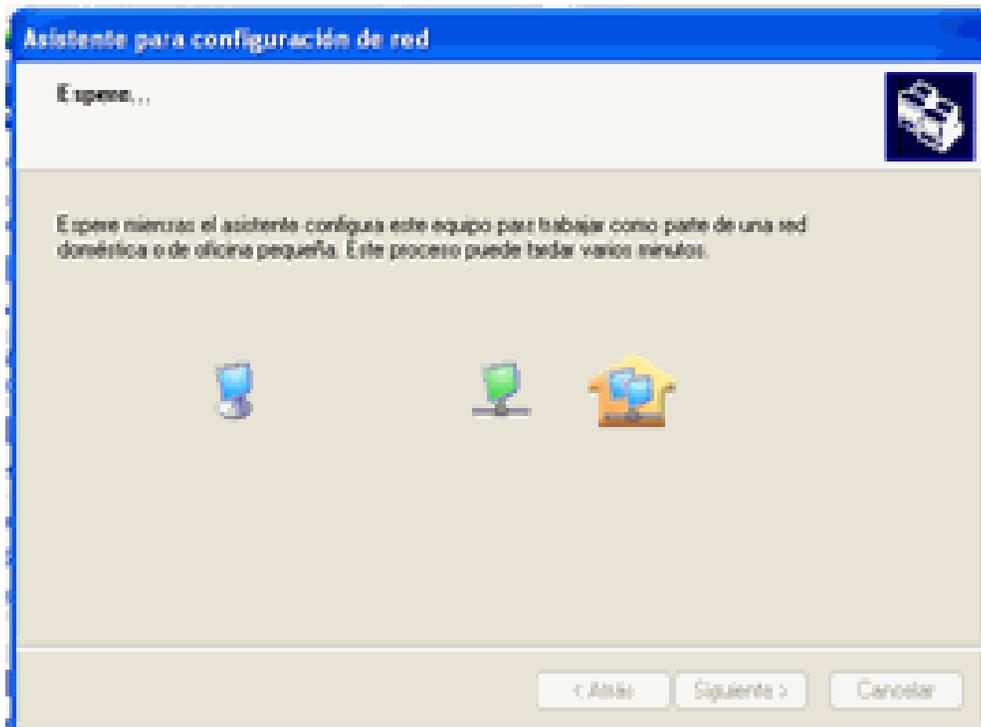
Nombre del grupo de trabajo:
Ejemplos: CASA u OFICINA

< Atrás Siguinte > Cancelar

Una vez que se ha terminado de configurar los datos de ordenador pulsa el botón Siguiente, Tendrás otra pantalla que te proporcionara todos los datos que recientemente configuraste, esto se hace para que verifiques que todos los datos son Aceptables. Una vez confirmado todos los datos pulsaremos el botón siguiente y seguiremos las instrucciones del Ordenador para culminar la instalación del Servidor (HOST)



Después de haber hecho esto saldrá una ventana que dirá que espere eso es porque está terminando de configurar los datos de la Red. Espera no Desesperes puede tardar varios minutos.



Bien luego de que el Ordenador termine de configurar los datos saldrá otra pantalla que te dará una serie de opciones y te preguntara que deseas hacer.

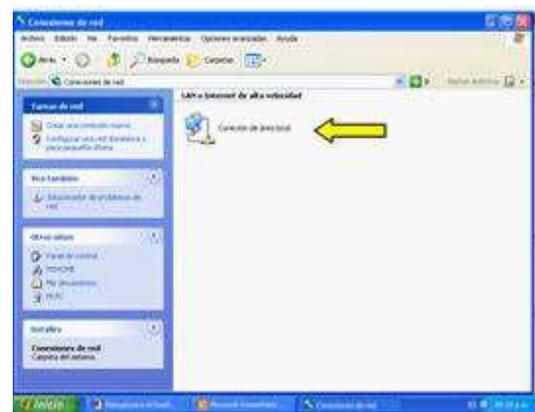


Bien la serie de opciones son las siguientes:

- 1 – Crear un disco de configuración de Red
- 2 – Usar el disco de configuración de Red que tengo
- 3 – Usar mi CD de Windows XP
- 4 – Finalizar el Asistente.

Tomaremos solamente la opción N° 4, **Finalizar el Asistente**

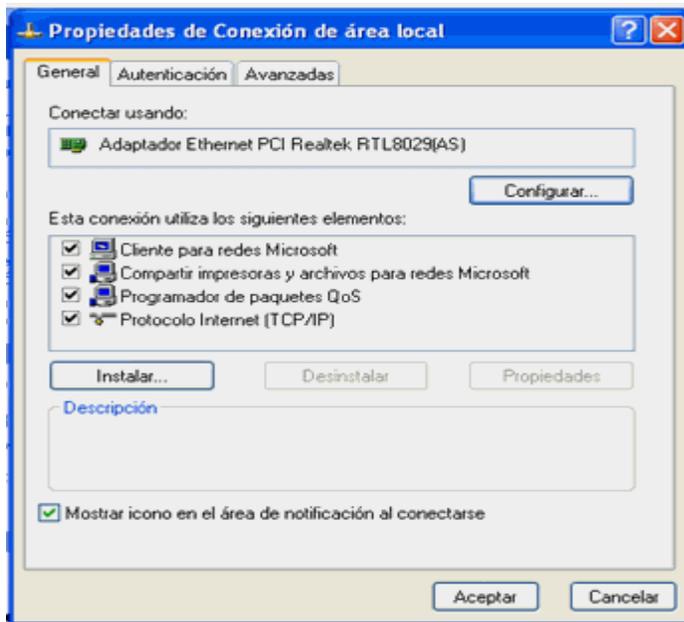
OK; Para la configuración de los protocolos (IP), La máscara de Subred y la Puerta de Enlace, tendremos que abrir la Ventana Conexiones de Red ubicada en el Panel de Control, como ya lo aviamos hecho en la ocasión anterior.



Daremos un Clic con el botón derecho del Mouse en el Icono Conexión de Área Local. Luego de haber hecho esta [función](#) aparecerá una pequeña ventana, que dirá. [Estado de conexión de Área Local](#).



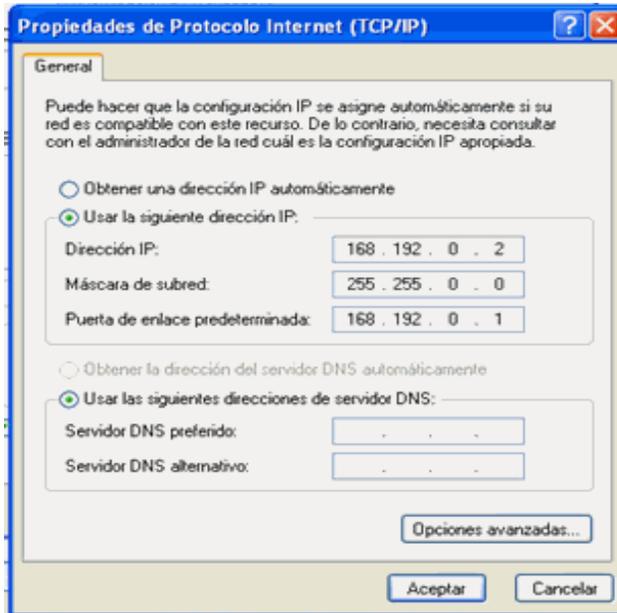
Luego que aparezca esta Ventana, daremos un Clic en el Botón Propiedades ubicado en la parte inferior izquierda de la ventana.



Luego que aparezca esta pantalla Buscaremos la opción que dice. Protocolo Internet (TCP/IP). Nos ubicaremos encima del mismo y a continuación daremos doble Clic.

Una vez que hayamos hecho esto tendremos una pequeña pantalla que dirá. Propiedades de Protocolo Internet (TCP/IP)





Dentro de esta pantalla tendremos la dirección IP, La máscara de Subred y La puerta de Enlace predeterminada. Dentro de estas opciones aremos lo siguiente.

En la dirección IP, aparecerá de Esta forma	<input type="text" value="....."/>
La rellenaremos de esta manera.....	<input type="text" value="168. 192. 0.. 1"/>
La mascara de Subred.....	<input type="text" value="....."/>
Quedara de esta forma.....	<input type="text" value="255. 255. 0.. 0"/>
Puerta de enlace predeterminada.....	<input type="text" value="....."/>
Bien.....	<input type="text" value="168. 192. 0.. 0"/>

Una vez que hayamos terminado de Hacer esta operación podemos proseguir con la configuración de las Estaciones de Trabajo.

Configuración de las Estaciones:

En este espacio debemos ser muy cuidadosos ya que un pequeño error nos costaría mucho tiempo y un mal funcionamiento, podría traer graves consecuencias como un (Colapso). A continuación, abriremos en la barra de menú Inicio daremos un Clic en la Solapa de Panel de Control.

5.4 Pruebas de comunicación.

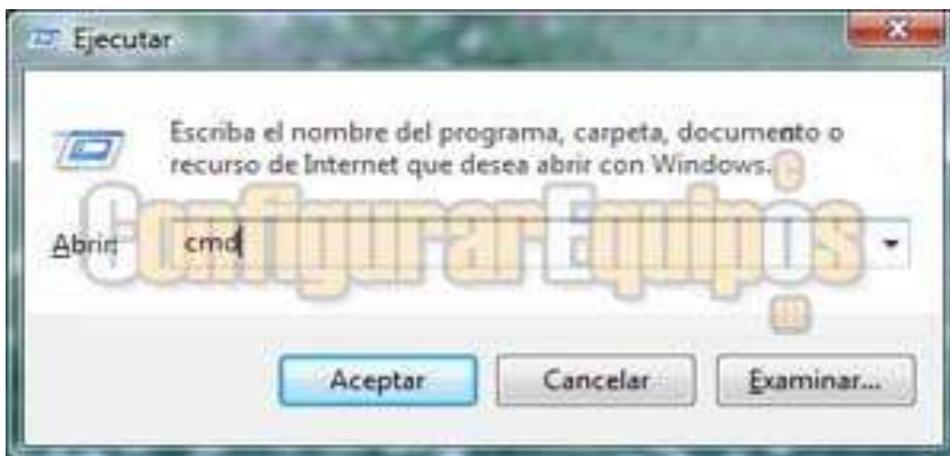
El primer paso será encender todas las Estaciones Impresoras y otros Equipos instalados a la Red, asegúrate que el Servidor esté conectado a Internet y que el concentrador este encendido y funcionando, otra forma de saber si las estaciones están conectadas con el Servidor es abriendo el Panel de Control, dando doble Clic sobre el Icono de Conexiones de Red. Una vez allí ubica en el lado izquierdo una pequeña pantalla llamada Otros Sitios, se le dará un Clic sobre el Nombre que le diste a tu Red. Aparecerá otra pantalla en la parte superior izquierda de la pantalla, allí darás un Clic en Ver Equipos de Red. Siguiendo estos sencillos pasos tendrás una vista completa de todos los Equipos conectados a la Red, de allí podrás Monitorearlos y acceder a ellos.

USO Y UTILIDAD DE LOS COMANDOS IPCONFIG Y PING.

A continuación, vamos a ver cómo podemos controlar nuestra red a través de los comandos IPConfig y Ping. Se trata de dos comandos de consola de Windows que nos permiten ver de forma rápida una serie de informaciones sobre nuestra red y su estado. Antes de nada, vamos a recordar cómo se accede al editor de comandos.



Para acceder al **Editor de comandos** vamos a **Inicio** y hacemos clic sobre **Ejecutar**.



En la ventana que se nos abre escribimos **CMD** y pulsamos en **Aceptar**. Con esto ya tenemos abierta la ventana del editor de comandos.

IPCONFIG:

El comando **IPConfig** nos muestra la información relativa a los parámetros de nuestra configuración **IP** actual. Este comando tiene una serie de modificadores para ejecutar una serie de acciones concretas.

Estos modificadores son:

/all Muestra toda la información de configuración.

/allcompartments Muestra información para todos los compartimientos.

/release Libera la dirección IP para el adaptador especificado (IPv4 e IPv6).

/renew Renueva la dirección IPv4 para el adaptador especificado.

/renew6 Renueva la dirección IPv6 para el adaptador especificado.

/flushdns Purga la caché de resolución de DNS.

/registerdns Actualiza todas las concesiones DHCP y vuelve a registrar los nombres DNS.

/displaydns Muestra el contenido de la caché de resolución DNS.

/showclassid Muestra todos los id de clase DHCP permitidas para este adaptador.

/setclassid Modifica el id de clase DHCP.

Vamos a centrarnos en la información que se nos ofrece al ejecutar **IPConfig /all**.

Para ello escribimos en el editor de comandos **IPConfig /all** y pulsamos **Intro**



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Versión 6.0.6000]
Copyright (c) 2006 Microsoft Corporation. Reservados todos los derechos.
C:\Users\Jose>IPCONFIG /ALL
```

A continuación, se nos muestra toda la información relativa a nuestra conexión y configuración IP.

```

C:\Windows\system32\cmd.exe
Microsoft Windows [Versión 6.0.6000]
Copyright (c) 2006 Microsoft Corporation. Reservados todos los derechos.

C:\Users\Jose>IPCONFIG /ALL

Configuración IP de Windows

Nombre de host . . . . . : Jose
Sufijo DNS principal . . . . . :
Tipo de nodo . . . . . : bcast
Enrutamiento IP habilitado . . . . . : no
Proxy WINS habilitado . . . . . : no

Adaptador de Ethernet Conexión de área local:

Sufijo DNS específico para la conexión. . . . . :
Descripción . . . . . : Controladora de red NUIDIA nForce

Dirección física . . . . . : 00-18-
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . . . : sí
Vínculo: dirección IPv6 local. . . . . : fe80::fd0c:
Dirección IPv4. . . . . : 192.168.1.37<Preferido>
Máscara de subred . . . . . : 255.255.255.0
Concesión obtenida. . . . . : martes, 30 de octubre de 2007 7:5
9:47
La concesión expira . . . . . : viernes, 02 de noviembre de 2007
7:59:47
Puerta de enlace predeterminada . . . . . : 192.168.1.1
Servidor DHCP . . . . . : 192.168.1.1
IAID DHCPv6 . . . . . : 201332979
Servidores DNS . . . . . : 80.58.61.250
NetBIOS sobre TCP/IP. . . . . : 80.58.61.254
: habilitado

Adaptador de túnel Conexión de área local*:

Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . . . . :
Descripción . . . . . : Teredo Tunneling Pseudo-Interface

Dirección física . . . . . : 02-00-
DHCP habilitado . . . . . : no
Configuración automática habilitada . . . . . : sí

C:\Users\Jose>

```

Como podemos ver en la imagen, la información que nos ofrece es bastante amplia, pero vamos a centrarnos en la que más nos puede interesar y más podemos usar.

DHCP habilitado. - Nos indica si el servicio DHCP está habilitado o no.

Configuración automática habilitado. - Nos indica si tenemos la configuración de nuestra red en forma automática.

Vínculo: dirección IPv6 local. - Nos muestra nuestra la dirección IPv6 de nuestra máquina (en SO que lo admitan).

Dirección IPv4. - Nos muestra la dirección IP actual de nuestra máquina.

Máscara de subred. - Nos muestra cual es la máscara de subred de nuestra red.

Puerta de enlace predeterminada. - Nos muestra la IP de la puerta de enlace (normalmente de nuestro router).

Servidor DHCP. - Muestra la IP del servidor DHCP al que estamos conectado.

IAID DHCPv6. - Muestra la información sobre DHCP en la versión IPv6 (en SO que lo admiten).

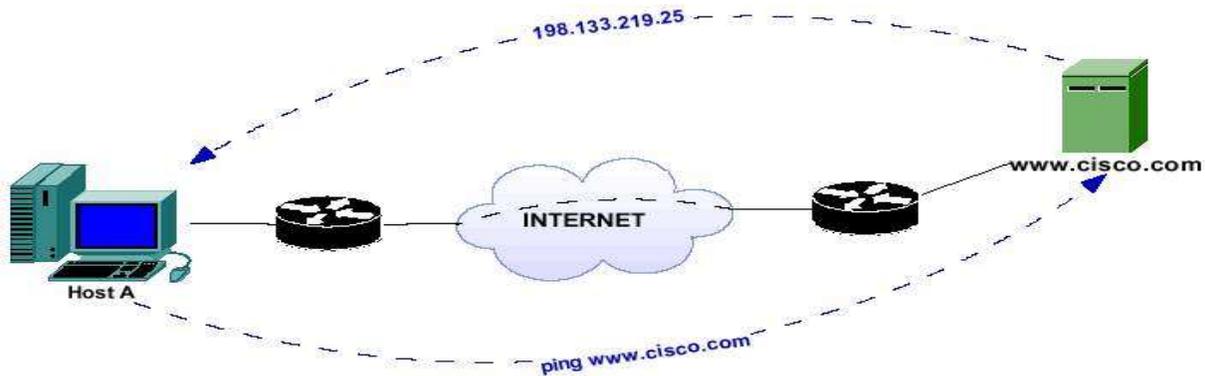
Servidores DNS. - Nos muestra la IP de los servidores DNS a los que estamos conectados.

Esta información es muy importante, ya que nos permite saber la IP de nuestro equipo, la Puerta de enlace (que usaremos si queremos configurar nuestro router para entrar en él) y las DNS.

PING: Cuando hacemos **ping** a un equipo (ejecutamos el comando **ping**) o a una dirección IP lo que hace el sistema es enviar a esa dirección una serie de paquetes (normalmente cuatro)

de un tamaño total de 64 bytes (salvo que se modifique) y queda en espera del reenvío de estos (eco), por lo que se utiliza para medir la latencia o tiempo que tardan en comunicarse dos puntos remotos. Una de las ventajas de ejecutar este comando es que los paquetes se envían atacando directamente la IP a la que dirigimos el ping, lo que hace que una de sus utilidades es comprobar la conectividad de nuestra red, ya que no están influidos por ningún controlador del sistema. Para comprobar el correcto funcionamiento de los elementos de nuestra red podemos hacer tres pings en el orden que se especifica:

Un primer ping a nuestra IP local, con lo que comprobamos que nuestra tarjeta de red funciona correctamente (en este caso hacemos PING 192.168.1.37).



Un segundo ping a nuestra Puerta de enlace, con lo que comprobamos que nuestro equipo se comunica correctamente con nuestro router (en este caso hacemos PING 192.168.1.1).

Un tercer ping a la IP de nuestro servicios DNS, con lo que comprobamos que nuestro router se conecta correctamente con el exterior, es decir, con Internet (en este caso hacemos PING 80.58.61.250). Para comprobar nuestra conexión de red podemos hacer ping a cualquier equipo de nuestra red, con lo que podemos comprobar si estamos realmente conectados a ese equipo, ya que en esta prueba no nos va a afectar ni configuraciones de Firewall (salvo que lo configuremos expresamente para no admitirlos) ni permisos de acceso al sistema, puesto que el ping se hace directamente sobre la tarjeta. También podemos hacer **PING** a una dirección de una *World Wide Web* determinada. Por ejemplo, podemos hacer **ping www.telefonica.net** y el efecto será el mismo, siempre y cuando nuestro servicio DNS funcione correctamente.

Al igual que ocurre con el comando **IPConfig** el comando **PING** tiene también una serie de modificadores que en un momento dado nos pueden ser de utilidad.

Estos modificadores son:

- t Hacer ping al host especificado hasta que se detenga.
- a Resolver direcciones en nombres de host.
- n **cuenta** Número de solicitudes de eco para enviar.

- l tamaño** Enviar tamaño del búfer.
- f** Establecer marcador *No fragmentar* en paquetes (sólo en IPv4).
- i TTL** Tiempo de vida.
- v TOS** Tipo de servicio (sólo en IPv4).
- r cuenta** Registrar la ruta de saltos de cuenta (sólo en IPv4).
- s cuenta** Marca de tiempo de saltos de cuenta (sólo en IPv4).
- j lista-host** Ruta de origen no estricta para lista-host (sólo en IPv4).
- k lista-host** Ruta de origen estricta para lista-host (sólo en IPv4).
- w tiempo de espera** Tiempo de espera en milisegundos para esperar cada respuesta.
- R** Usar encabezado de enrutamiento para probar también la ruta inversa (sólo en IPv6).
- S srcaddr** Dirección de origen que se desea usar (sólo en IPv6).
- 4** Forzar el uso de IPv4.
- 6** Forzar el uso de IPv6.

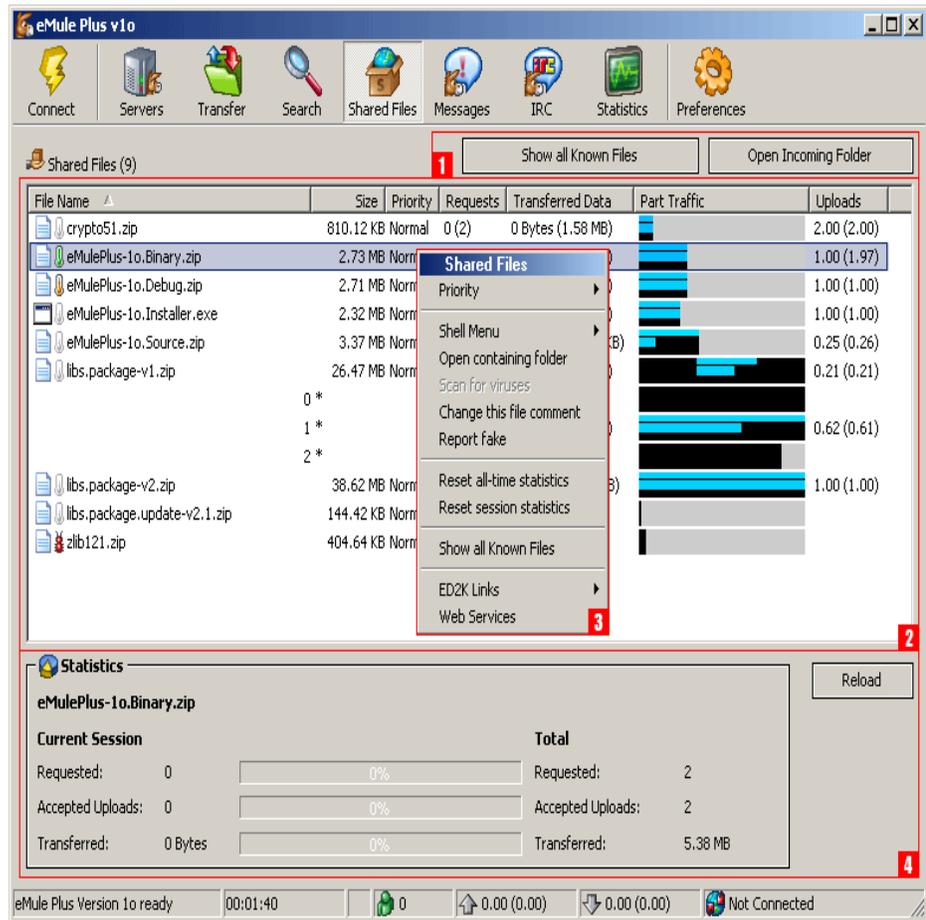
Reporte de resultados de la práctica			
Nombre de la práctica			
Competencia que a desarrollar según el programa			
La práctica la realicé de manera:	Grupal	Individual	Fecha de realización
Desempeños que debo mostrar			
El producto obtenido en la práctica es:			
Lo que aprendí con la práctica			
Indicadores de la competencia que trabajé			
Dónde puedo aplicar lo aprendido			
Con qué contenidos de otras unidades de aprendizaje se relaciona			
En dónde encontré información complementaria para trabajar la práctica			
Cómo seleccioné la información utilizada			
Criterios con los que me evaluaron			
Qué más me gustaría aprender sobre el tema			

TEMA 06: RECURSOS COMPARTIDOS.

- ✓ 6.1 Archivos y carpetas compartidas.
- ✓ 6.2 Niveles de acceso en archivos y carpetas compartidas.

6.1 Archivos y carpetas compartidas.

En un equipo con Windows XP, puede compartir archivos entre usuarios locales y entre usuarios remotos. Los usuarios locales inician sesión directamente en su equipo con su propia cuenta o con una cuenta de invitado. Los usuarios remotos que conectan con su equipo por red tienen acceso a los archivos compartidos que hay en el equipo. Puede tener acceso a la IU Uso compartido simple de archivos viendo las propiedades de una carpeta. Mediante la IU Uso compartido simple de archivos, puede configurar a nivel de carpeta los permisos de recursos compartidos y los del sistema de archivos NTFS.



Estos permisos se aplican a la carpeta, a todos los archivos de esa carpeta, a las carpetas secundarias y a todos los archivos de las carpetas secundarias. Los archivos y carpetas que se crean o copian en una carpeta, heredan los permisos definidos para su carpeta principal. Este artículo describe cómo configurar el acceso a sus archivos dependiendo de los niveles de permisos. Parte de la información que contiene este artículo acerca de los niveles de permisos no está documentada en los archivos del sistema operativo o en el archivo de Ayuda.

Con el uso de archivos compartidos en Windows XP, puede configurar cinco niveles de permisos. Con la IU Uso compartido simple de archivos puede configurar los niveles 1, 2, 3, 4 y 5. Para ello, Da clic con el botón secundario del mouse (ratón) y después Da clic en **Compartir y seguridad** para abrir la interfaz. Para configurar el Nivel 3, copie un archivo o carpeta en la carpeta Documentos compartidos que encontrará debajo de Mi PC. Esta configuración no cambia cuando activa o desactiva la interfaz Uso compartido simple de archivos. La

configuración de Nivel 1 es la más privada y segura, mientras que la de Nivel 5 es la más pública y menos segura.

Los sistemas Windows traen activado "de serie" un sistema para poder compartir ciertos recursos, orientado a facilitar dicha tarea en una red, como la que pueden formar varios ordenadores domésticos o de una oficina. Netbios es una interfaz entre aplicaciones que fue desarrollada por IBM para acceder a los recursos de redes locales. Dicho así la cosa no parece ir más allá, pero es uno de los agujeros de seguridad de Windows más frecuentemente ignorado, aunque no pueda calificarse técnicamente como tal. ¿Por qué? porque dicho protocolo es aplicado por Windows a todas las conexiones, no sólo a las de red local sino también a las de Internet, sin filtrar dicha circunstancia, lo que se traduce en que nuestro sistema es receptivo a esas conexiones exteriores.

Mantener esa configuración puede significar que alguien se conecte por uno de los puertos destinado a esa interfaz de comunicación y acceda a las carpetas o recursos designados (que pueden ser desde impresoras compartidas, unas carpetas específicas o todo el disco duro). Esto es comúnmente utilizado para entrar de una manera sencilla en ordenadores ajenos, y está al alcance de cualquier aprendiz de Hacker. Alguien con algo más de conocimientos puede acceder a todo el sistema impunemente aprovechando las características de inseguridad de los sistemas Windows, averiguando passwords etc.

Nos preguntábamos hasta qué punto era esto cierto, pues esta circunstancia nunca ha sido considerada como "Agujero" por Microsoft y ha venido repitiéndose en cada sistema operativo que sacaba al mercado, con lo cual se supone que la gente ya debe saberlo y no tendrá activado en sus equipos el compartir recursos si no lo necesita. Para empezar, ningún ordenador que no forme parte de una red necesita compartir nada, salvo contadas excepciones, y los ordenadores en red deben proteger el acceso a dichos recursos mediante passwords. Pues bien, lo cierto es que los cortafuegos continúan registrando y bloqueando muchos intentos de conexión Netbios, y aprovechamos para decir que es básico disponer de un firewall, eso como norma de seguridad nº 2. (La nº 1 es mantener un antivirus residente y actualizado.) Bueno, ya estamos concienciados de la necesidad de mantenernos al tanto de aquello que pueda significar una vía de entrada a nuestro PC. Veamos ahora cual es el estado del mismo respecto a Netbios.

Comprobando los recursos compartidos. Básicamente, en los sistemas Windows tenemos tres maneras de requerir la información sobre los recursos que están puestos a disposición común:

1. Por Aplicación Gráfica de Windows.
2. Consultando el Entorno de Red
3. Consultando la información mediante un comando MS-DOS en una ventana del mismo.

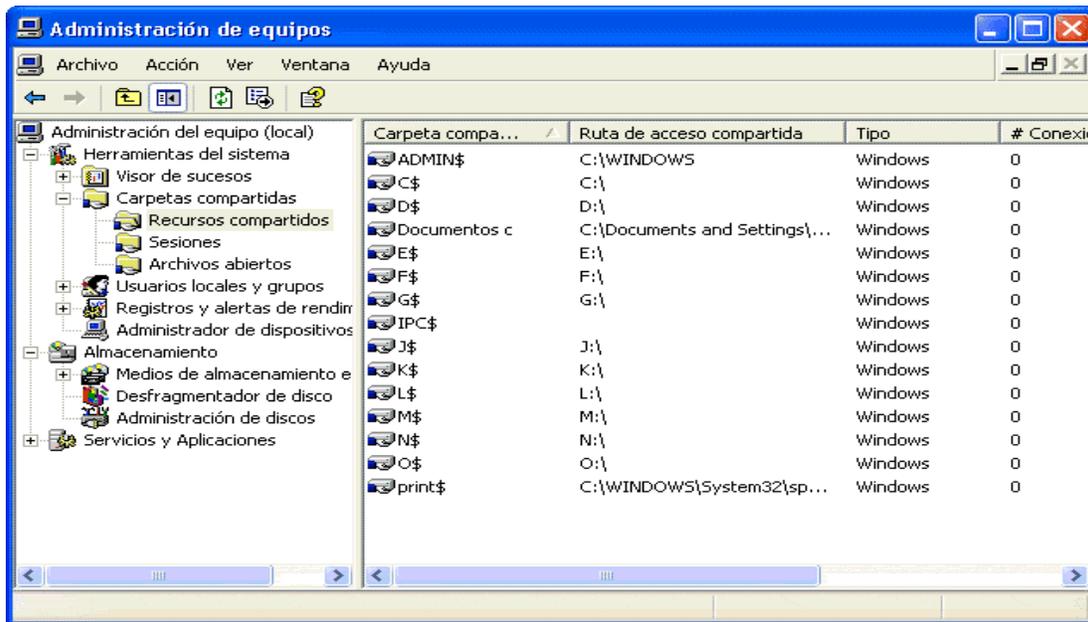
Los recursos compartidos no ocultos, en un alarde imaginativo de los diseñadores de Windows, muestran una mano generosa que ofrece el recurso en cuestión: Veamos como comprobar todas las carpetas establecidas para ser compartidas, sean ocultas o visibles:

En Windows XP.

· Inicio - Configuración - Panel de control - Herramientas administrativas - Administración de equipos - Árbol - Administración del equipo (local) - Herramientas del sistema - Carpetas compartidas -

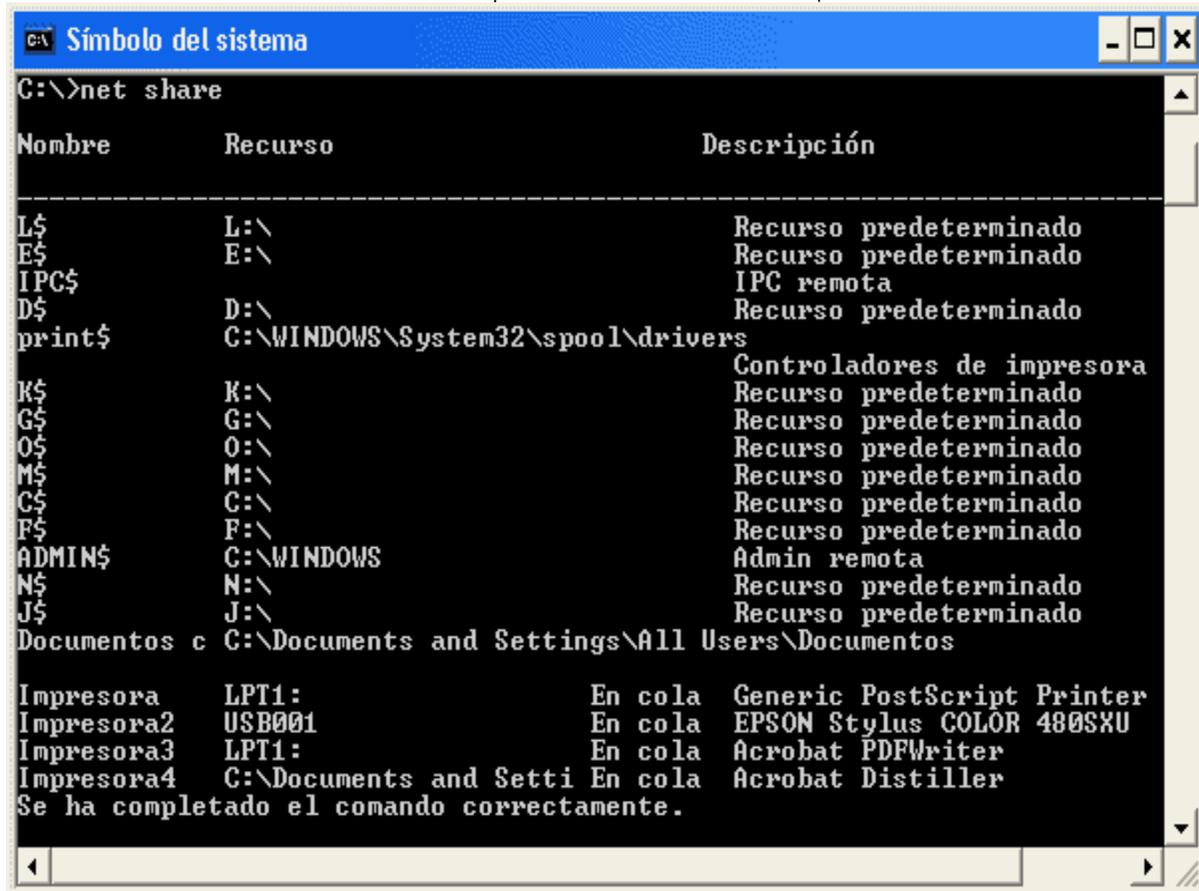
Recursos compartidos

Son visibles las que carecen del símbolo \$ al final.



Inicio - Programas - Accesorios - Símbolo del sistema Ejecutamos net share

Son visibles las que carecen del símbolo \$ al final.



Deshabilitando compartir recursos. En el caso de que no tengamos necesidad de compartir, deberemos quitar las opciones que posibilitan hacerlo. Además, es conveniente tenerlo por costumbre, y debemos recordar hacerlo después de formatear o actualizar nuestro sistema operativo.

Eso es lo evidente, pero lo mejor es irse al registro:

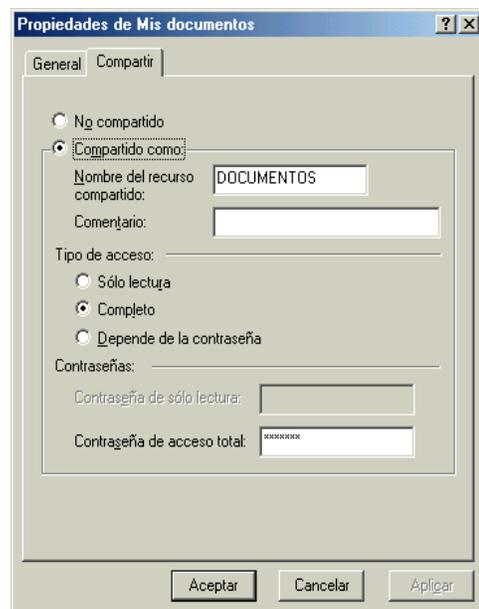
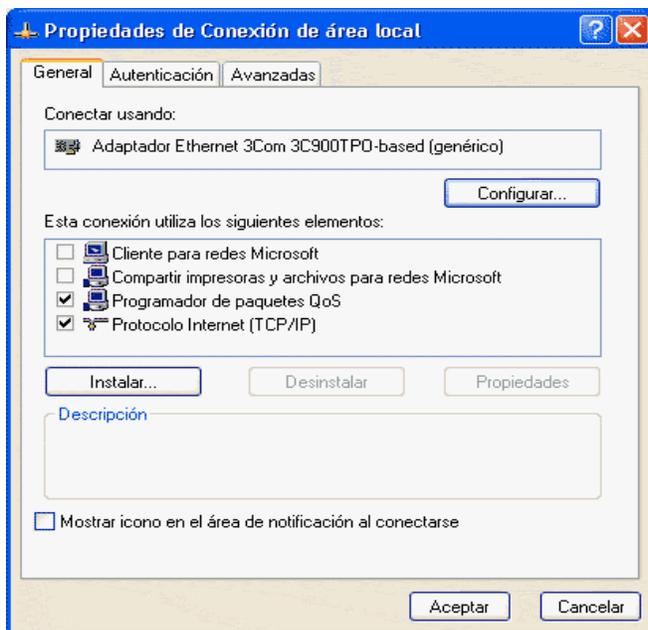
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters
y renombrar la clave TransportBindName a TransportBindNameX

Con esto se desactivan la interfaz Netbios (puertos 137, 138,139) y la smb (445). Esto es así porque para acceder a una sesión Netbios en W2000 puedes acceder por el puerto 139 o por el puerto 445." Esto es aplicable, asimismo, a Win XP.

· Inicio - Panel de control - Conexiones de red - Conexión de área local - Menú archivo - Propiedades

Desinstalar "Compartir impresoras y archivos para redes Microsoft" y "Cliente para redes Microsoft." o

Registro:



HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters
y renombrar la clave TransportBindName a TransportBindNameX

Compartiendo recursos. En el caso de necesitar compartir los recursos, deberemos seguir unas medidas de precaución para la protección del sistema, evidentemente lo principal es gestionar adecuadamente la política de acceso de los usuarios y sus acciones mediante passwords. Eso significa que las contraseñas han de ser impuestas con criterios rigurosos de efectividad, procurando que no sean cortas o evidentes y deben ser cambiadas cada cierto tiempo. Ver "Contraseñas Seguras". Se supone que tenemos activada de antemano la configuración del sistema para compartir, de otra forma habría que activarla recurriendo a las opciones mencionadas en el paso anterior, pero a la inversa. Ahora vamos a establecer el control de acceso a los recursos:

Sólo lectura. Obviamente recomendable, ya que no permite la modificación o borrado del recurso.

Completo/Total. Para usuarios con necesidad de ejecutar acciones que modifiquen los archivos.

Dependiendo de la contraseña. El recurso se dotará de dos contraseñas, una de acceso al mismo con permiso de solo lectura y otra de permiso total. Dependiendo la contraseña que conozca el usuario tendrá uno u otro privilegio sobre el archivo.

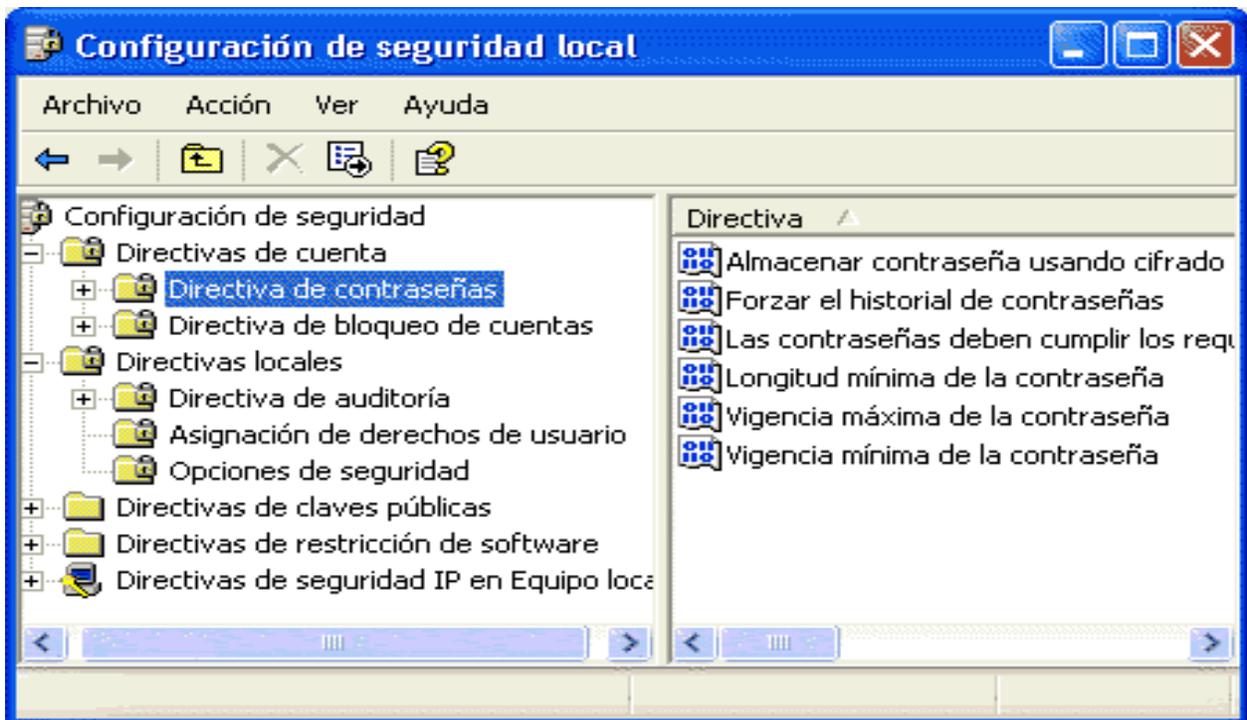
Sentar una base. En XP la administración de los recursos compartidos tiene otro concepto, basado en una operativa multiusuario. Es por ello que es de suma importancia mantener desde el principio una claridad de ideas y un orden en este aspecto.

Los administradores pueden establecer unas opciones de seguridad de contraseñas para las cuentas de cada usuario local, que no vienen configuradas de inicio. De esta forma se minimizan los ataques a los passwords, otra práctica habitual del mundo Hack.

· Panel de control - Herramientas administrativas - Directiva de seguridad local

En esta ventana obtendremos un árbol muy interesante y que merece ser revisado detenidamente, pues ofrece la posibilidad de configurar las opciones de seguridad ajustando el nivel de protección a nuestras preferencias.

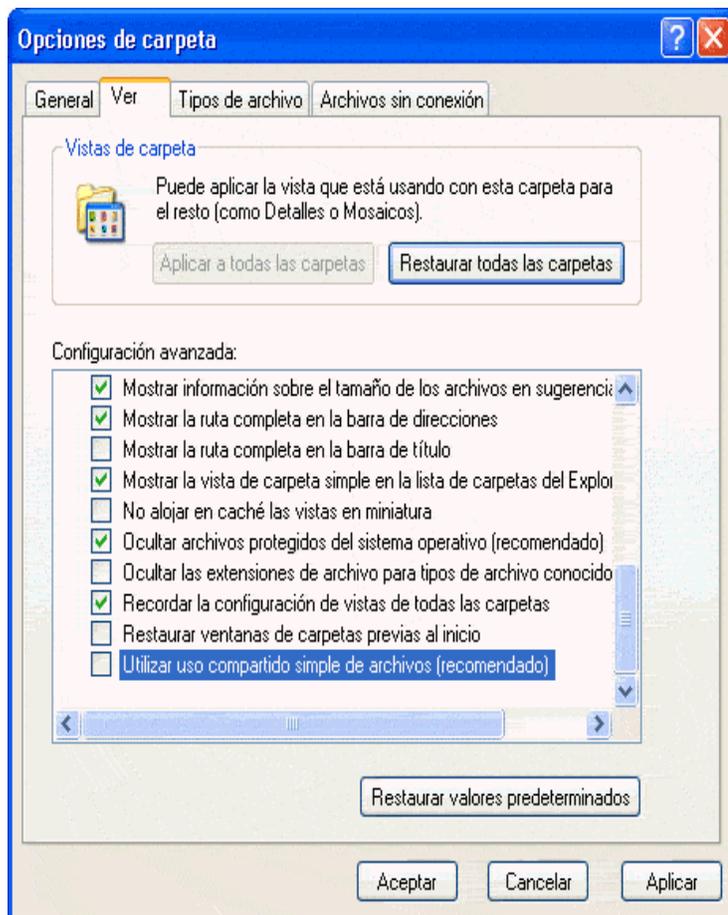
Por ejemplo, en las "Directivas de cuenta" - "Directivas de contraseña" podemos forzar a que las contraseñas cumplan los requisitos de complejidad, la longitud mínima, así como la vigencia máxima y mínima de las mismas.



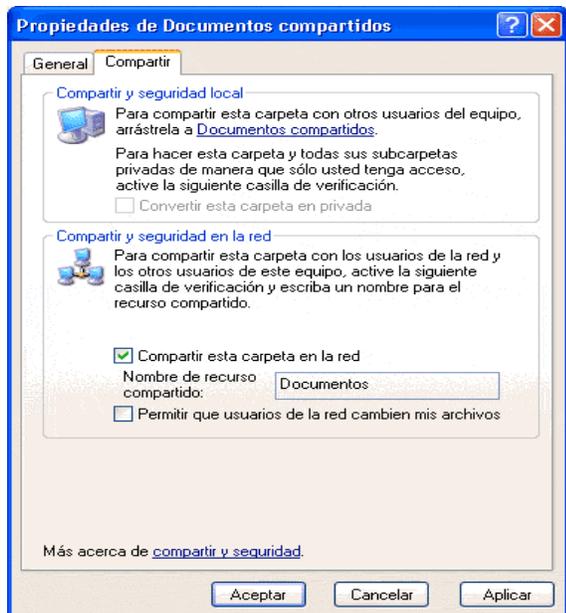
En las "Directivas locales" - "Asignación de derechos de usuario" estableceremos determinados permisos a los usuarios o los reduciremos a la potestad del Administrador. En "Opciones de seguridad" tenemos directivas relativas a seguridad de red, acceso a redes, inicio de sesión, dispositivos, cuentas... aquí podemos habilitar y deshabilitar o definir una larga serie de opciones, algunas muy interesantes... incluso podemos cambiar el nombre de la cuenta del Administrador y renombrar como tal una cuenta sin privilegios, al objeto de despistar al posible intruso que busque asaltar esa cuenta tan golosa...

Designando recursos compartidos.

Lo primero es desactivar el "Modo simple" del uso compartido de archivos, en las Opciones de Carpeta del Panel de Control:



De esta forma no limitamos las opciones de la pestaña "Compartir" de las carpetas o recursos elegidos, para que en lugar de que dicha pestaña se muestre de esta forma...



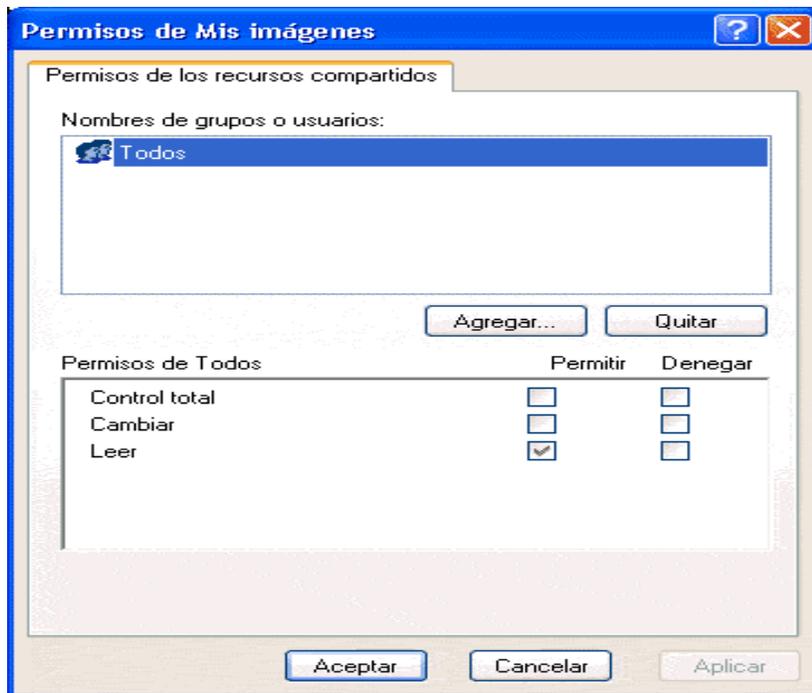
Una vez en este punto, asignaremos los permisos designando los usuarios que queremos que puedan acceder a esta carpeta. Estos lo harán autenticándose con su propio password. Por defecto, todos los usuarios tienen el mismo acceso a los recursos, pero podemos agregar y quitar usuarios, o permitir o denegar las acciones sobre los archivos, crear grupos etc. Es conveniente clasificar en los mismos grupos a los usuarios con igual nivel de acceso o acción sobre los recursos, así como agrupar en las mismas carpetas los recursos destinados a los mismos usuarios o grupos, facilitando así su administración.

Para eso crearemos nuevos usuarios, desde esta ventana de "Permisos" - Agregar - Seleccionar usuarios o grupos. Desde aquí accedemos a las los botones- "Tipos de objetos"... "Ubicaciones"... o "Avanzadas"... donde podremos seleccionar las características de los usuarios o grupos a crear.

6.2 Niveles de acceso en archivos y carpetas compartidas.

Activar y desactivar la interfaz Uso compartido simple de archivos

En los equipos con Windows XP Home Edition está siempre activada. La interfaz uso compartido simple de archivos está activada de manera predeterminada en los equipos con Windows XP Professional unidos a un grupo de trabajo. Los equipos con Windows XP Professional que se unen a un dominio sólo usan la interfaz clásica de seguridad y uso compartido de archivos. Cuando usa la interfaz



Uso compartido simple de archivos (ubicada en las propiedades de carpeta), se configuran tanto los permisos de archivos como los de recursos compartidos. Si la desactiva, tiene más control sobre los permisos concedidos a usuarios individuales. Sin embargo, para mantener seguras sus carpetas y archivos debe tener un conocimiento avanzado de los permisos de recursos compartidos y de NTFS. Si desactiva la interfaz Uso compartido simple de archivos, no se desactiva la característica Documentos compartidos. Para activar o desactivar la interfaz Uso compartido simple de archivos en Windows XP

Professional, siga estos pasos:

1. Da doble clic en Mi PC en el escritorio.
2. En el menú Herramientas, Da clic en Opciones de carpeta.
3. Da clic en la ficha Ver y active la casilla de verificación Utilizar uso compartido simple de archivos (recomendado) para activar la interfaz. (Para desactivar la característica, anule la selección de esa casilla de verificación.)

Administrar los niveles de acceso a los archivos y recursos compartidos.

Puede usar la interfaz Uso compartido simple de archivos para configurar cinco niveles de acceso diferentes a los archivos y los recursos compartidos:

- Nivel 1: mis documentos (privado)
- Nivel 2: mis documentos (predeterminado)
- Nivel 3: archivos de documentos compartidos que están a la disposición de los usuarios locales
- Nivel 4: archivos compartidos en red (todos tienen permiso de lectura)
- Nivel 5: archivos compartidos en red (todos tienen permiso de lectura y escritura)

Notas:

- De manera predeterminada, los archivos almacenados en Mis documentos son de Nivel 2.
- Las carpetas de los niveles 1, 2 y 3 sólo están disponibles para un usuario que inicie sesión localmente. Los usuarios que inician sesión localmente incluyen al que la inicia en un equipo con Windows XP Professional desde una sesión de escritorio remoto (RDP).
- Las carpetas de los niveles 4 y 5 están a la disposición de los usuarios que inician sesión localmente, así como a la de los usuarios remotos por red.

Nivel 1: mis documentos (privado).

El propietario del archivo o de la carpeta tiene sobre ella permiso de lectura y escritura. Nadie más puede leer o escribir en la carpeta o en los archivos que hay en ella. Todas las subcarpetas que están contenidas en una carpeta marcada como privada seguirán siendo privadas a menos que cambie los permisos de la carpeta principal.

Si es administrador del equipo y crea una contraseña de usuario para su cuenta utilizando la herramienta Panel de control de Cuentas de usuario, se le pedirá que marque como privados sus archivos y carpetas.

Nota: la opción de marcar como privada una carpeta (Nivel 1) sólo está a la disposición de una cuenta de usuario en su carpeta Mis documentos.

Para configurar en el Nivel 1 una carpeta con todos sus archivos, siga estos pasos:

1. Da clic con el botón secundario del mouse (ratón) en la carpeta y, a continuación, Da clic en **Compartir y seguridad**.

2. Active la casilla de verificación **Convertir esta carpeta en privada** y, a continuación, Da clic en **Aceptar**.

Nivel 2 (predeterminado):

Mis documentos (predeterminado). El propietario del archivo o de la carpeta y los administradores locales del equipo tienen sobre ella permiso de lectura y escritura.

Nadie más puede leer o escribir en la carpeta o en los archivos que hay en ella. Esta es la configuración predeterminada para todas las carpetas y archivos en la carpeta Mis documentos de cada usuario. Para configurar en el Nivel 2 una carpeta con todos sus archivos, siga estos pasos:

1. Da clic con el botón secundario del mouse (ratón) en la carpeta y, a continuación, Da clic en **Compartir y seguridad**.

2. Compruebe que se ha anulado la selección de las casillas de verificación **Convertir esta carpeta en privada** y **Compartir esta carpeta en la red**, y Da clic en **Aceptar**.

Permisos NTFS locales:

- Propietario: Control total
- Administradores: Control total
- Sistema: Control total
- Permisos de recurso compartido en red:
- no compartidos

Nivel 3:

Archivos de documentos compartidos que están a la disposición de los usuarios locales.

Los archivos que son compartidos con los usuarios que inician sesión localmente en el equipo. Los administradores locales del equipo pueden leer, escribir y eliminar los archivos de la carpeta Documentos compartidos.

Los usuarios restringidos sólo pueden leer los archivos de la carpeta Documentos compartidos. En Windows XP Professional, los Usuarios avanzados también pueden leer, escribir o eliminar archivos de la carpeta Documentos compartidos. El grupo Usuarios avanzados sólo está disponible en Windows XP Professional. Los usuarios remotos no pueden tener acceso a las carpetas o archivos de Nivel 3. Para permitir que los usuarios remotos tengan acceso a los archivos, debe compartirlos en red (niveles 4 ó 5).

Para configurar en el Nivel 3 un archivo o una carpeta con todos sus archivos, inicie el Explorador de Microsoft Windows y, a continuación, copie o mueva el archivo o carpeta en la carpeta Documentos compartidos debajo de Mi PC.

Permisos NTFS locales:

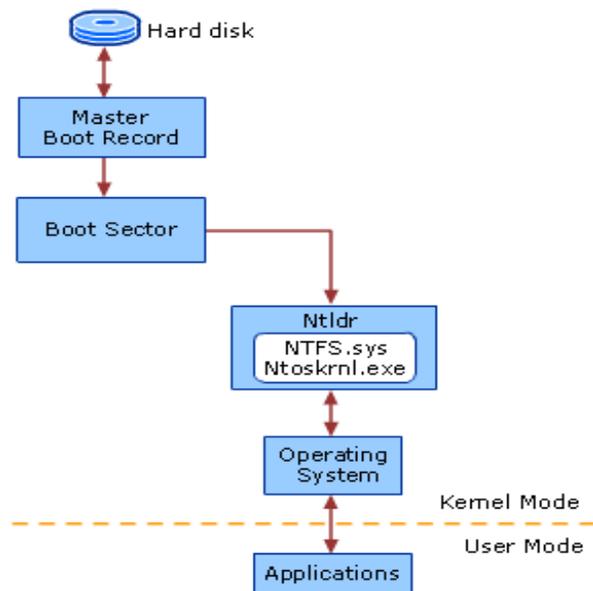
- Propietario: Control total
- Administradores: Control total
- Usuarios avanzados: cambiar
- Usuarios restringidos: lectura
- Sistema: Control total

Permisos de recurso compartido en red:

- no compartidos

Nivel 4: compartidos en red (sólo lectura).

Los archivos son compartidos para lectura por todos los que están en la red. Todos los usuarios locales, incluida la cuenta de invitado, pueden leer los archivos. Pero no pueden modificar los contenidos. Cualquier usuario puede leer y cambiar los archivos.



Para configurar en el Nivel 4 una carpeta con todos sus archivos, siga estos pasos:

- Da clic con el botón secundario del mouse (ratón) en la carpeta y, a continuación, Da clic en Compartir y seguridad.
- Seleccione la casilla de verificación Compartir esta carpeta en la red.
- Anule la selección de la casilla de verificación Permitir que usuarios de la red cambien mis archivos y, después, Da clic en Aceptar.

Permisos NTFS locales:

- Propietario: Control total
- Administradores: Control total
- Sistema: Control total
- Todos: lectura

Permisos de recurso compartido en red:

- Todos: lectura

Nivel 5: compartidos en red (lectura y escritura).

Este nivel de acceso es el de mayor disponibilidad y menor seguridad. En este nivel de acceso, cualquier usuario (local o remoto) puede leer, escribir, cambiar o eliminar un archivo de una carpeta compartida. Recomendamos que este nivel sólo se utilice en una red cerrada que tenga configurado un servidor de seguridad. Todos los usuarios locales, incluida la cuenta de invitado, pueden leer y modificar los archivos.

Para configurar en el Nivel 5 una carpeta con todos sus archivos, siga estos pasos:

1. Da clic con el botón secundario del mouse (ratón) en la carpeta y, a continuación, Da clic en Compartir y seguridad.
2. Seleccione la casilla de verificación Compartir esta carpeta en la red y Da clic en Aceptar.

Permisos NTFS locales:

- Propietario: Control total
- Administradores: Control total
- Sistema: Control total
- Todos: cambiar
- Permisos de recurso compartido en red: Todos: Control total

Nota: todos los permisos NTFS que se refieren a Todos incluyen la cuenta de invitado.

Todos los niveles que describe este artículo son mutuamente excluyentes. Las carpetas privadas (Nivel 1) no se pueden compartir hasta que dejen de estar marcadas como tales. Las carpetas compartidas (niveles 4 y 5) no se pueden marcar como privadas hasta que dejen de estar compartidas. Si crea una carpeta en Documentos compartidos (Nivel 3), la comparte en red y permite después que los usuarios de red modifiquen los archivos (Nivel 5), los permisos para el nivel 5 son efectivos para la carpeta, los archivos de la carpeta y las carpetas secundarias. Los otros archivos y carpetas de Documentos compartidos siguen configurados en el Nivel 3.

Nota: La única excepción se produce cuando tiene una carpeta (*SampleSubFolder*) que está compartida en el Nivel 4 dentro de una carpeta (*SampleFolder*) que está compartida en el Nivel 5. Los usuarios remotos tienen el nivel de acceso correcto a cada una de las carpetas compartidas. Los usuarios que han iniciado sesión localmente tienen permisos de escritura (Nivel 5) a las carpetas principales y secundarias.

Directrices

Recomendamos que sólo comparta en red las carpetas a las que deban tener acceso los usuarios remotos de los otros equipos. Recomendamos que no comparta la raíz de la unidad del sistema. Si lo hace, su equipo será más vulnerable a los usuarios remotos malintencionados.

La ficha Compartir del cuadro de diálogo Propiedades de la unidad incluye una advertencia cuando intenta compartir una carpeta raíz (por ejemplo, C:\). Para continuar, debe hacer clic en el vínculo Si ha comprendido el riesgo de compartir la raíz de unidad y aún desea hacerlo, Da clic aquí. Sólo los administradores del equipo pueden compartir la raíz de la unidad.

Los archivos que están en un dispositivo de sólo lectura, como un CD-ROM compartido en los niveles 4 ó 5, sólo estarán disponibles cuando el CD-ROM esté en su unidad. Cualquier CD-ROM que se encuentre en su unidad estará a la disposición de todos los usuarios de la red.

El permiso de un archivo puede ser diferente del de la carpeta que lo contiene si es cierta alguna de las condiciones siguientes:

- Utiliza el comando move en un símbolo del sistema para mover un archivo a la carpeta desde una carpeta de la misma unidad que tenga permisos diferentes.
- Usa una secuencia de comandos para mover el archivo a la carpeta desde una carpeta desde una carpeta de la misma unidad que tenga diferentes permisos.
- Puede ejecutar Cacls.exe en un símbolo del sistema o una secuencia de comandos para cambiar los permisos de archivos.
- Había archivos en el disco duro antes de que instalara Windows XP.
- Cambió los permisos de archivo cuando la interfaz Uso compartido simple de archivos estaba desactivada en Windows XP Professional.

Nota: los permisos NTFS no se mantienen en las operaciones de mover archivos cuando usa el Explorador de Windows con la interfaz Uso compartido simple de archivos activados.

Si activa y desactiva Uso compartido simple de archivos, los permisos de los archivos no se cambian.

Los permisos de NTFS y de los recursos compartidos no se cambian hasta que cambie los permisos de la interfaz. Si configura los permisos con la interfaz Uso compartido simple de archivos activados, sólo se ven afectadas las entradas de control de acceso (ACE) en los archivos que se usan para el Uso compartido simple de archivos. Se ven afectadas por la interfaz Uso compartido simple de archivos las siguientes ACE de la Lista de control de acceso (ACL) de los archivos o carpetas: Propietario, Administradores, Todos, System

Solución avanzada de problemas para configurar el uso compartido de archivos en Windows XP

Un equipo basado en Windows 2000 Professional o en Windows NT 4.0 que se una a un dominio o un grupo de trabajo que se actualice a Windows XP Professional mantiene respectivamente su pertenencia al dominio o grupo de trabajo y tiene activada la IU clásica de seguridad y de uso compartido de archivos. Los permisos de los recursos compartidos y de NTFS no se cambian con la actualización.

De manera predeterminada, si actualiza un equipo que está ejecutando Microsoft Windows 98, Windows 98 Segunda edición o Windows Millennium Edition que tenga permisos de compartir "por recursos" para Windows XP, la interfaz Uso compartido simple de archivos está siempre activada. Los recursos compartidos que tienen contraseñas asignadas se quitan y los que tienen contraseñas en blanco permanecen compartidos después de la actualización.

Si actualiza a Windows XP Professional un equipo que está ejecutando Windows 98, Windows 98 Segunda edición o Windows Millennium Edition y ese equipo ha iniciado sesión en un dominio, si ese equipo tiene activado el acceso al nivel de recursos compartidos y se une al dominio mientras el programa de instalación se está ejecutando, el equipo se inicia con la interfaz Uso compartido simple de archivos desactivada.

Los servidores de seguridad de Internet pueden impedir el examen y el uso compartido de archivos

Cuando está activada la interfaz Uso compartido simple de archivos, la administración remota y la edición remota del Registro no funcionan tal como se esperaba desde un equipo remoto,

mientras que las conexiones a los recursos compartidos administrativos (como C\$) no funcionan porque todos los usuarios remotos se autentican como invitados. Las cuentas de invitados no tienen derechos administrativos. Cuando la interfaz Uso compartido simple de archivos está activada, si configuran las ACE de usuario específico los usuarios remotos no se ven afectados porque con esa interfaz activada todos ellos se autentican como invitados.

Los usuarios remotos pueden recibir un mensaje de "Acceso denegado" en un recurso compartido con el que antes habían conectado correctamente. Este comportamiento se produce después de que la unidad de disco duro se ha convertido a NTFS. Este comportamiento se produce en los equipos con Windows XP que tienen activada la interfaz Uso compartido simple de archivos y fueron actualizados a Windows 98, Windows 98 Segunda edición o Windows Millennium Edition. Este comportamiento se produce porque los permisos predeterminados de un disco duro que se ha convertido a NTFS no contienen el grupo Todos. Se necesita el grupo Todos para que los usuarios remotos que utilizan la cuenta de invitado tengan acceso a los archivos para configurar los permisos, anular el uso compartido de las carpetas afectadas y volver a activarlo.

Reporte de resultados de la práctica			
Nombre de la práctica			
Competencia que a desarrollar según el programa			
La práctica la realicé de manera:	Grupal	Individual	Fecha de realización
Desempeños que debo mostrar			
El producto obtenido en la práctica es:			
Lo que aprendí con la práctica			
Indicadores de la competencia que trabajé			
Dónde puedo aplicar lo aprendido			
Con qué contenidos de otras unidades de aprendizaje se relaciona			
En dónde encontré información complementaria para trabajar la práctica			
Cómo seleccioné la información utilizada			
Criterios con los que me evaluaron			
Qué más me gustaría aprender sobre el tema			

TEMA 07: PERIFERICOS COMPARTIDOS

- ✓ 7.1 Periféricos y recursos compartidos.
- ✓ 7.2 Impresoras compartidas en Windows 7 y Windows XP

7.1 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.

Un servidor de impresión ofrece la misma conectividad a una impresora que una tarjeta adaptadora de red ofrece a una computadora.

Permite a todas las computadoras de la red compartir la misma impresora. Los servidores de impresión son a menudo un componente básico de las redes cliente/servidor.

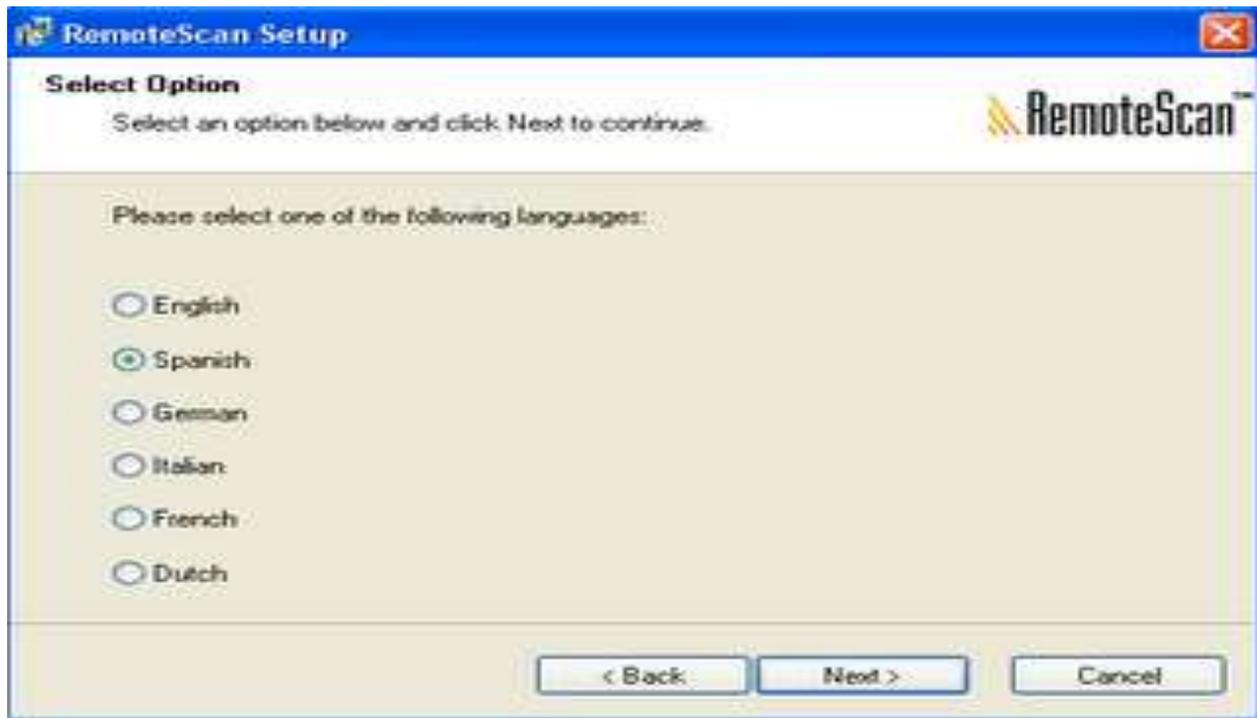


Entre los productos de comunicación se cuentan tarjetas de fax, módems y enrutadores que hacen posibles conexiones con Internet. Todos estos productos le permiten comunicarse con computadoras no conectadas a su red de área local (LAN).

Como compartir un scanner en red con el Software RemoteScan.

El programa se divide en dos tipos de instalación:

- La instalación/es correspondiente a las computadoras clientes (las que van a usar el scanner vía red)
- La instalación para la computadora servidor (donde está alojado el scanner).



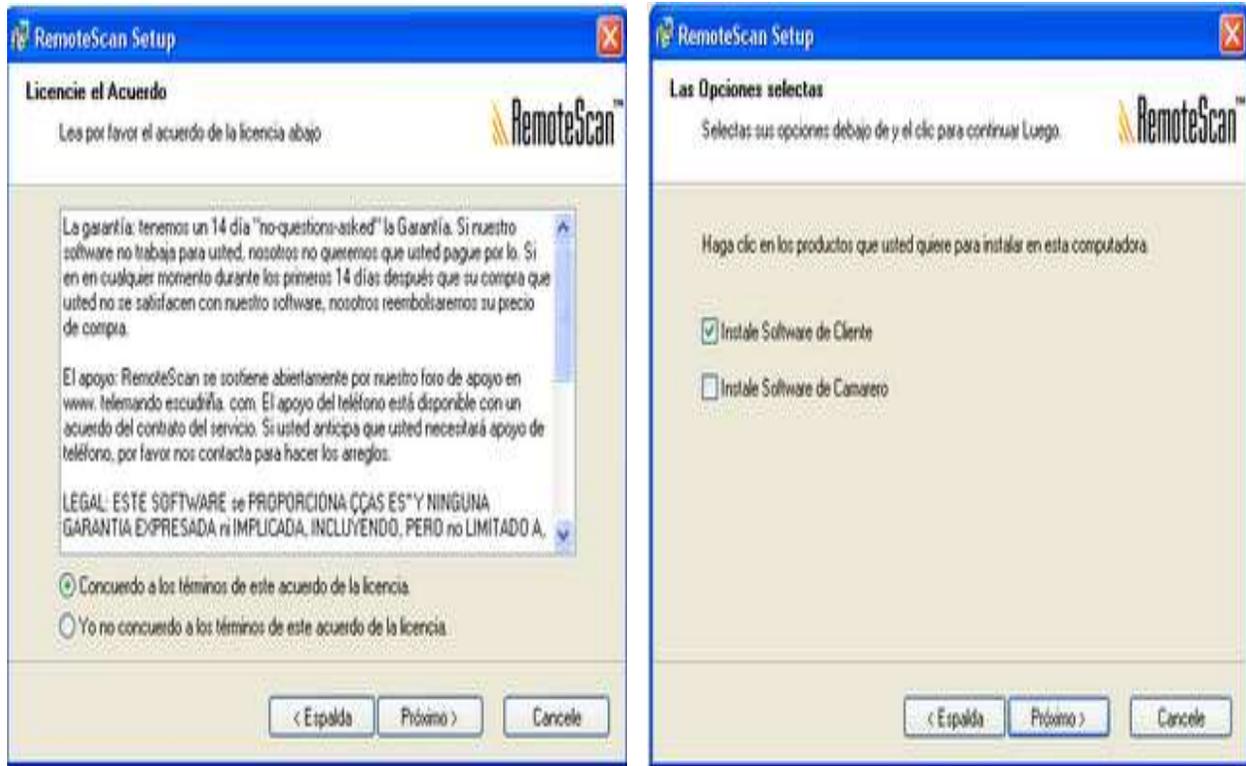
Instalación de RemoteScan:

Primer paso. Abrimos el programa ejecutable.

En la pantalla inicial elegimos el idioma en el cual queremos que este la interface del programa, en nuestro caso elegimos español y damos click a Next

El contrato de licencia del programa, tildar la opción de que estás de acuerdo con la licencia y darle click en "Próximo" para continuar con la instalación.

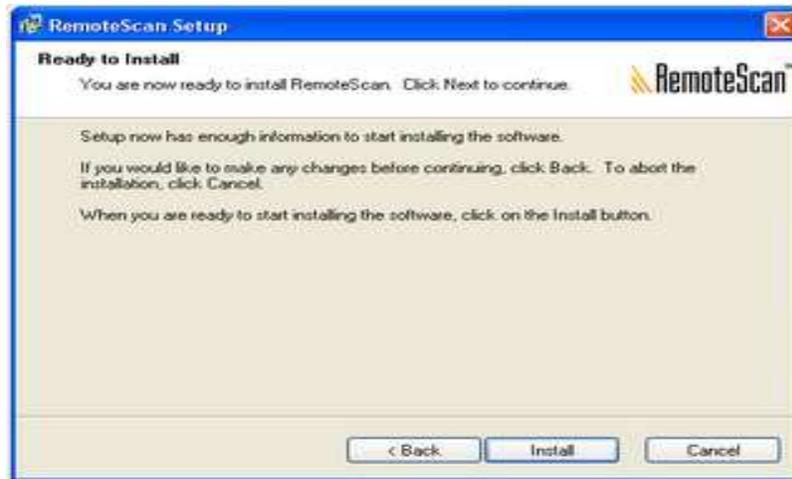
Debemos escoger según el tipo de instalación que estamos llevando a cabo, si deseamos que la PC se conecte al scanner de la red (instalada en otra PC) debemos elegir la instalación "Cliente", caso contrario, la instalación "Camarero" (Server), en este caso le damos click a la instalación Cliente.



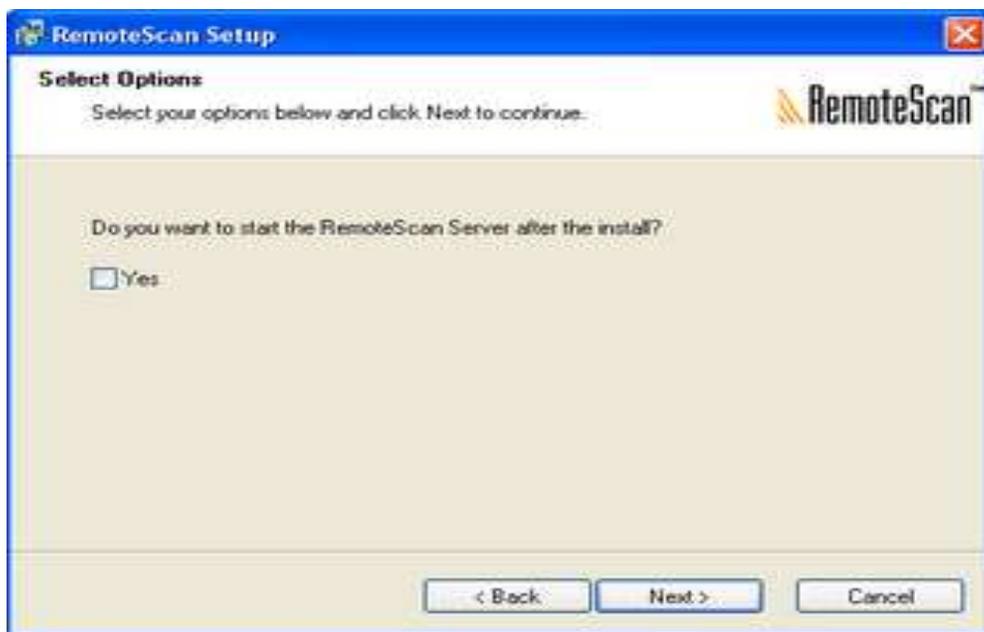
Ahora, el programa nos avisa si queremos que automáticamente RemoteScan establezca los permisos necesarios en el firewall para que el servicio funcione correctamente, o si lo queremos hacer nosotros manualmente, recomendado dejarlo como está.



Click a "Next" y en seguida a Install.



Una vez finalizado, ya tendremos el programa, instalado en nuestro sistema operativo. El proceso de instalación "camarero" o sea, del lado del servidor, es exactamente igual que al del cliente, la única variación que tiene es cuando se llega a esta etapa.



Nos pregunta si queremos que automáticamente cuando termina la instalación activar el servicio de RemoteScan para que pueda el scanner ser compartido por las otras PC's de la red. Ejemplo: Uso con Fireworks MX, abrimos el Fireworks Mx

Vamos a archivo...explorar...Adquisición Twain.



Le damos click y aparecemos en la siguiente pantalla de RemoteScan.



En la parte que nos dice scan server debería ir seleccionada la computadora donde está conectado el scanner, verificar que la dirección ip coincida. Para dar comienzo al scaneo del documento simplemente darle click a SCAN.

Nota de Aclaración: Recuerden que para que funcione correctamente, van a tener que instalar los dos componentes del programa, el cliente (en el pc donde queramos usar remotamente el scanner, y el servidor, tendrá que instalarse en el pc donde este físicamente el scanner)

7.2 Impresoras compartidas en Windows 7 y Windows XP.

Como compartir Impresoras entre Windows 7 y Windows XP.

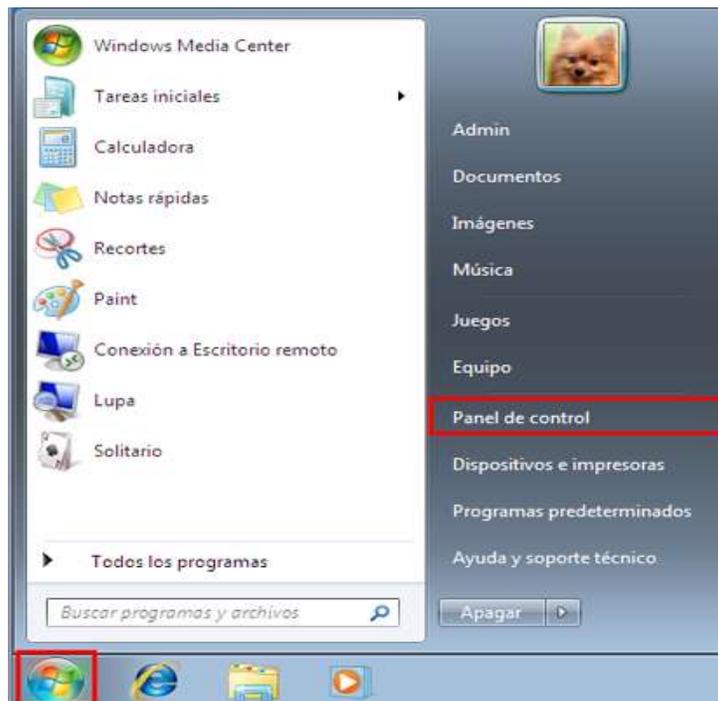
En este artículo se describe cómo compartir una impresora en una red doméstica o en una red que disponga de un enrutador o conmutador y cómo configurar el firewall de Windows para activar el uso compartido de archivos e impresoras en Windows 7 y Windows XP. En una red doméstica o de trabajo, no siempre se tiene un periférico por cada uno de los ordenadores de la red, como por ejemplo una impresora por cada equipo. Sin embargo, es posible que un periférico conectado a un equipo de la red sea utilizado por otro ordenador. Podemos suponer que se trata de una red a la cual están conectados el Equipo A y el Equipo B. Y que el equipo A corre Windows 7, mientras que el equipo B corre Windows XP.



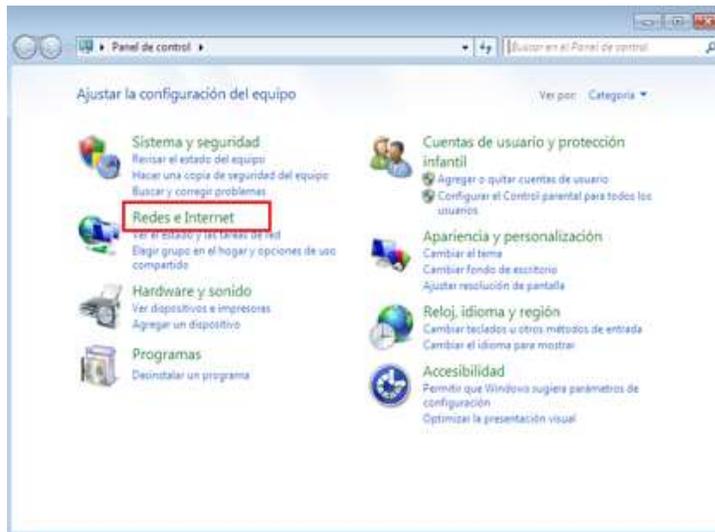
Entonces, si el equipo A tiene una impresora conectada y el equipo B necesita utilizar esa impresora, puede hacerlo sin necesidad de desconectar la impresora de su equipo original.

Cómo activar compartir impresoras en Windows 7

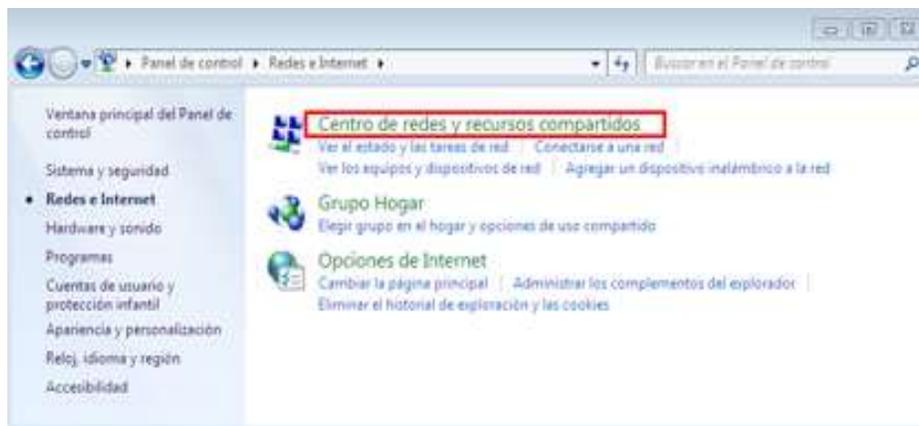
1. Haz click en **Inicio**  , y luego en Panel de control.



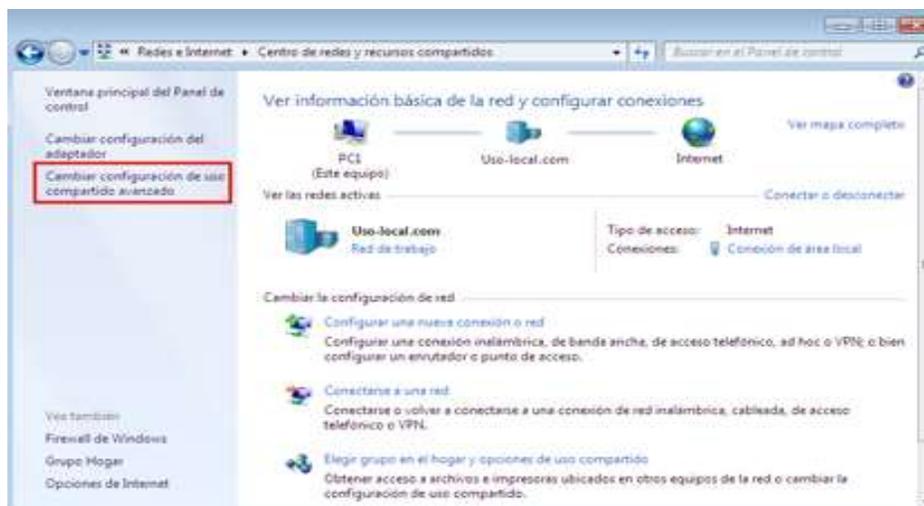
2. En la ventana del Panel de control, haz click en Redes e Internet.



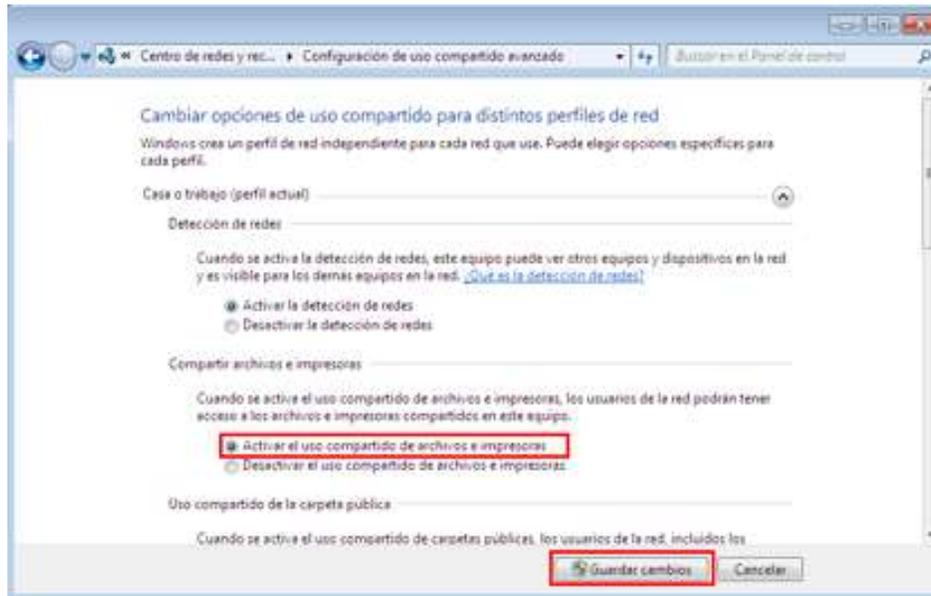
3. Haz click en Centro de redes y recursos compartidos.



4. Haz click en Cambiar configuración de uso compartido avanzado.

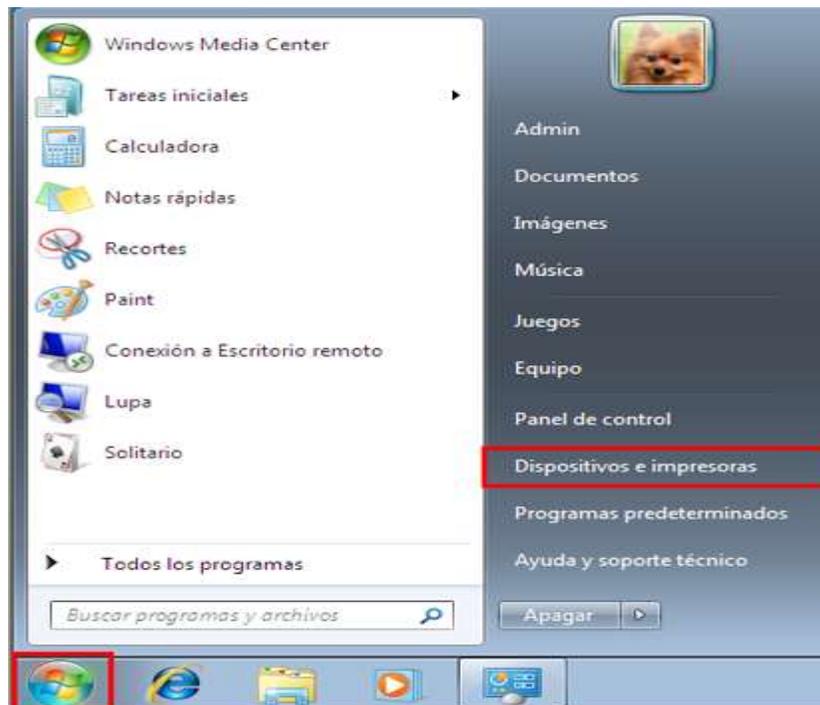


5. Marca la opción Activar el uso compartido de archivos e impresoras, y haz click en Guardar Cambios.

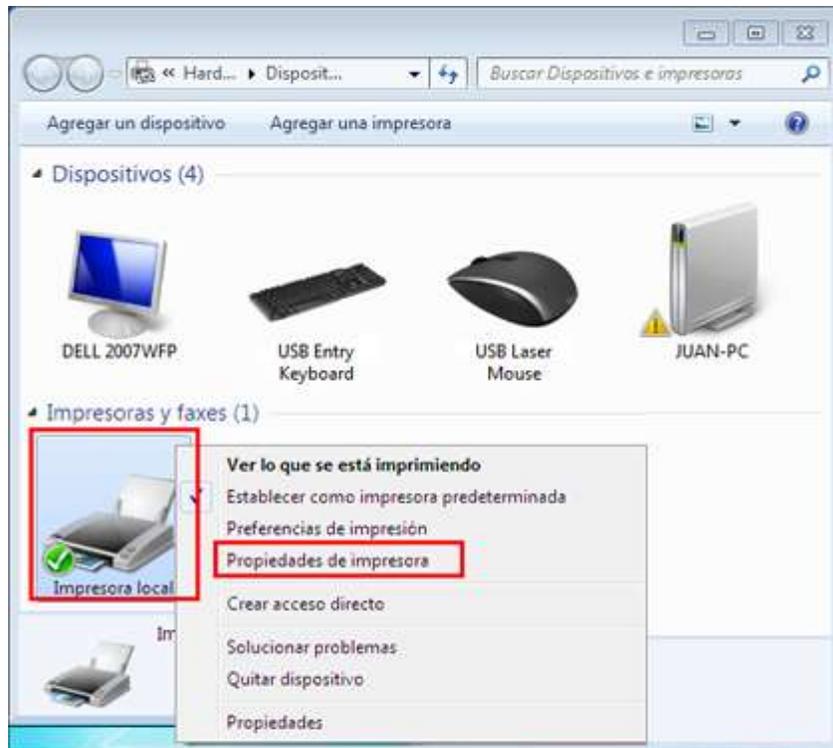


Instalación de Impresoras

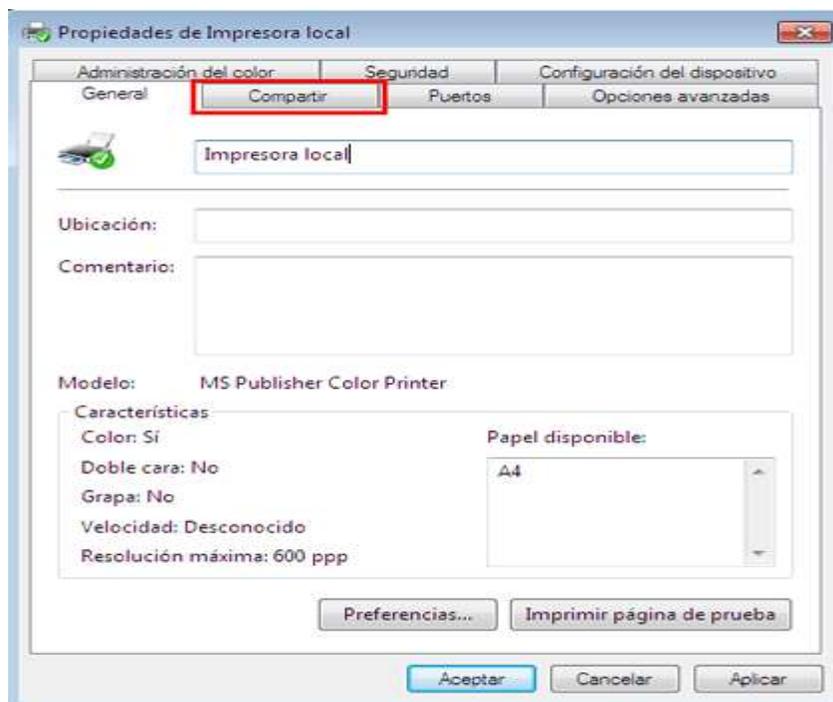
1. Haz click en Inicio  y luego en Dispositivos e impresoras.



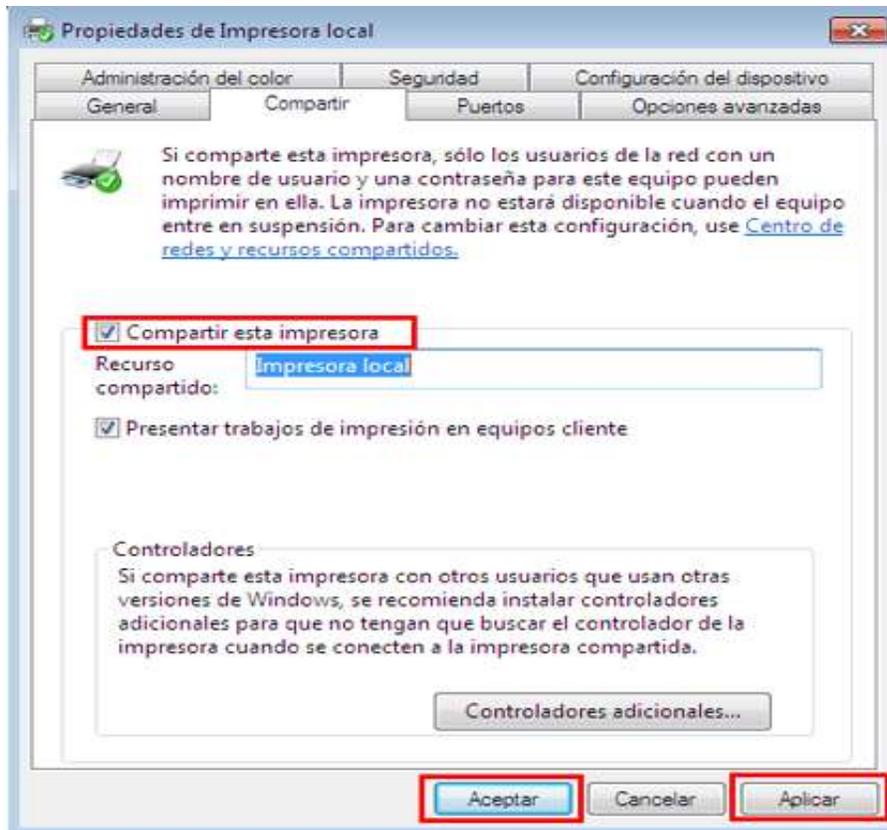
2. Haz click con el botón secundario del ratón en la impresora que desees compartir y haz click en Propiedades de impresora.



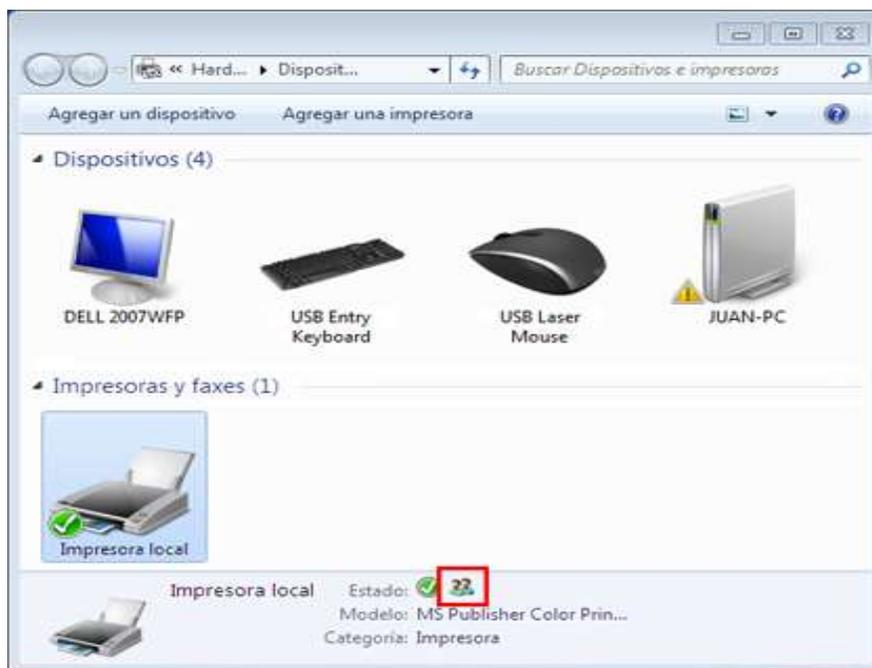
3. A continuación, haz click en la etiqueta Compartir.



4. En la etiqueta Compartir, haz click en Compartir esta impresora, luego en Aplicar y en Aceptar.



5. Ahora Windows indicará con un pequeño icono que la impresora ya se encuentra compartida.

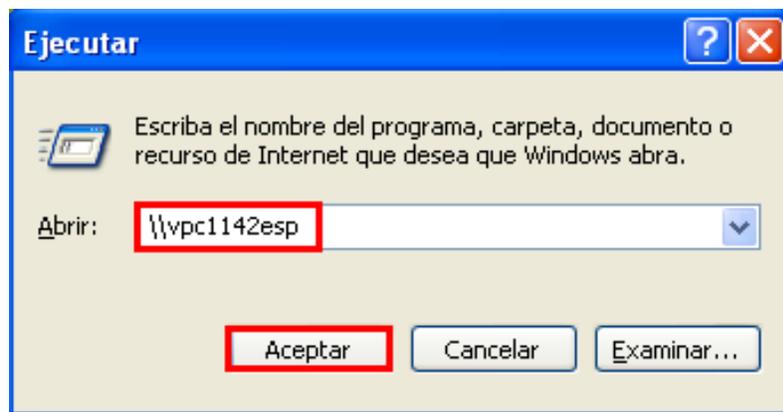


Cómo compartir una impresora en Windows XP. Ahora tendremos que conectar la Computadora B (con Windows XP) con la A (Windows 7)

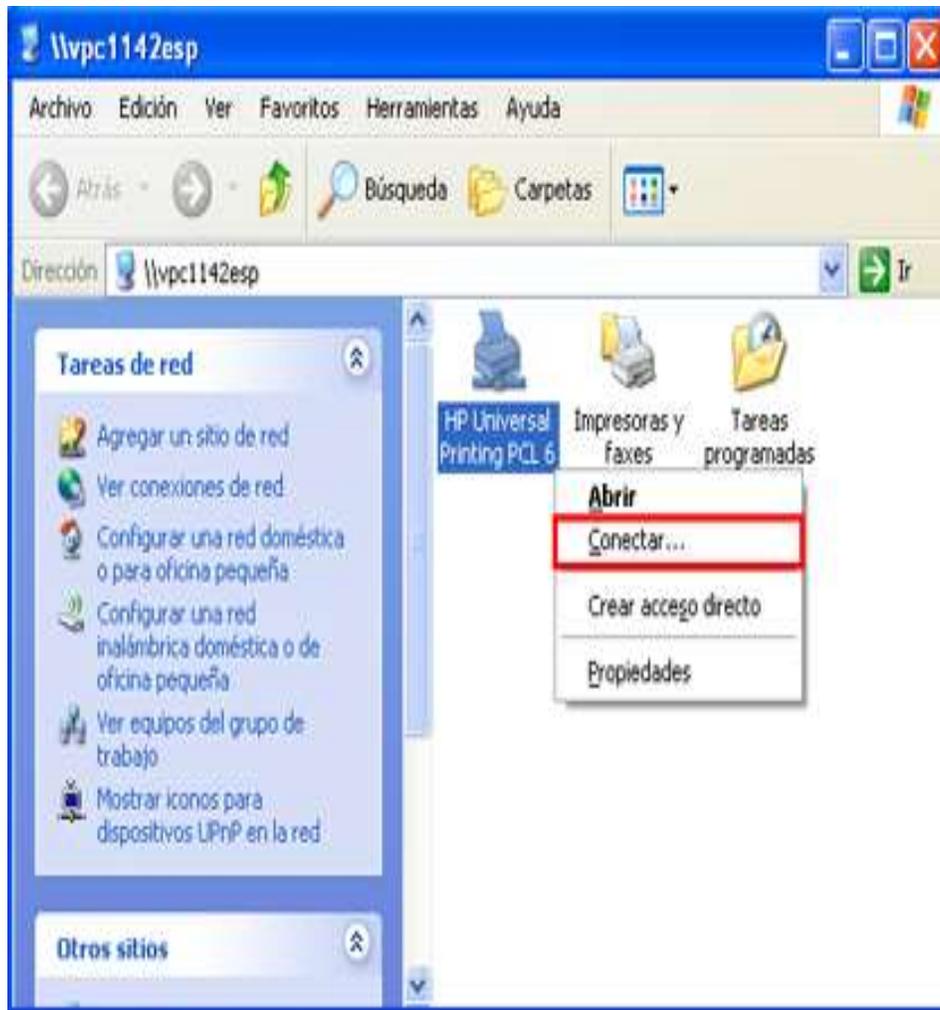
1. En la Computadora con Windows XP. Ve a **Inicio**, haz click en **Ejecutar**



2. En la ventana de Ejecutar escribe el nombre de la Computadora A empezando con "\\Nombre del equipo". En este ejemplo sería `\\vpc1142esp` y haz click en **Aceptar**.



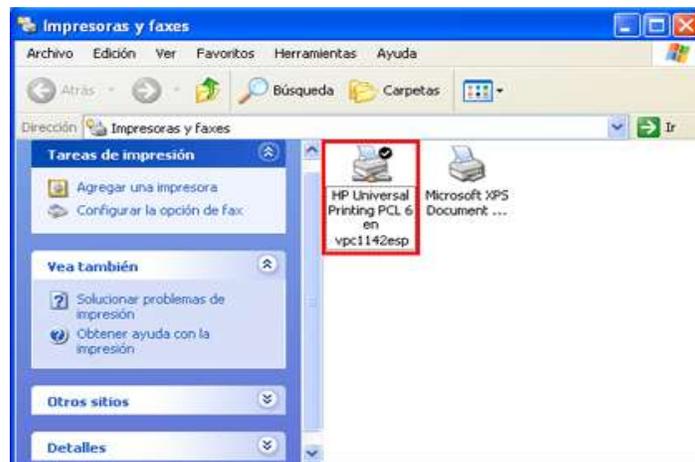
3. En la siguiente ventana haz click con el botón secundario en la impresora y selecciona **Conectar**.



4. Aparecerá un cuadro de diálogo preguntándote si quieres conectarte. Haz click en **Sí**.
5. Finalmente, la impresora quedará instalada en la computadora B lista para usarse como una local. Podrás ver en la lista de impresoras, la impresora que esta compartida.
6. Para ello:
 1. Ve a **Inicio**, haz click en **Impresoras y faxes**.



2. Podrás ver que la impresora aparece y está lista para usarse.



Nota: si tienes otra impresora como predeterminada, recuerda que si quieres usar la compartida tienes que hacer click con el botón secundario en ella y seleccionar la opción **Establecer como Impresora Predeterminada**.

Reporte de resultados de la práctica			
Nombre de la práctica			
Competencia que a desarrollar según el programa			
La práctica la realicé de manera:	Grupal	Individual	Fecha de realización
Desempeños que debo mostrar			
El producto obtenido en la práctica es:			
Lo que aprendí con la práctica			
Indicadores de la competencia que trabajé			
Dónde puedo aplicar lo aprendido			
Con qué contenidos de otras unidades de aprendizaje se relaciona			
En dónde encontré información complementaria para trabajar la práctica			
Cómo seleccioné la información utilizada			
Criterios con los que me evaluaron			
Qué más me gustaría aprender sobre el tema			

TEMA 08: REDES INALAMBRICAS

- ✓ 8.1 Redes inalámbricas wireless (Wi-Fi)
- ✓ 8.2 Como conectarse a una red inalámbrica

8.1 Redes Inalámbricas Wireless (Wi-Fi).

Wi-Fi es un sistema de envío de datos sobre redes computacionales que utiliza ondas de radio en lugar de cables. La tecnología WiFi permite crear redes inalámbricas, también conocidas como **wireless**. Las redes inalámbricas WiFi constituyen una tecnología de uso cada vez más generalizado por diversos **equipos informáticos: PCs, organizadores (PDA), consola de video juegos** e incluso las impresoras también utilizan la tecnología WiFi para facilitar su conexión.

Los siguientes se conocen como **tipos de redes inalámbricas WiFi**:

- **Ad-Hoc**: No es preciso contar con un punto de acceso que se encargue de la gestión de la red, por cuanto cada miembro de la red retransmite la información que recibe a los otros miembros. Este modo es aconsejable para uso en el hogar en el caso de una red simple, donde ofrece la ventaja adicional de la accesibilidad de su precio.
- **Infraestructura**: La gestión en este caso se centraliza en un punto de acceso, de tal manera que los datos que un host emite llegan al punto de acceso y éste los transfiere a los otros miembros de la red, ofreciendo economía en el ancho de banda. Además, se pueden conectar puntos de acceso entre sí (por cable o WiFi) para aumentar el alcance de la red WiFi. Este tipo es de uso más frecuente, por cuanto ofrece mayor seguridad en redes inalámbricas.

En cuanto a la **configuración de las redes inalámbrica WiFi**, los requerimientos mínimos para el efecto son:

- Un **router WiFi** o un punto de acceso - necesarios únicamente en el tipo anteriormente denominado infraestructura.



- Una o más tarjetas WiFi, las cuales usualmente se conectan a un puerto **USB, PCI o PCMCIA**. También existen adaptadores Ethernet / WiFi que son utilizados especialmente para las consolas de videojuegos que solo disponen de un puerto Ethernet.

Infortunadamente, la **tecnología de redes inalámbricas** enfrenta, como uno de sus más graves problemas, la progresiva saturación del espectro radioeléctrico, debida a la masificación de usuarios, lo cual tiene efectos adversos particularmente en las conexiones de larga distancia (mayor de 100 metros).

En realidad, Wi-Fi está diseñado para conectar ordenadores a la red a **distancias reducidas**, cualquier uso de mayor alcance está expuesto a un excesivo riesgo de interferencias. La instalación de redes inalámbricas WiFi sin consideración convierte dichas redes en redes abiertas, vale decir altamente vulnerables a los crackers, dejando desprotegida la información que por ellas circula.

Enunciamos a continuación las especiales **características de las redes inalámbricas** Wi-Fi, que igualmente representan las ventajas de una tecnología con expectativas de crecimiento incalculables, son ellas:

- Movilidad: desde cualquier sitio dentro de su cobertura, incluso en movimiento.
- Fácil instalación: más rapidez y simplicidad que la extensión de cables.
- Flexibilidad: permite el acceso a una red en entornos de difícil cableado.
- Facilidad: permite incorporar redes en lugares históricos sin necesidad de extender cable.
- Adaptabilidad: permite frecuentes cambios de la topología de la red y facilita su escalabilidad.



El estándar IEEE 802.11 se basa en el mismo marco de estándares que Ethernet. Esto garantiza un excelente nivel de interoperabilidad y asegura una implantación sencilla de las funciones y dispositivos de interconexión Ethernet/WLAN.

A menudo, las infraestructuras de comunicación basadas en esquemas de cableado tradicionales no son factibles debido a motivos técnicos o económicos. En estos casos, los productos inalámbricos se erigen como alternativas flexibles a las redes cableadas.

La tecnología inalámbrica también ofrece excelentes soluciones cuando se necesitan instalaciones de red temporales.

Éstas son algunas de las aplicaciones habituales de las redes WLAN:

- Redes temporales
- Motivos arquitectónicos (leyes urbanísticas, protección de edificios históricos, etc.)
- Aplicaciones móviles
- Soluciones de red flexibles
- LAN interconectadas

Los productos de red inalámbrica son seguros no sólo respecto a otros productos electrónicos y de red, sino, lo que es más importante, respecto a las personas. Los productos de redes inalámbricas, estandarizados como IEEE 802.11, se han diseñado para usarse en oficinas y otros lugares de trabajo. Por lo tanto, emiten un grado reducido de energía, lo cual es inofensivo. De hecho, los niveles de energía son significativamente más bajos que las emisiones de los teléfonos GSM comunes, que funcionan a unos 2 W en el caso de teléfonos de clase 2 GSM (intervalo de frecuencia de 880-960 MHz).



Bluetooth.

Bluetooth es la especificación "factor de alcance corto" "solución de radio a bajo costo," y permite la comunicación inalámbrica entre computadoras portátiles, celulares (móviles), impresoras, cámaras y otros aparatos electrónicos portátiles a través de una frecuencia de radio de alcance corto. Bluetooth permite conectarse e intercambiar de información de forma inalámbrica.

¿De dónde viene el nombre Bluetooth?

El nombre de Bluetooth viene de Harald Bluetooth, rey de Dinamarca -940-985- quien unificó a su país y lo convirtió al cristianismo y conquistó Noruega.

De acuerdo con los creadores de Bluetooth, Harald Bluetooth era reconocido por la habilidad de ayudar a las personas a comunicarse, haciendo de éste un nombre apropiado para su nuevo invento. Los logos de Bluetooth representan sus iniciales H y al B de las runas nórdicas.

Harald Bluetooth (Harald "Dientes Azules") fue un gran rey Vikingo que unió Dinamarca y Noruega en el siglo X. Su nombre quedará, no obstante, para siempre ligado a la tecnología revolucionaria que permite a los aparatos electrónicos trabajaren en conjunto sin necesidad de cables: el Bluetooth.

¿Qué es Bluetooth?

Es la norma que define un estándar global de comunicación inalámbrica, que posibilita la transmisión de voz y **datos** entre diferentes equipos mediante un enlace por radiofrecuencia.

Los principales objetivos que se pretende conseguir con esta norma son:

- Facilitar la comunicación entre equipos móviles y fijos.
- Eliminar cables y conectores entre estos.

- Ofrecer la posibilidad de crear pequeñas **redes inalámbricas** y facilitar la sincronización de datos entre equipos personales. La tecnología Bluetooth comprende hardware, software y requerimientos de interoperabilidad, por lo que para su desarrollo ha sido necesaria la participación de los principales fabricantes de los sectores de las telecomunicaciones y la informática, tales como: Ericsson, Nokia, Toshiba, IBM, Intel, 3Com, Agere, Ericsson y Microsoft.

Posteriormente se han ido incorporando muchas más compañías, y se prevé que próximamente los hagan también empresas de sectores tan variados como: automatización industrial, maquinaria, ocio y entretenimiento, fabricantes de juguetes, electrodomésticos, etc., con lo que en poco tiempo se nos presentará un panorama de total conectividad de nuestros aparatos tanto en casa como en el trabajo.

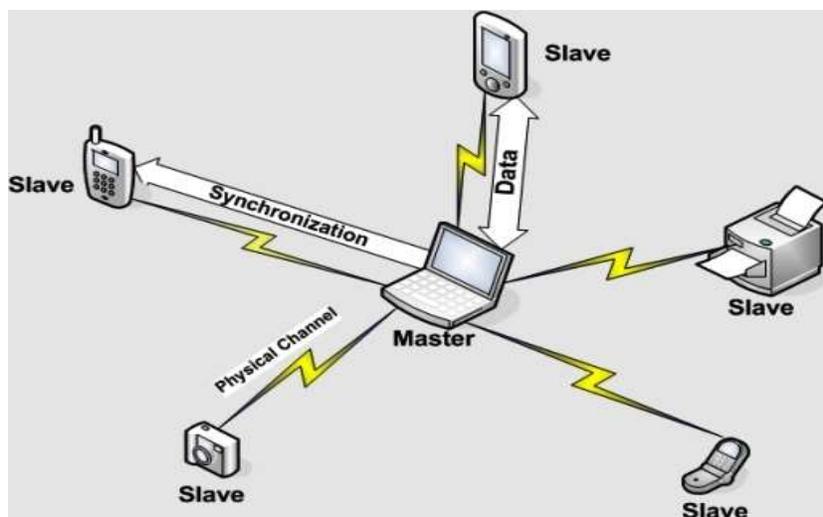
¿Cómo funciona Bluetooth?

El primer objetivo para los productos Bluetooth era los entornos de la gente de negocios. Por lo que se pensó en integrar el chip de **radio** Bluetooth en equipos como: ordenadores portátiles, teléfonos móviles, agendas electrónicas, auriculares... Esto generaba una serie de cuestiones previas que deberían solucionarse tales como:

- El **sistema** debería operar en todo el mundo.
- El emisor de radio deberá consumir poca energía, ya que debe integrarse en equipos alimentados por baterías.
- La conexión debería soportar voz y datos, y por lo tanto aplicaciones multimedia.

Para poder operar en todo el mundo es necesaria una banda de frecuencia abierta a cualquier sistema de radio independientemente del lugar del planeta donde nos encontremos.

Sólo la banda ISM (médico-científica internacional) de 2,45 GHz cumple con éste requisito, con rangos que van de los 2.400 MHz a los 2.500 MHz, y solo con algunas variaciones de ancho de banda en países como Francia, España y Japón, y no necesita licencia.

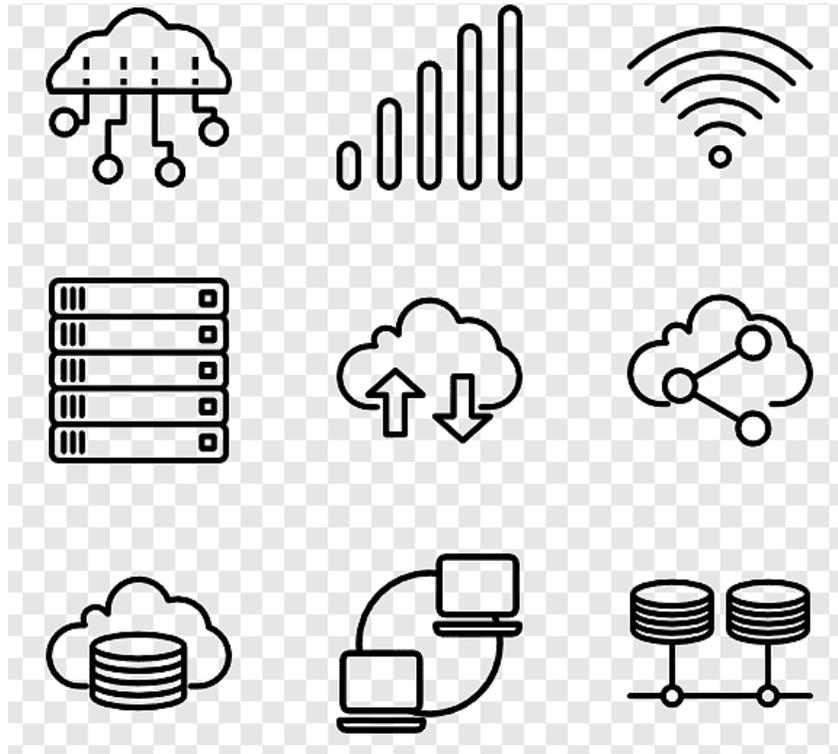


8.2 Como conectarse a una red inalámbrica.

Pasos para conectarse a una red inalámbrica:

Paso 1: barra de tarea

Iniciaremos buscando el icono de redes, que se encuentra en la barra de tareas, allí podremos saber si la máquina tiene la red desconectada o no ha sido instalada.



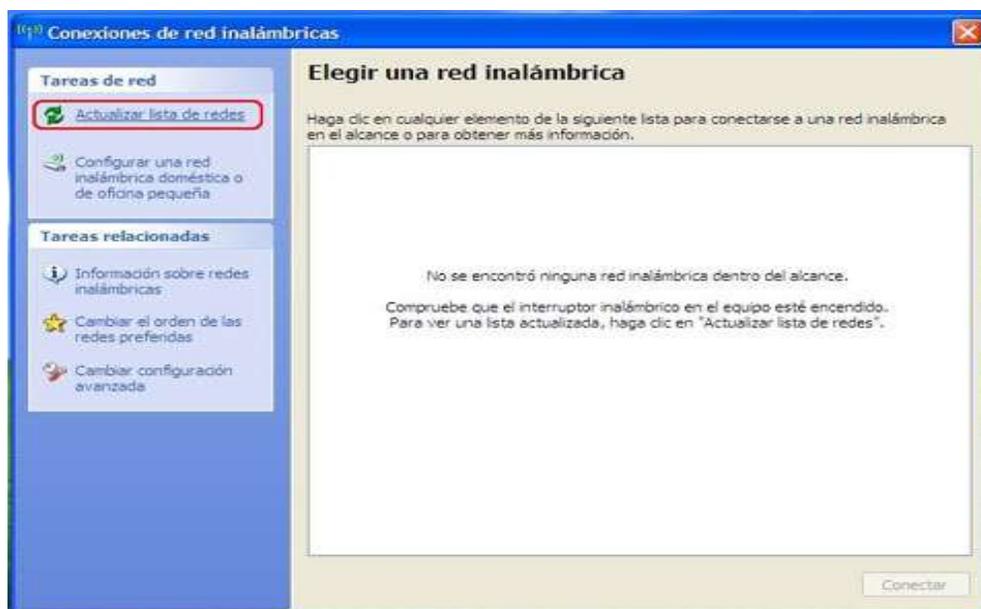
Paso 2: búsqueda de la red

Al encontrar el icono, damos click derecho sobre él y a continuación nos saldrá un menú textual, con varias opciones, de las cuales debemos seleccionar "ver redes inalámbricas disponibles".



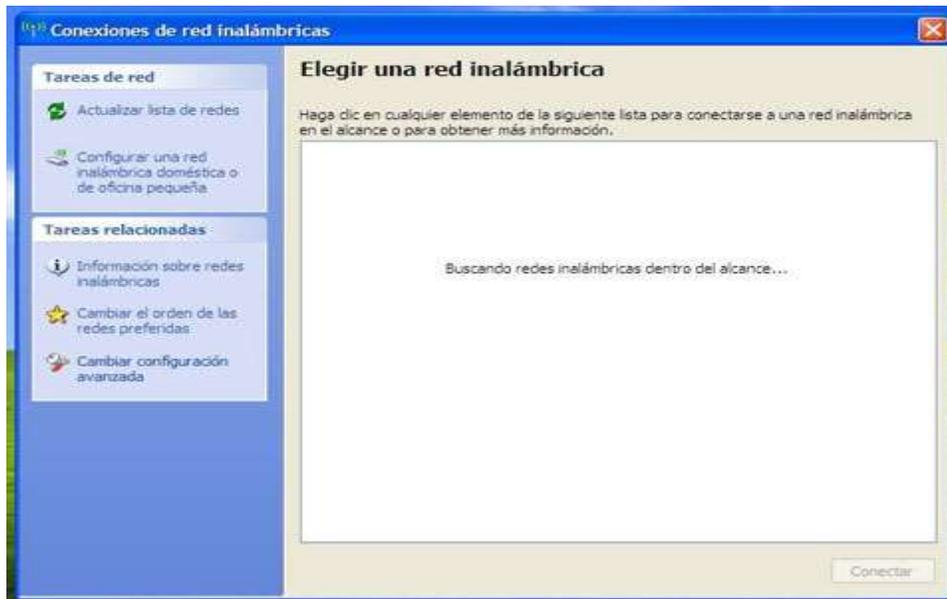
Paso 3: elegir red

En la ventana de conexiones de redes inalámbricas, debemos seleccionar la opción "elegir una red inalámbrica". Luego, seleccionamos la opción "actualizar lista de redes" con esto podremos ver las redes inalámbricas a las cuales tenemos alcance.



Paso 4: redes disponibles

Luego de realizar el tercer paso, aparecerá la ventana como la siguiente imagen que indica que está buscando las redes disponibles en tu computadora. Para que puedas efectuar los pasos siguientes. Puede que se demore un poco, pero no te preocupes en esta misma ventana te aparecerá el resultado.



Paso 5: datos para la configuración

Como ven se ha encontrado una red inalámbrica disponible, en este caso el nombre de prueba es "Palma Del Rio-WIRELESS". Luego, seleccionamos el botón "conectar".



En el caso de "Palma Del Rio-WIRELESS", es una red libre. Por lo que no necesita ninguna clave. Podemos pasarnos al Paso 8

Paso 6: clave

Al intentar conectarnos a esta red inalámbrica, nos solicita la clave de red para acceder a ella, la introducimos y luego seleccionamos nuevamente el botón "conectar".



Paso 7: asistente de conexión

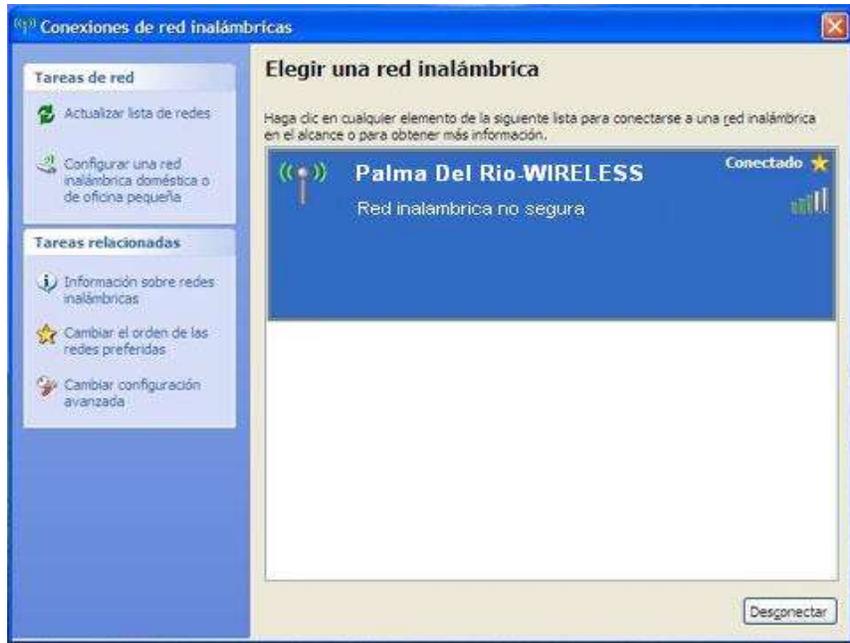
El asistente de conexión nos intentará conectar a la red seleccionada. Se completará si la clave de red introducida es correcta.



En nuestro caso continuamos por aquí.

Paso 8: red conectada

Si la red ha sido conectada exitosamente, nos aparecerán los detalles de la conexión en la siguiente ventana.



Paso 9: seleccionar estado

Regresamos a la barra de tareas nuevamente realizando el paso 2 y seleccionamos nuevamente el "estado".



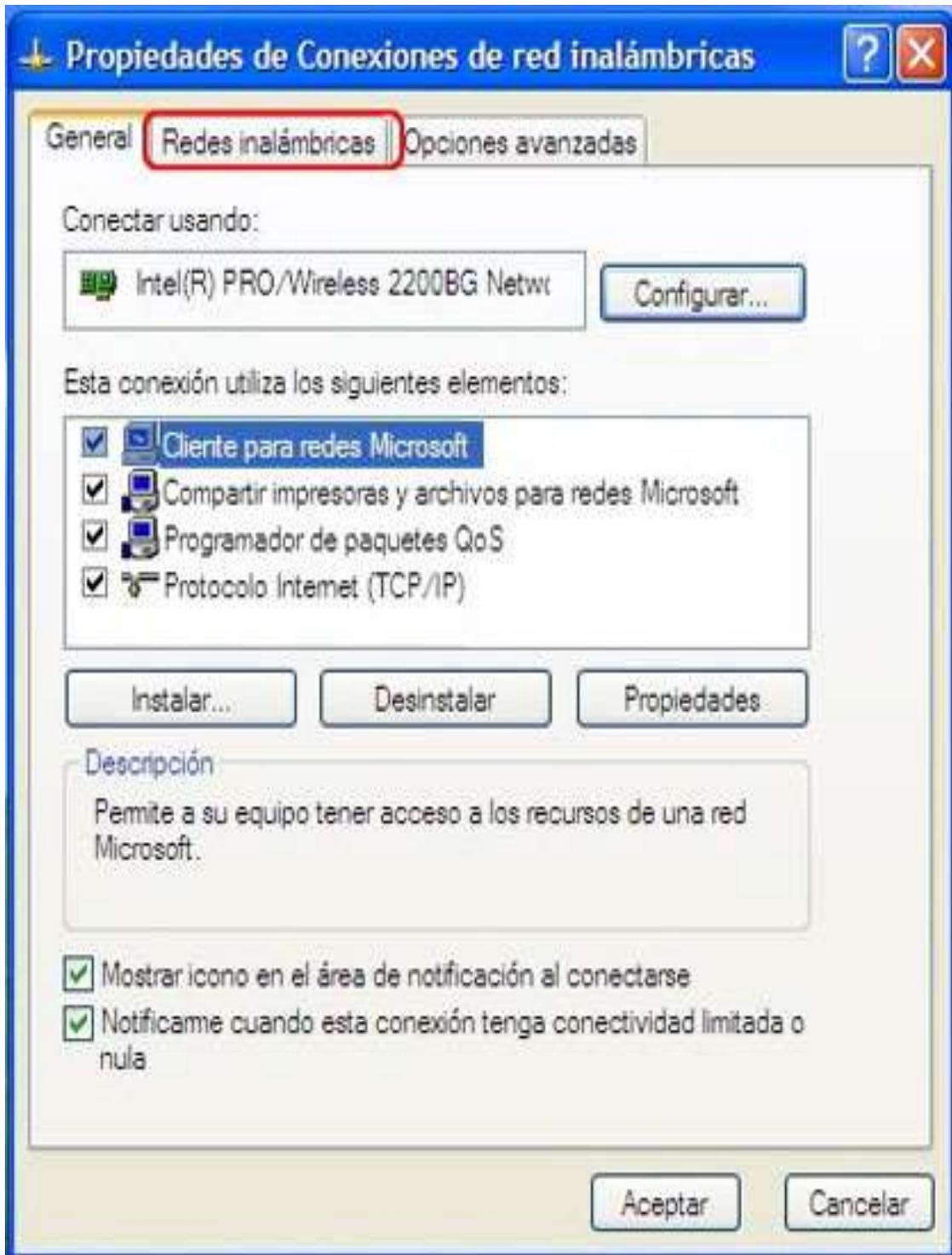
Pasó 10: velocidad de conexión

En la ventana de Estado de conexiones de las redes inalámbricas, nos muestra las características de la conexión: estado, red, duración, velocidad, intensidad de señal.



Paso 11: propiedades

Al seleccionar el botón de propiedades, nos aparecerá en la misma ventana el adaptador de red que se está utilizando y los tipos de componentes de red.



Paso 12: características

En la pestaña "Redes inalámbricas" podemos definir, si esta conexión que creamos se

conectará automáticamente. También, podemos agregar nuevas conexiones, quitar, o ver las propiedades.



Paso 13: opciones avanzadas

En la pestaña "Opciones avanzadas" se pueden definir las configuraciones de los cortafuegos o Firewall, definir si la conexión será compartida.



Este proceso puede ser aplicado tanto a computadoras de escritorio, portátiles y PDA's.

Reporte de resultados de la práctica			
Nombre de la práctica			
Competencia que a desarrollar según el programa			
La práctica la realicé de manera:	Grupal	Individual	Fecha de realización
Desempeños que debo mostrar			
El producto obtenido en la práctica es:			
Lo que aprendí con la práctica			
Indicadores de la competencia que trabajé			
Dónde puedo aplicar lo aprendido			
Con qué contenidos de otras unidades de aprendizaje se relaciona			
En dónde encontré información complementaria para trabajar la práctica			
Cómo seleccioné la información utilizada			
Criterios con los que me evaluaron			
Qué más me gustaría aprender sobre el tema			

Cámaras de vigilancia

Una de las principales aplicaciones en el uso de redes en la actualidad es la vigilancia mediante cámaras, las cuales pueden ser observadas de forma remota, ahora que ya conoces el funcionamiento y la instalación de redes es un hecho que puedes instalar este tipo de equipos, los cuales no requieren de un servidor, son accesibles en cuanto a costo, requieren un mínimo de materiales para su instalación y pueden conseguirse de forma sencilla. Este tipo de dispositivos pueden ser de manera desde un computador, Tablet, teléfono, etc., con la posibilidad de observar y/o vigilar de manera remota lo que pasa en el lugar donde se instala la cámara, existen muchas alternativas de modelos y tipos, haciendo viable la posibilidad de que ofrezcas el servicio de instalación a casas y/o negocios.



Dos principales tipos de cámaras de vigilancia

- Cámaras analógicas: estas cámaras son unidas por un cable coaxial a un televisor o un monitor, donde las imágenes se muestran. Envían flujos continuos de datos (barrido) a un dispositivo de almacenamiento (registrador digital).
- Cámaras IP: la cámara IP permiten una conexión a una red informática (conectada a Internet) o por cable Ethernet o por Wi-Fi (inalámbrica). Las imágenes filmadas pueden ser registradas y consultadas en tiempo real desde una PC o un smartphone vía Internet.

Utilizar una cámara IP

La instalación y la utilización de estas cámaras se desarrollan en cuatro etapas:

- Conectar la cámara de vigilancia al router: la utilización de un cable es necesaria en esta etapa.
- Encontrar y atribuir la dirección IP de la cámara (este paso necesita una contraseña, disponible en el equipo vendido).
- Colocar la cámara en un lugar estratégico.
- Una vez que el router esté sincronizado con la cámara, el flujo de imagen es accesible en línea mediante una página web (acceso protegido por contraseña).

Los elementos técnicos de una cámara de vigilancia

- Calidad de la imagen: para las cámaras IP, la calidad de la imagen es determinada por la resolución de visualización (1600 x 1200 píxeles = muy alta resolución).



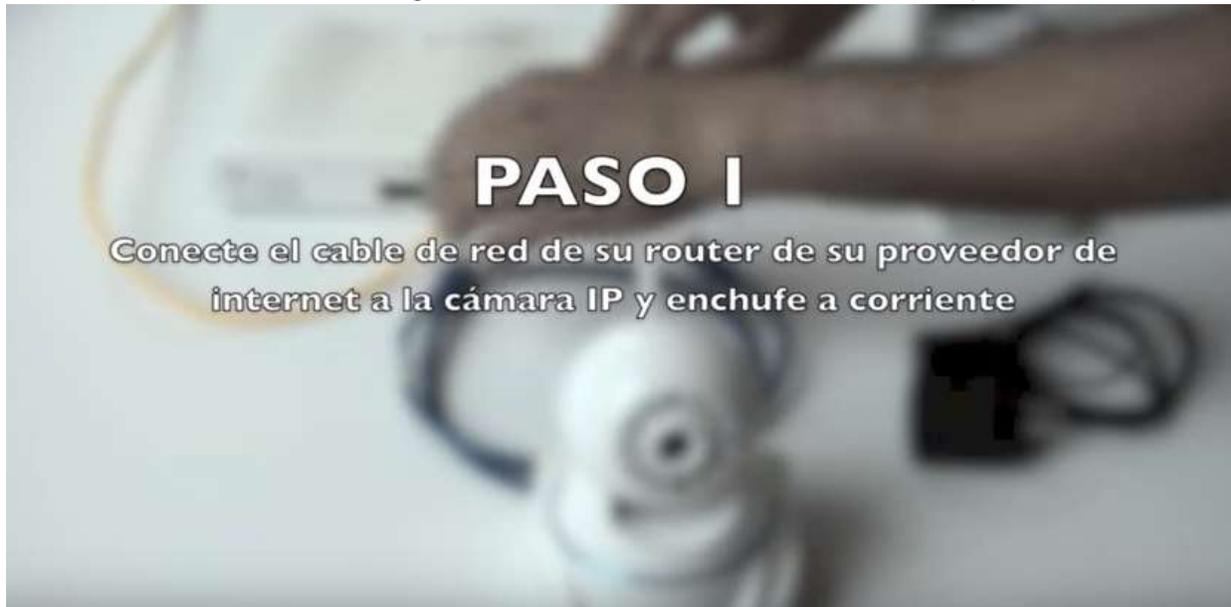
- El sensor: el elemento esencial, situado detrás del objetivo, que permite captar la luz.
- La luminosidad (lux): la luminosidad es expresada en lux (comprendida entre 0, la oscuridad total y 50 000 lux).
- El objetivo: varía según el ángulo deseado de visión.

Las diferentes categorías de cámara de vigilancia

- Cámaras infrarrojas: por la noche, utilizan los diodos emisores de luz (LEDs) colocados alrededor de su lente para detectar en los brillos infrarrojos (ondas de calor) y retransmitir las imágenes en blancas y negro.
- Cámaras para el día y la noche: se adaptan automáticamente en modo día o en modo noche según el nivel de luminosidad.
- Cámara discreta en forma de domo, domos motorizados (rotaciones posibles), cámaras espía (que se funden en el decorado).

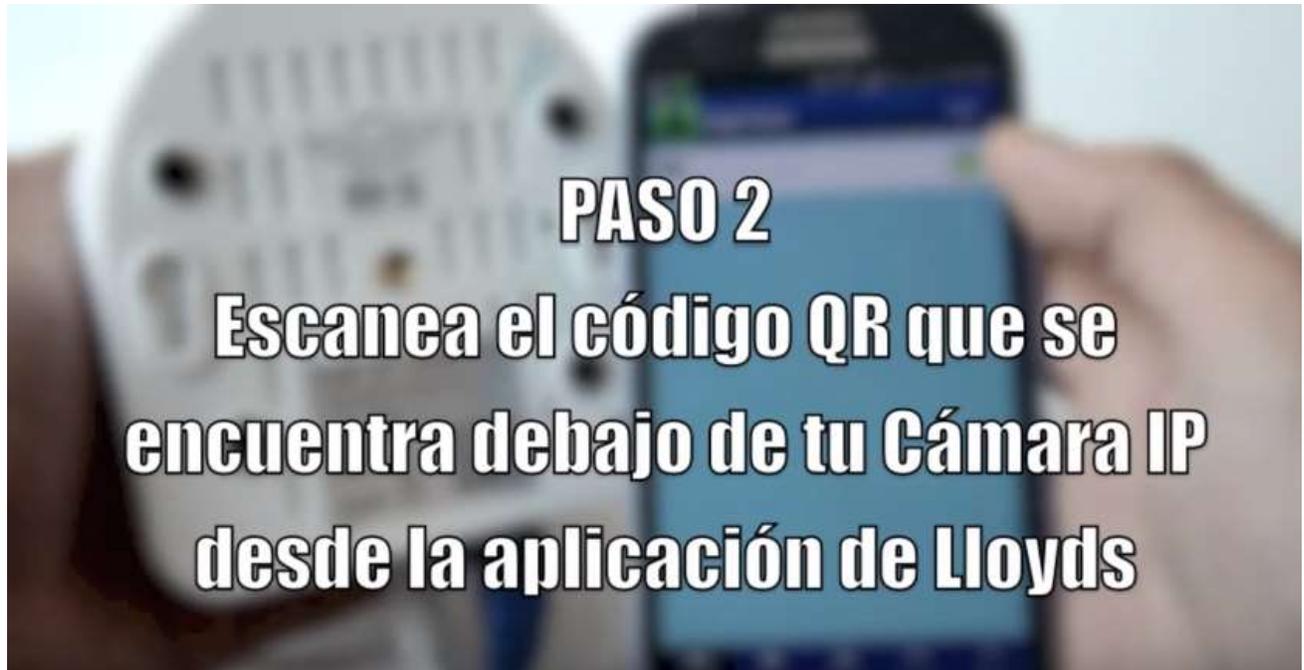


A continuación, el procedimiento para la instalación de una cámara IP, para un modelo de la marca Lloyd's, que se asemeja en gran medida a otras marcas de este tipo de cámara, con características de costo muy accesible, con movilidad de casi 360°, con audio en ambas vías, visión nocturna, fácil de conseguir en conocida cadena de tiendas con presencia nacional,



etc.





PASO 2

Escanea el código QR que se encuentra debajo de tu Cámara IP desde la aplicación de Lloyds



Paso 3

Visualiza y usa tu Cámara IP desde tu celular a través de tu red de datos WiFi, 3G/4G .

GLOSARIO

@: Arroba (en inglés significa "at" [en]). En las direcciones de e-mail, es el símbolo que separa el nombre del usuario del nombre de su proveedor de correo electrónico. Por ejemplo: pepe@hotmail.com.

Acceso directo: es un ícono que permite abrir más fácilmente un determinado programa o archivo.

ADSL: Asymmetric Digital Subscriber Line. Tecnología para transmitir información digital a elevados anchos de banda. A diferencia del servicio dial up, ADSL provee una conexión permanente y de gran velocidad. Esta tecnología utiliza la mayor parte del canal para enviar información al usuario, y sólo una pequeña parte para recibir información del usuario.

AGP: puerto acelerador de gráficos. Permite correr velozmente archivos gráficos tridimensionales.

AI: Artificial Intelligence: Inteligencia Artificial.

Algoritmo: conjunto de reglas bien definidas para la resolución de un problema. Un programa de software es la transcripción, en lenguaje de programación, de un algoritmo.

Amazon: librería mundial online. Ofrece más de un millón de títulos a través de Internet.

AMIBIOS: una de las marcas de BIOS más usadas.

Ancho de banda (bandwidth): expresa la cantidad de datos que pueden ser transmitidos en determinado lapso. En las redes se expresa en bps.

Antivirus: programa que busca y eventualmente elimina los virus informáticos que pueden haber infectado un disco rígido o disquete.

AOL: America Online: proveedor de servicios de Internet de los Estados Unidos.

Apache: servidor web de distribución libre. Fue desarrollado en 1995 y ha llegado a ser el más usado de Internet.

Archivo adjunto: archivo que acompaña un mensaje de e-mail. Es apropiado para el envío de imágenes, sonidos, programas y otros archivos grandes.

ARPA: Advanced Research Projects Agency: Agencia del Departamento de Defensa de los Estados Unidos que creó ARPAnet, la red que dio origen a Internet.

ARPAnet: Advanced Research Projects Agency Network: Red de comunicación desarrollada por ARPA a fines de la década de los 60. Se la considera el origen de la actual Internet.

ASCII: American Standard Code of Information Interchange: Código normalizado estadounidense para el intercambio de la información. Código que permite definir caracteres alfanuméricos; se lo usa para lograr compatibilidad entre diversos procesadores de texto. Se pronuncia "aski".

Attachement: archivo adjunto.

APC: Asociación para el Progreso de las Comunicaciones. Algunas de las redes que conforman dicha Asociación son: Alternex (Brasil), Fredsnaetet (Suecia), GreenNet (Inglaterra), Nicarao (Nicaragua), Peacenet/EcoNet/ConflicNet/HomeoNet (USA), Pegasus (Australia) y Web (Canadá).

Asincrónico: Forma y estilo de transmisión de datos en la cual el envío y la recepción no están sincronizadas.

Bandeja de entrada: buzón de entrada.

Base de datos: conjunto de datos organizados de modo tal que resulte fácil acceder a ellos, gestionarlos y actualizarlos.

Bit: abreviatura de binary digit (dígito binario). El bit es la unidad más pequeña de almacenamiento en un sistema binario dentro de una computadora.

Bookmark: anotación, en el navegador, de una dirección de Internet que se almacena para agilizar su uso posterior. En el programa Internet Explorer, se llama "Favoritos".

Qboot (butear): cargar el sistema operativo de una computadora.

Bps: bits por segundo.

Browser: navegador.

Buffer: área de la memoria que se utiliza para almacenar datos temporariamente durante una sesión de trabajo.

Bug: bicho, insecto. Error de programación que genera problemas en las operaciones de una computadora.

Bus: enlace común; conductor común; vía de interconexión. Método de interconexión de dispositivos mediante una sola línea compartida.

Bus serial: método de transmisión de un bit por vez sobre una sola línea. (Véase bus y serial.)

Buscador, motor de búsqueda: search engine. Es un programa, ubicado en un sitio de Internet, que recibe un pedido de búsqueda, lo compara con las entradas de su base de datos y devuelve el resultado. Algunos de los más conocidos: Yahoo, Altavista, Lycos, Infoseek.

Buzón de entrada: carpeta de un programa de e-mail donde aparecen los mensajes recibidos.

Buzón de salida: carpeta de un programa de e-mail donde aparecen los mensajes enviados.

By default: por defecto; predeterminado.

Byte: unidad de información utilizada por las computadoras. Cada byte está compuesto por ocho bits.

Bell standards: Modem standart de los Estados Unidos, desarrollado por Bell.

Binario: Archivo de computadora no textual.

Bulletin Board System (BBS): Sistema que trabaja en un computador brindando servicios, consulta a documentos organizados por temas (forums), acceso al sistema operativo del computador para poder dar comandos, etc. Aunque el acceso suele ser vía modem, también se puede operar el sistema localmente.

Cablemódem: Dispositivo que permite conectar una computadora a Internet a través de la conexión de coaxil de la televisión por cable. No es realmente un módem ya que no debe modular/demodular porque el sistema es puramente digital. Se perfila como una de las posibilidades de conexión que resolverían la problemática del limitado ancho de banda que se puede obtener a través de una conexión telefónica. Ver DirectPC.

Cache: Almacenamiento intermedio o temporario de información. Por ejemplo, un navegador posee un cache donde almacena las últimas páginas visitadas por el usuario y, si alguna se solicita nuevamente, el navegador mostrará la que tiene acumulada en lugar de volver a buscarla en Internet. El término se utiliza para denominar todo depósito intermedio de datos solicitados con mayor frecuencia. Ver Proxy Server.

Chat: Sistema de conversación en línea que permite que varias personas de todo el mundo conversen en tiempo real a través de sus teclados. Existen varios sistemas de chat, uno de los más difundidos es el IRC.

Click-throughs: Sistema de medición que almacena la cantidad de veces que un cliente potencial hace click en un banner de publicidad y visita el sitio del anunciante. Utilizado como métrica para la venta de espacios de publicidad en los sitios Web.

Conexión remota: Tipo de comunicación que permite acceder a un computador remoto como si se tratase de una terminal local del mismo.

Cookies (galletitas): Pequeños archivos con datos que algunos sitios Web depositan en forma automática en las computadoras de los visitantes. Lo hacen con el objetivo de almacenar allí información sobre las personas y sus preferencias. Por ejemplo, la primera vez que un navegante visita un site y completa algún formulario con sus datos y perfil, el sistema podrá enviarle una cookie al asignarle una identificación. Cuando el usuario retorne, el sitio Web pedirá a la computadora cliente la cookie y, a través de ella, lo reconocerá.

Cracker (pirata informático): Persona que se especializa en violar medidas de seguridad de una computadora o red de computadoras, venciendo claves de acceso y defensas para obtener información que cree valiosa. El cracker es considerado un personaje ruín y sin honor, a diferencia del hacker. Ver Firewall.

Cross-platform (multi-plataforma): Programa o dispositivo que puede utilizarse sin inconvenientes en distintas plataformas de hardware y sistemas operativos. Un programa en lenguaje Java posee esta característica.

CSLIP (Compressed Serial Line Internet Protocol, Protocolo Internet Comprimido para Líneas Seriales) Una variante comprimida del protocolo SLIP, que permite una conexión vía módem más rápida.

Hit (acceso o pedido): Unidad de medición de accesos ha determinado recurso. Forma de registrar cada pedido de información que un usuario efectúa a un server. Por ejemplo, en el caso de un sitio Web, la solicitud de cada imagen, página y frame genera un hit. Por lo tanto, para conocer en realidad cuántos accesos hubo, debe dividirse la cantidad de hits por la cantidad de objetos independientes (texto, frames e imágenes) que una página contiene, o usar un contador de accesos.

Hipertexto: Concepto y término inventado por Ted Nelson en 1969. Nelson era un famoso visionario de la informática que investigó durante 25 años, las posibilidades de interacción entre las computadoras y la literatura. Uno de los conceptos básicos para el desarrollo de la WWW. El hipertexto es una forma diferente de organizar información. En lugar de leer un texto en forma continua, ciertos términos están unidos a otros mediante relaciones (enlaces o links) que tienen entre ellos. El hipertexto permite saltar de un punto a otro en un texto, y a través de los enlaces (con un simple click sobre las palabras subrayadas y en negrita), permite que los navegantes busquen información de su interés en la Red, guiándose por un camino distinto de razonamiento. Algunos programas muy difundidos, como la Ayuda de Windows o las enciclopedias en CD-ROM, están organizadas como hipertextos.

Home page (página principal o, de entrada): Página de información de la Web, escrita en HTML. En general, el término hace referencia a la página principal o de acceso inicial de un site.

Host: Actualmente, sinónimo de servidor. Computador central con el cual se comunican otros computadores de menor jerarquía y usualmente de menores recursos.

Hosting Ver Farming.

Hostname (nombre de un host): Denominación otorgada por el administrador a una computadora. El hostname es parte de la dirección electrónica de esa computadora, y debe ser único para cada máquina conectada a Internet.

HTML (HyperText Markup Language, Lenguaje de Marcado de Hipertextos) Lenguaje que define textos, subgrupo del SGML, destinado a simplificar la escritura de documentos estándar. Es la base estructural en la que están diseñadas las páginas de la World Wide Web. Su definición está a cargo del Web Consortium.

HTTP (HyperText Transfer Protocol, Protocolo de Transferencia de Hipertexto) Es el mecanismo de intercambio de información que constituye la base funcional de la World Wide Web.

Hyperdocuments (Hiperdocumentos) Documento que tiene estructura de hipertexto, pero contiene además referencias a objetos multimediales (como sonidos, imágenes, videos).

Hyperlink: Enlace entre dos nodos de un hipertexto.

Intercambio de archivos: Transmisión de volúmenes de información en forma rápida y confiable.

IAB (Internet Activities Board, Panel de Actividades de Internet) Comité coordinativo creado para el diseño, ingeniería y administración de Internet. Supervisa al IETF.

IANA (Internet Assigned Numbers Authority, Autoridad de Asignación de Números de Internet)

Organismo que asigna los números IP a las instituciones que desean participar de Internet. Actualmente funciona junto a Internic.

IETF (Internet Engineering Taskforce. Fuerza de trabajo de Ingeniería de Internet) Gran comunidad abierta de ingenieros, operadores, vendedores e investigadores cuyo propósito es coordinar la operación, administración y evolución de Internet. Más datos en <http://www.ietf.org/>

IMO (In My Opinión, En Mi Opinión) Una de las siglas utilizadas en los mensajes de Internet. También

IMHO (In My Humble Opinión, En Mi Humilde Opinión).

Impressions (visualizaciones) Unidad de medida que verifica cuántas veces un navegante ve un determinado banner de publicidad.

Inteligencia Artificial (Artificial Intelligence o AI) Rama de la computación que analiza la computadora y sus posibilidades de poseer inteligencia. La IA estudia las habilidades inteligentes de razonamiento, capacidad de extracción de conclusiones y reacciones ante nuevas situaciones de las computadoras y sus programas. El razonamiento es parecido al del cerebro humano (no es lineal, se aprende de cada situación). Existen dos ramas de la IA: la fuerte (strong) sostiene que llegará el día en que puedan construirse programas que sean realmente inteligentes y computadoras pensantes. La débil (weak) considera que las computadoras sólo pueden ser diseñadas para convertirse en importantes herramientas para modelar y simular el pensamiento humano.

Interficie (Interfaz): Cara visible de la pantalla. Aquello que interactúa con los usuarios en los programas de informática, los videojuegos o la red Internet. La interficie abarca las superficies de las pantallas y su diseño, pero también el lenguaje usado por las

personas que interactúan, los botones y los mensajes de error, entre otros aspectos de la comunicación persona - ordenador - persona.

Internet Address: Sinónimo de número IP. Número asignado que identifica a un server en Internet. Está compuesto por dos o tres partes: número de red, número opcional de sub-red y número de host. Ver direcciones electrónicas, DNS.

Internet Worm: Programa similar a un virus de computadora creado por Robert Morris, un estudiante de Cornell University que fue famoso en 1988. El Worm se aprovechó de una falla de seguridad de un programa de e-mail muy utilizado y causó desastres al reproducirse sin límite, infectando y luego dejando catatónicas a la mayor parte de las computadoras conectadas a Internet. El pánico causado por el virus fue tan grande que generó el nacimiento de varios organismos dedicados a investigar las fallas de seguridad de los programas.

Internets: La red de computadoras más extendida del planeta, que conecta y comunica a más de 50 millones de personas. Nació a fines de los años sesenta como ARPANet y se convirtió en un revolucionario medio de comunicación. Su estructura técnica se basa en millones de computadoras que ofrecen todo tipo de información. Estas computadoras, encendidas las 24 horas, se llaman servidores y están interconectadas entre sí en todo el mundo a través de diferentes mecanismos de líneas dedicadas. Sin importar qué tipo de computadoras son, para intercomunicarse utilizan el protocolo TCP/IP. Las computadoras que utilizan las personas para conectarse y consultar los datos de los servidores se llaman clientes, y acceden en general a través en un tipo de conexión llamado dial-in, utilizando un módem y una línea telefónica.

Internet: Denomina un grupo interconectado de redes locales, que utilizan un mismo protocolo de comunicación.

InterNIC (Internet Network Information Centre, Centro de Información de Red de Internet) Centro de información que almacena documentos de Internet: RFCs y borradores de documentos. Organismo que se ocupa de otorgar grupos de números IP y direcciones electrónicas a cada organización que desee conectarse a Internet, garantizando que sean únicas. Más datos en <http://www.internic.net/>.

Intranet: Utilización de la tecnología de Internet dentro de la red local (LAN) y/o red de área amplia (WAN) de una organización. Permite crear un sitio público donde se centraliza el acceso a la información de la compañía. Bien utilizada, una intranet permite optimizar el acceso a los recursos de una organización, organizar los datos existentes en las PCs de cada individuo y extender la tarea colaborativa entre los miembros de equipos de trabajo. Cuando una intranet extiende sus fronteras más allá de los límites de la organización, para permitir la intercomunicación con los sistemas de otras compañías, se la llama Extranet.

IP (Internet Protocol): Protocolo de Internet definido en el RFC 791. Confirma la base del estándar de comunicaciones de Internet. El IP provee un método para fragmentar (deshacer en pequeños paquetes) y rutear (llevar desde el origen al destino) la información. Es inseguro, ya que no verifica que todos los fragmentos del mensaje lleguen a su destino sin perderse en el camino. Por eso, se complementa con el TCP.

IP Número o dirección (IP address) Dirección numérica asignada a un dispositivo de hardware (computadora, router, etc.) conectado a Internet, bajo el protocolo IP. La dirección se compone de cuatro números, y cada uno de ellos puede ser de 0 a 255, por ejemplo 200.16.232.123. Esto permite contar con hasta 256 elevado a los 4 números para asignar a las computadoras: cerca de 4 mil millones. Las direcciones IP se agrupan

en clases. Para convertir una dirección IP en una dirección electrónica humana (por ejemplo, <http://www.37sur.com/> se utilizan los DNS.

IPv6 (IP versión 6) Propuesta para aumentar los números IP disponibles, utilizando seis grupos de números en lugar de cuatro. Probablemente sea válido a partir de 1998. Más información sobre este nuevo estándar en <http://www.cis.ohio-state.edu/htbin/rfc/rfc1885.html>.

IRC (Internet Relay Chat) Uno de los sistemas más populares de charlas interactivas (chats) de múltiples usuarios vía Internet. Permite que miles de personas de todo el mundo se reúnan a "conversar" simultáneamente en forma escrita.

IRTF (Internet Research Taskforc, Equipo de Investigación de Internet) Comunidad de investigadores de redes, generalmente enfocados a Internet. Dedicados al avance tecnológico de la Red y asociados a la ISOC.

ISDN (Integrated Sevices Data Network, Red Digital de Servicios Integrados) Tecnología rápida de conexión para líneas dedicadas y transmisión de datos. Se utiliza para tener acceso a Internet o a una videoconferencia. Si bien esta tecnología existe hace varios años, aún se encuentra poco difundida.

ISOC (Internet Society, Sociedad Internet) Asociación civil sin fines de lucro integrada por profesionales, técnicos, investigadores y gente interesada en colaborar en la difusión, desarrollo y organización de la comunidad Internet. Está constituida por capítulos (chapters), es decir, asociaciones regionales. Para más información <http://www.isoc.org/>, ISP (Internet Service Provider, Proveedor de servicios de Internet) Ver Provider.

Java: Lenguaje de programación creado por Sun Microsystems. Desde su aparición, Java se perfila como un probable revolucionario de la Red. Como lenguaje es simple, orientado a objetos, distribuido, interpretado, robusto, seguro, neutral con respecto a la arquitectura, portable, de alta performance, multithreaded y dinámico. Java es un lenguaje de programación, un subset seguro de C++. Subset, porque algunas instrucciones (como las que tienen que ver con la administración de memoria) no se pueden usar. Seguro, porque agrega características de seguridad a los programas. Un applet de Java se baja automáticamente con la página Web y es compilado y ejecutado en la máquina local. Permite, entre otras cosas, agregar animación e interactividad a una página Web, pero su característica más importante es que un programa escrito en Java puede correr en cualquier computadora. Para más datos <http://java.sun.com/>.

Javascript: Lenguaje de scripts para utilizar en páginas Web desarrollado por Netscape. Permite aumentar la interactividad y la personalización de un sitio.

LAN (Local Area Network, Red de Area Local) Red de computadoras interconectadas, distribuida en la superficie de una sola oficina o edificio. También llamadas redes privadas de datos. Su principal característica es la velocidad de conexión. Ver WAN y MAN.

Latencia: Lapso necesario para que un paquete de información viaje desde la fuente hasta su destino. La latencia y el ancho de banda, juntos, definen la capacidad y la velocidad de una red.

Latency: Ver Latencia.

Línea dedicada (Leased line) Forma de conexión a Internet (con acceso las 24 horas) a través de un cable hasta un proveedor de Internet. Esta conexión puede ser utilizada por varias personas en forma simultánea.

Link: Ver Enlaces.

Listas de interés: Ver Mailing List.

List serv: Software robot usado para la administración de un servidor de mailing list. Ampliamente utilizado.

Log: Archivo que registra movimientos y actividades de un determinado programa (log file). Utilizado como mecanismo de control y estadística. Por ejemplo, el log de un Web server permite conocer el perfil de los visitantes a un sitio Web.

Login: Proceso de seguridad que exige que un usuario se identifique con un nombre (user-ID) y una clave, para poder acceder a una computadora o a un recurso. Ver Telnet.

Linx: Browser de Web en modo texto, que no permite ver imágenes. Aún es ampliamente utilizado por quienes navegan desde estaciones UNIX.

Mail Robot (auto responder) Programa que responde e-mail en forma automática, enviando al instante información. Simplifica la tarea de administrar un correo. Los programas utilizados para administrar mailing lists son un tipo de mail robots.

Mailing List (listas de interés) Modo de distribución de e-mail grupal. Mecanismos de debate grupales entre distintas personas interesadas en un determinado tema. Similares en concepto a los newsgroups, pero no es necesario utilizar un servidor especial ya que los mensajes son recibidos por el usuario como correo electrónico.

Majordomo: Uno del software de tipo mail robot usado para la administración de una mailing list.

MAN (Metropolitan Area Network, Red de Area Metropolitana) Red que resulta de varias redes locales (LANs) interconectadas por un enlace de mayor velocidad o backbone (por ejemplo, de fibra óptica) en varias zonas. Es el tipo de estructura de red que se utiliza, por ejemplo, en un campus Universitario, donde se conectan los diversos edificios, casas de estudiantes, bibliotecas y centros de investigación. Una MAN ocupa un área geográfica más extensa que una LAN, pero más limitada que una WAN.

Mensajes interactivos: Intercambio de información breve transmitido en forma inmediata entre personas conectadas simultáneamente.

MIME (Multipurpose Internet Mail Extensions, Extensiones Multipropósito para e-mail) Formato específico de codificación para la transferencia de correo electrónico y attachments entre dos computadoras; contiene cualquier tipo de datos. Más moderno que el UUEncoding; aunque menos difundido.

Modem local: Es el módem que se encuentra en su computadora, desde el cual Ud. realiza la llamada al módem remoto.

Modem remoto: Es el módem que se encuentra en otra computadora, a la cual Ud. llamará para comunicarse desde su módem local.

Moos (Multiuser Object Oriented MUDDs) Similares a los Mudds.

Mosaic: Primer browser de gran difusión, utilizado para navegar la Web. Desarrollado en febrero de 1993 por Marc Andreessen, fundador luego de la empresa Netscape.

Motor de búsqueda Ver Buscador.

Mudd (Multi user Dungeons & Dragons, castillos multi-usuarios) Conjunto de juegos virtuales de texto para jugar a través de Internet. Originados en las universidades y basados en los llamados juegos de rol (role-playing games). Consisten en "universos" virtuales con cientos de partes, definidos por programadores, donde los participantes deben resolver acertijos y enigmas, muchas veces con la ayuda de otros jugadores.

Multimedia Combinación de varias tecnologías de presentación de información (imágenes, sonido, animación, video, texto) con la intención de captar tantos sentidos humanos como sea posible. Previamente a la existencia de la multimedia, el

intercambio de información con las computadoras estaba limitado al texto. Luego, con el nacimiento de las interfaces de usuario gráficas y los desarrollos en video y sonido, la multimedia permitió convertir el modo de comunicación entre personas y dispositivos aumentando la variedad de información disponible. El uso de la multimedia fue la razón principal por la que la World Wide Web facilitó la difusión masiva de Internet.

Navegar: Recorrer la Web, sin destino fijo, siguiendo enlaces o direcciones.

Navegador: Ver Browser/Web browser.

Netiquette: Reglas de etiqueta, usos y buenas costumbres de Internet. Surgieron como una serie de políticas informales de "buen comportamiento", y se difunden de usuario en usuario para mantener vivo el espíritu de respeto propio de la Red. Un ejemplo de estas reglas es no escribir mensajes de correo electrónico todo en letras MAYUSCULAS, ya que equivale a ¡GRITAR!

Newsgrups (grupos de debate) Mecanismos de debate grupales entre personas de todo el mundo interesadas en un determinado tema. Permiten crear mensajes públicos, que los usuarios pueden crear, leer y contestar. Son distribuidos diariamente por toda Internet. También es el área en la que se agrupan los mensajes públicos según su temática. Similares en concepto, aunque no en funcionamiento, a las mailing lists.

Nickname (Nick, sobrenombre o alias) Nombre de fantasía que un usuario de Internet utiliza, por ejemplo, para participar de un Chat.

Request (pedido) Solicitud de información o datos que una computadora cliente efectúa a un servidor.

RFC (Request For Comment, pedido de comentario) Documentos a través de los cuales se proponen y efectúan cambios en Internet, en general con orientación técnica. Los RFC son formularios con una estructura determinada, que pueden ser generados y distribuidos por cualquier persona que tenga una buena idea para cambiar o mejorar algún aspecto de Internet. Las propuestas que contienen estos documentos se analizan, modifican y se someten a votación. Si resultan útiles, son puestas en práctica, convirtiéndose así en normas de Internet. La mayoría de los aspectos técnicos de la Red nacieron primero como RFCs, por eso hoy en día hay cientos de ellos. Se puede consultar una base de datos en hipertexto de los RFC en <http://www.auc.dk/RFC>.

SSL (Secure Socket Layer, Capa de Seguridad) Estándar para transacciones electrónicas encriptados que está siendo ampliamente utilizado para hacer negocios vía la Red. Ver SET.

Standard. Ver Norma.

Streaming (Transferencia Continua) Sistema de envío continuo de información, que permite, por ejemplo, ver un video a medida que se baja de la Red.

Stylesheets (hojas de estilo): Novedosa facilidad de HTML, similar a la que poseen los procesadores de texto, que permite definir un parámetro de diseño que se repite en todas las páginas de un sitio.

Sysop (System operator, operador del sistema): Persona encargada de la administración y el mantenimiento de un host. Ver Postmaster y Webmaster.

Tag (etiqueta): Código marcador de estructura de lenguaje HTML utilizado para estructurar las páginas de la Web.

Telnet (Unix) Programa que permite el acceso remoto a un host. Utilizado para conectarse y controlar computadoras ubicadas en cualquier parte del planeta.

Thread, threaded messages (hilación, mensajes hilados): Mensajes de correo electrónico, (de un newsgroup o una lista de interés), relacionados al mismo tema, o que son respuestas a un mismo asunto.

Throughput: Rendimiento final de una conexión. Volumen de datos que una conexión brinda como resultante de la suma de su capacidad y la resta de los overheads que reducen su rendimiento. Ver Red.

UUCP: (UNIX-to UNIX Copy Program, o UNIX-to UNIX Communications Protocol). Es el conjunto de conceptos que permiten copiar archivos de un sistema Unix a otro en forma automática.

Virus: Pequeños programas de computadora que tienen la capacidad de auto duplicarse y parasitar en otros programas. Una vez que se difunden, los virus se activan bajo determinadas circunstancias y, en general, provocan algún daño o molestia. Ver Worm.

Verónica (Very Easy Rodent-Oriented Netwide Index to Computarized Archives) Una herramienta de búsqueda, que explora bases de datos de Gophers. Ver Gopher

W3C (World Wide Web Consortium) Organización que desarrolla estándares para guiar la expansión de la Web. Organizado por el CERN y el MIT y apadrinado por varias empresas. Su Website es <http://www.w3.org/>. Ver Sistemas Abiertos.

WAIS (Wide Area Information Services, Servicio de Información de Grandes Areas) Herramienta que permite la búsqueda de información en grandes bases de datos remotas. Está cayendo en desuso desde el nacimiento de la World Wide Web.

WAN (Wide Area Network, Red de área amplia) Resultante de la interconexión de varias redes locales localizadas en diferentes sitios (distintas ciudades o países), comunicadas a través de conexiones públicas (líneas dedicadas). La conexión puede ser física directa (un cable) o a través de un satélite, por ejemplo. La conexión es más lenta que una LAN. Ver MAN, RED.