INSTITUTO POLITÉCNICO NACIONAL

ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA

UNIDAD CULHUACAN

TESINA

Seminario de Titulación:
"Las tecnologías aplicadas en redes de computadoras"
DES/ ESIME-CUL/ 5092005/08/10

DISEÑO DE UNA RED INTRANET.

Que como prueba escrita de su
Examen Profesional para obtener
el Título de: Ingeniero en
Comunicaciones y Electrónica

Presentan:

ROMAN AMEZCUA SALGADO
ROGELIO RIVERO SÁNCHEZ

México D.F **Junio 2010.**

INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA
UNIDAD CULHUACAN
TESINA

POR LA OPCIÓN DE	SEMINARIO DE TITULACIÓN DES/ESIME-CUL/5092005/08/10
QUE PARA OBTENER EL TITULO DE	INGENIERO EN COMUNICACIONES Y ELECTRÓNICA
PRESENTAN:	AMEZCUA SALGADO ROMÁN RIVERO SÁNCHEZ ROGELIO

DISEÑO DE UNA RED INTRANET

IMPLEMENTAR UNA RED DE INTRANET ES POR QUE HOY EN DÍA ES IMPORTANTE EL SABER ENTENDER EL FUNCIONAMIENTO DE ESTA, YA QUE SE ENTIENDE POR UNA RED INFORMÁTICA COMO UN SISTEMA DE COMUNICACIÓN QUE CONECTA ORDENADORES Y OTROS EQUIPOS INFORMÁTICOS ENTRE SÍ, CON LA FINALIDAD DE COMPARTIR INFORMACIÓN Y RECURSOS.
A TRAVÉS DE LA COMPARTICIÓN DE INFORMACIÓN Y RECURSOS EN UNA RED, LOS USUARIOS DE LOS SISTEMAS INFORMÁTICOS DE UNA ORGANIZACIÓN PODRÁN HACER UN MEJOR USO DE LOS MISMOS, MEJORANDO DE ESTE MODO EL RENDIMIENTO GLOBAL.

CAPITULADO

México D.F. 12 de Junio de 2010

M. en C. Diana Salomé Vázquez Estrada
Coordinador Académico del Seminario

Ing. Patricia Cortés Pineda.
Asesor.

Ing. Ignacio Monroy Ostria
Jefe del Departamento de Ingeniería
en Comunicaciones y Electrónica

Agradecimientos

En primera instancia doy gracias a dios y a mis padres por darme la vida y a su vez inculcarme los valores que una persona debe tener. Los quiero mucho.

A mi querida esposa y mis dos angelitos por ser los pilares de nuestra familia y darme la fuerza para seguir adelante en las metas que nos proponemos, las quiero mucho.
Carmen, Ivonne y mi Daniela.

A mis abuelos por ser mis segundos padres y por demostrarme su amor.

A mis hermanos por haber compartido cada una de nuestras etapas de la vida los quiero mucho.
A mis sobrinos por darme al gusto y el placer de verlos crecer y darles algunos consejos.
A mi compañero de tesis (mi compadre querido) por ofrecerme su amistad y su afecto en forma incondicional, gracias.

A nuestra coordinadora académica por darnos todas las facilidades en este seminario.

Román Amezcua Salgado

A mi Esposa, por su comprensión, apoyo incondicional, amor, tiempo y todo lo bueno que me ha dado a lo largo de nuestra vida, que Dios la bendiga.

A mis Hijas, por su amor, alegría y bellos momento que me han dado siempre.

A mis Padres, por todo el amor y cuidados que me dieron a lo largo de mi infancia y adolescencia.

A mis Hermanos, por su cariño, apoyo y grandes momentos que hemos vivido.

A mis Amigos de toda la vida, en especial a mi gran amigo José Luis, por su amistad, apoyo y enseñanza, que Dios lo bendiga a él y a su familia.

A mi gran amigo y compadre Román, por su amistad y apoyo, que la felicidad y alegría siempre estén con él y con su familia.

A la autoridades de ESIME Culhuacan, en especial a Diana la coordinadora y a José por su gran apoyo.

Rogelio Rivero Sánchez

Índice

Introducción

La idea de realizar una tesina acerca de cómo implementar una RED de INTRANET es por que hoy en día es importante el saber entender el funcionamiento de esta, ya que se entiende por una red informática como un sistema de comunicación que conecta ordenadores y otros equipos informáticos entre sí, con la finalidad de compartir información y recursos.

A través de la compartición de información y recursos en una red, los usuarios de los sistemas informáticos de una organización podrán hacer un mejor uso de los mismos, mejorando de este modo el rendimiento global de la organización. Entre las ventajas que supone el tener instalada una red, pueden citarse las siguientes:

- Mayor facilidad en la comunicación entre usuarios
- Reducción en el presupuesto para software
- Reducción en el presupuesto para hardware
- Posibilidad de organizar grupos de trabajo
- Mejoras en la administración de los equipos y programas
- Mejoras en la integridad de los datos
- Mayor seguridad para acceder a la información

Objetivos.

Para obtener todas las ventajas que supone el uso de una red, se deben tener instalados una serie de servicios de red, como son:

Acceso.

Los servicios de acceso se encargan tanto de verificar la identidad del usuario (para asegurar que sólo pueden acceder a los recursos para los que tienen permiso) como de permitir la conexión de usuarios a la red desde lugares remotos.

Ficheros.

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

Impresión.

Permite compartir impresoras entre varios ordenadores de la red, lo cual evitará la necesidad de tener una impresora para cada equipo, con la consiguiente reducción en los costos. Las impresoras de red pueden ser conectadas a un servidor de impresión, que se encargará de gestionar la impresión de trabajos para los usuarios de la red, almacenando trabajos en espera (cola de impresión), asignando prioridades a los mismos, etc.

Información.

Los servidores de información pueden almacenar bases de datos para su consulta por los usuarios de la red u otro tipo de información, como por ejemplo documentos de hipertexto.

Otros.

En el campo de la comunicación entre usuarios existen una serie de servicios que merece la pena comentar. El más antiguo y popular es el correo electrónico (e-mail) que permite la comunicación entre los usuarios a través de mensajes escritos. Los mensajes se enviarán y se recuperarán usando un equipo servidor de correo. Resulta mucho más barato, económico y fiable que el correo convencional. Además, tenemos los servicios de conferencia (tanto escrita, como por voz y vídeo) que permitirán a dos o más usuarios de la red comunicarse directamente (on line).

Beneficios de una red local.

Bien planificada e implementada, una red local aumenta la productividad de los PCs y periféricos implicados en ella. Algunas de las facilidades que nos abre el uso de una red local son:

- Compartir los recursos existentes: impresoras, módems, escáner, etc.
- Uso de un mismo software desde distintos puestos de la red.
- Acceder a servicios de información internos (Intranet) y externos (Internet).
- Intercambiar archivos.
- Uso del correo electrónico.
- Permite conexiones remotas a los distintos recursos.
- Copias de seguridad centralizadas.
- Simplifica el mantenimiento del parque de máquinas.

Aplicaciones.

La red local nos abre una serie de posibilidades muy interesantes para su uso como herramienta. Algunas de ellas son:

- Compartir los recursos existentes en el centro, desde las impresoras, escáner y las comunicaciones con el exterior, hasta le propio software instalado en los distintos equipos de la red.
- Correo electrónico.
- Multimedia en red.
- Servidores de información internos, intranet.
- Conferencias o contactos en directo usando las tres posibilidades técnicas existentes:
    - Tecleadas, denominadas Chat.
    - Por voz o audio conferencias.
    - Por voz y videoconferencia.

Es por eso que se decidió realizar la tesina acerca de la "Implementación de una red intranet", ya que el campo laboral es muy extenso hoy en día.

Capítulo 1.- Conceptos generales de redes.

1.1.-Red LAN.

1.1.1.- ¿Qué es una Red de Área Local (Local Area Network) (LAN)?

Una LAN es un sistema de interconexión de equipos informáticos basado en líneas de alta velocidad y que suele abarcar cuando mucho un edificio.
Las principales tecnologías usadas en una LAN son: Ethernet, Token ring, ARCNET y Dispositivo Interface de Fibra (óptica) Digital (Fiber Digital Device Interface) FDDI.
Un caso típico de LAN es en la que existe un equipo servidor de LAN desde el que los usuarios cargan las aplicaciones que se ejecutarán en sus estaciones de trabajo. Los usuarios pueden también solicitar tareas de impresión y otros servicios que están disponibles mediante aplicaciones que se ejecutan en el servidor. Además pueden compartir ficheros con otros usuarios en el servidor. Los accesos a estos ficheros están controlados por un administrador de la LAN.

1.1.2.-Definición de LAN.

LAN es la abreviatura de Network Area Local. Una red local es la interconexión de varios ordenadores y periféricos para el intercambio de recursos e información. Permite que dos o más máquinas se comuniquen.

El término red local incluye tanto el hardware (impresoras) como el software (programas de aplicación) necesario para la interconexión de los distintos dispositivos y el tratamiento de la información.

Todos los dispositivos pueden comunicarse con el resto aunque también pueden funcionar de forma independiente. Las velocidades de comunicación son elevadas estando en el orden de varios millones de bits por segundo (Mbps) dependiendo del tipo de red que se use. Es un sistema fiable ya que se dispone de sistemas de detección y corrección de errores de transmisión.

Dentro de una red local existen algunos ordenadores que sirven información, aplicaciones o recursos a los demás. Estos ordenadores se les conocen con el nombre de servidores.

Los servidores pueden ser dedicados o no dedicados:

Dedicados.

Normalmente tienen un sistema operativo más potente que los demás y son usados por el administrador de la red.

No dedicados.

Pueden ser cualquier puesto de la red que además de ser usado por un usuario, facilita el uso de ciertos recursos al resto de los equipos de la red, por ejemplo comparte su impresora.

El creciente uso de las redes locales se debe al abaratamiento de sus componentes y a la generalización de sistemas operativos orientados al uso en red. Con esto se facilitan las operaciones de compartir y usar recursos de los demás ordenadores y periféricos.

Las LAN constan de los siguientes componentes:

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

1.1.3.-Beneficios de las redes locales.

Bien planificada e implementada, una red local aumenta la productividad de los PCs y periféricos implicados en ella. Algunas de las facilidades que nos abre el uso de una red local son:

- Compartir los recursos existentes: impresoras, módems, escáner, etc.
- Uso de un mismo software desde distintos puestos de la red.
- Acceder a servicios de información internos (Intranet) y externos (Internet).
- Intercambiar archivos.
- Uso del correo electrónico.
- Permite conexiones remotas a los distintos recursos.
- Copias de seguridad centralizadas.
- Simplifica el mantenimiento del parque de máquinas.

1.1.4.-Aplicaciones.

La red local nos abre una serie de posibilidades muy interesantes para su uso como herramienta. Algunas de ellas son:

- Compartir los recursos existentes en el centro, desde las impresoras, escáner y las comunicaciones con el exterior, hasta el propio software instalado en los distintos equipos de la red.
- Correo electrónico.
- Multimedia en red.
- Servidores de información internos, intranet.
- Conferencias o contactos en directo usando las tres posibilidades técnicas existentes:
    - Tecleadas, denominadas Chat.
    - Por voz o audio conferencias.
    - Por voz y vídeo, videoconferencias.

1.2.-Tipo de redes informáticas según sus topologías.

La topología se refiere a la forma en que están interconectados los distintos equipos (nodos) de una red. Un nodo es un dispositivo activo conectado a la red, como un ordenador o una impresora. Un nodo también puede ser dispositivo o equipo de la red como un concentrador, conmutador o un router.

1.2.1.-Topología en 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.

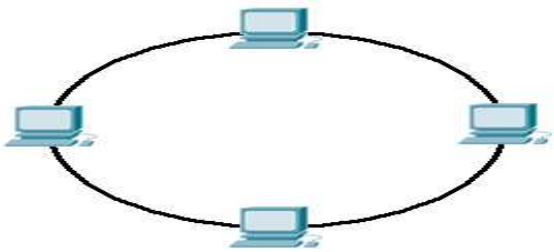

Figura 1.1.- Topología en anillo.

1.2.2.-Topología en 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.

Figura 1.2.-Topología en bus.

1.2.3.-Topología en 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.

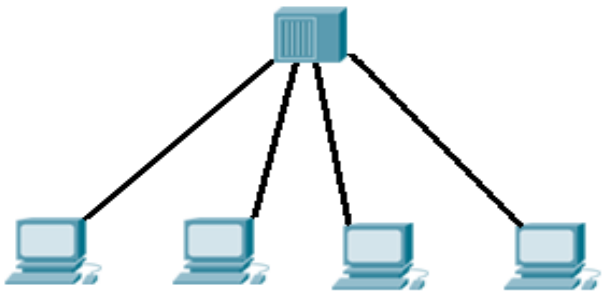

Figura 1.3.- Topología en estrella.

1.2.4.-Topología en árbol.

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

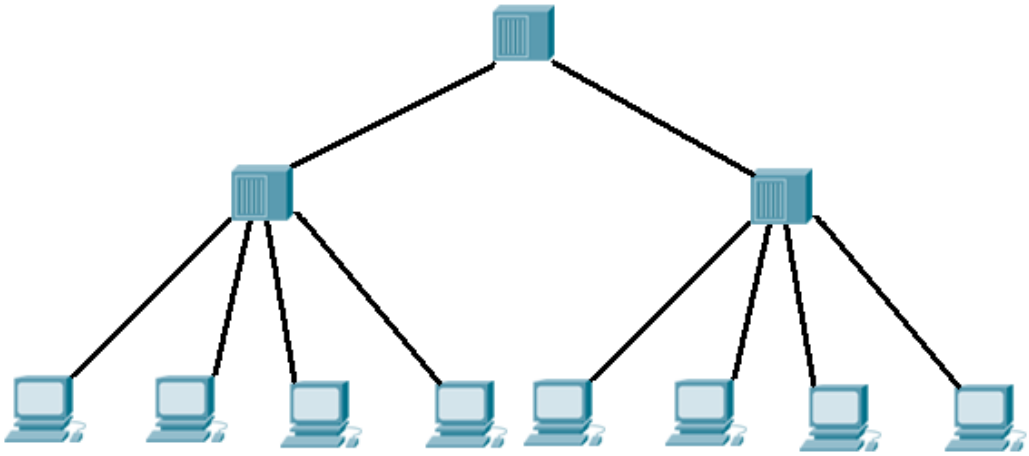

Figura 1.4.- Topología en árbol.

1.3.-Tipo de redes informáticas según su protocolo.

Se podría definir protocolo como el conjunto de normas que regulan la comunicación entre los distintos dispositivos de una red. Es como el lenguaje común que deben de usar todos los componentes para entenderse entre ellos.

Los protocolos se clasifican en dos grupos: protocolos de bajo nivel que son los que se encargan de gestionar el tráfico de información por el cable, o sea a nivel físico, y son los que nos interesan en este apartado y los protocolos de red que se verán más adelante cuando necesitemos configurar la red y que fundamentalmente definen las normas a nivel de software por las que se van a comunicar los distintos dispositivos de la red.

Existen bastantes protocolos de bajo nivel como pueden ser Ethernet, Token Ring, FDDI, ATM, LocalTalk, etc. Aunque los más usados para implementaciones similares a la que nos ocupa en este proyecto son los dos primeros:

1.3.1.- Token Ring.

Es un sistema bastante usado aunque mucho menos que Ethernet. Llega a conseguir velocidades de hasta 16 Mbits/s aunque también existen especificaciones para velocidades superiores. La topología lógica que usa es en anillo aunque en la práctica se conecta en una topología física en estrella, a través de concentradores llamados unidad de conexión al medio (Medium Attachment Unit) (MAU).

Es más fácil de detectar errores que en Ethernet. Cada nodo reconoce al anterior y al posterior. Se comunican cada cierto tiempo. Si existe un corte, el nodo posterior no recibe información del nodo cortado e informa a los demás de cual es el nodo inactivo.

1.3.2.- Ethernet.

Es el método de conexión más extendido porque permite un buen equilibrio entre velocidad, costo y facilidad de instalación. Todo esto combinado con su buena aceptación en el mercado y la facilidad de soportar prácticamente todos los protocolos de red, convierten a Ethernet en la tecnología ideal para la mayoría de las instalaciones de LAN.

Consigue velocidades de conexión de 10 Mbits/s aunque existen especificaciones de velocidades superiores como es el caso de Fast Ethernet que llega a conseguir hasta 100 Mbits/s.

Es la tecnología de red de área local más extendida en la actualidad.

Fue diseñado originalmente por Digital, Intel y Xerox por lo cual, la especificación original se conoce como Ethernet DIX. Posteriormente en 1983, fue formalizada por el Instituto de Ingenieros Eléctricos y Electrónicos. (Institute of Electrical and Electronics Engineers.) IEEE como el estándar Ethernet 802.3.

La velocidad de transmisión de datos en Ethernet es de 10Mbits/s en las configuraciones habituales pudiendo llegar a ser de 100Mbits/s en las especificaciones Fast Ethernet.

Al principio, sólo se usaba cable coaxial con una topología en BUS, sin embargo esto ha cambiado y ahora se utilizan nuevas tecnologías como el cable de par trenzado (10 Base-T), fibra óptica (10 Base-FL) y las conexiones a 100 Mbits/s (100 Base-X o Fast Ethernet). La especificación actual se llama IEEE 802.3u.

Ethernet/IEEE 802.3, está diseñado de manera que no se puede transmitir más de una información a la vez. El objetivo es que no se pierda ninguna información, y se controla con un sistema conocido como CSMA/CD (Carrier Sense Multiple Access with Collision Detection, Detección de Portadora con Acceso Múltiple y Detección de Colisiones), cuyo principio de funcionamiento consiste en que una estación, para transmitir, debe detectar la presencia de una señal portadora y, si existe, comienza a transmitir. Si dos estaciones empiezan a transmitir al mismo tiempo, se produce una colisión y ambas deben repetir la transmisión, para lo cual esperan un tiempo aleatorio antes de repetir, evitando de este

modo una nueva colisión, ya que ambas escogerán un tiempo de espera distinto. Este proceso se repite hasta que se reciba confirmación de que la información ha llegado a su destino.

Según el tipo de cable, topología y dispositivos utilizados para su implementación podemos distinguir los siguientes tipos de Ethernet:

- 10 Base-5.
- 10 Base-2.
- 10 Base-T.
- Fast Ethernert.

1.3.2.1.-10 Base-5.

También conocida como THICK ETHERNET (Ethernet grueso), es la Ethernet original. Fue desarrollada originalmente a finales de los 70 pero no se estandarizó oficialmente hasta 1983.

Utiliza una topología en BUS, con un cable coaxial que conecta todos los nodos entre sí. En cada extremo del cable tiene que llevar un terminador. Cada nodo se conecta al cable con un dispositivo llamado transceptor.

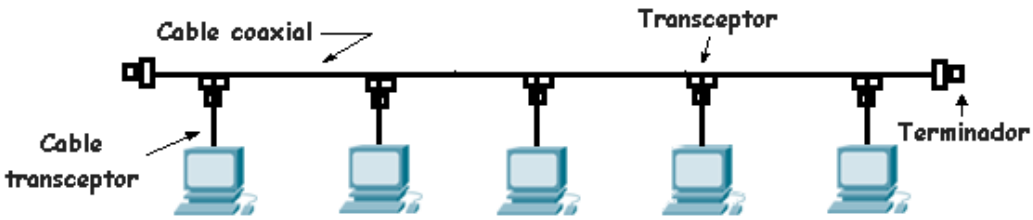

Figura 1.5.- Ethernet Thick Ethernet.

El cable usado es relativamente grueso (10mm) y rígido. Sin embargo es muy resistente a interferencias externas y tiene pocas pérdidas. Se le conoce con el nombre de RG8 o RG11 y tiene una impedancia de 50 ohmios. Se puede usar conjuntamente con el 10 Base-2.

Tabla 1.1.-Caracteristicas de una red Ethernet.

Características Ethernet	
Tipo de cable usado	RG8 o RG11
Tipo de conector usado	AUI
Velocidad	10 Mbits/s
Topología usada	BUS
Mínima distancia entre transceptores	2.5 m
Máxima longitud del cable del transceptor	50 m
Máxima longitud de cada segmento	500 m
Máxima longitud de la red	2.500 m
Máximo de dispositivos conectados por segmento	100
Regla 5-4-3	Sí

La regla 5-4-3 es una norma que limita el tamaño de las redes

Ventajas.

- Es posible usarlo para distancias largas.
- Tiene una inmunidad alta a las interferencias.
- Conceptualmente es muy simple.

Desventajas.

- Inflexible. Es difícil realizar cambios en la instalación una vez montada.
- Intolerancia a fallos. Si el cable se corta o falla un conector, toda la red dejará de funcionar.
- Dificultad para localización de fallos. Si existe un fallo en el cableado, la única forma de localizarlo es ir probando cada uno de los tramos entre nodos para averiguar cual falla.

Aplicaciones en la actualidad.

Debido a los inconvenientes antes mencionados, en la actualidad 10 Base-5 no es usado para montaje de redes locales. El uso más común que se le da en la actualidad es el de "Backbone". Básicamente un backbone se usa para unir varios HUB de 10 Base-T cuando la distancia entre ellos es grande, por ejemplo entre plantas distintas de un mismo edificio o entre edificios distintos.

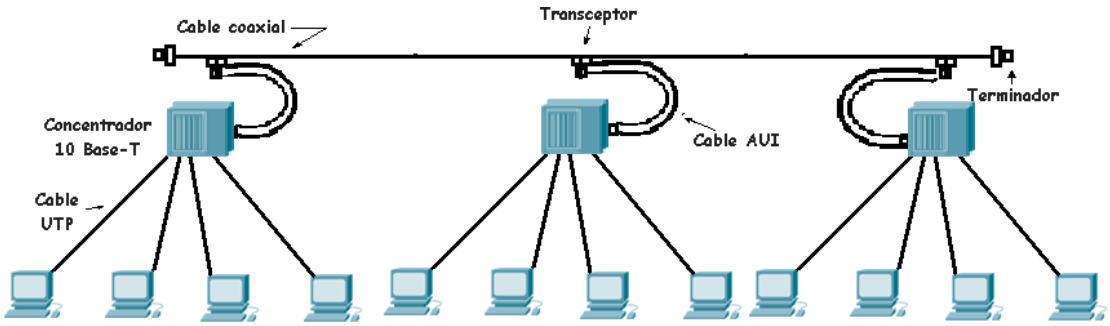

Figura 1.6.- Backbone.

1.3.2.2.- 10 Base-2.

En la mayoría de los casos, el costo de instalación del coaxial y los transceptores de las redes 10 Base-5 las hacía prohibitivas, lo que indujo la utilización de un cable más fino y, por tanto más barato, que además no necesitaba transceptores insertados en él. Se puede decir que 10 Base-2 es la versión barata de 10 Base-5. Por esto, también se le conoce Thin Ethernet (Ethernet fino) o cheaper-net (red barata).

Figura 1.7. - 10 Base-2.

Este tipo de red ha sido la más usada en los últimos años en instalaciones no muy grandes debido a su simplicidad y precio asequible. Se caracteriza por su cable coaxial fino (RG-58) y su topología en BUS. Cada dispositivo de la red se conecta con un adaptador BNC en forma de "T" y al final de cada uno de los extremos del cable hay que colocar un terminador de 50 Ohmios.

Tabla 1.2.- Características De Una Red En Bus.

Características De Una Red En Bus	
Tipo de cable usado	RG-58
Tipo de conector usado	BNC
Velocidad	10 Mbits/s
Topología usada	BUS
Mínima distancia entre transceptores	0.5 m
Máxima longitud de cada segmento	185 m
Máxima longitud de la red	925 m
Regla 5-4-3	Sí

Ventajas.

- Simplicidad. No usa ni concentradores, ni transceptoras ni otros dispositivos adicionales.
- Debido a su simplicidad es una red bastante económica.
- Tiene una buena inmunidad al ruido debido a que el cable coaxial dispone de un blindaje apropiado para este fin.

Desventajas.

- Inflexible. Es bastante difícil realizar cambios en la disposición de los dispositivos una vez montada.
- Intolerancia a fallos. Si el cable se corta o falla un conector, toda la red dejará de funcionar. En un lugar como un aula de formación donde el volumen de uso de los

ordenadores es elevado, es habitual que cualquier conector falle y por lo tanto la red completa deje de funcionar.

- Dificultad para localización de fallos. Si existe un fallo en el cableado, la única forma de localizarlo es ir probando cada uno de los tramos entre nodos para averiguar cual falla.
- El cable RG-58, se usa sólo para este tipo de red local, por lo que no podrá ser usado para cualquier otro propósito como ocurre con otro tipo de cables.

Aplicaciones en la actualidad.

La tecnología 10 Base-2 se usa para pequeñas redes que no tengan previsto cambiar su disposición física.

De igual manera que 10 Base-5, uno de los usos habituales de esta tecnología es como backbone para interconectar varios concentradores en 10 Base-T. Normalmente los concentradores no se mueven de lugar. Si la distancia entre ellos es grande, por ejemplo si están en plantas o incluso en edificios distintos, la longitud máxima que se puede conseguir con este cable (185m) es mucho mayor que la que se consigue usando el cable de par trenzado sin blindaje (Unshieldded Twisted Pair) UTP de la tecnología 10 Base-T (100m).

1.3.2.3.- 10 Base-T.

Ya se ha comentado, que ETHERNET fue diseñado originalmente para ser montado con cable coaxial grueso y que más adelante se introdujo el coaxial fino. Ambos sistemas funcionan excelentemente pero usan una topología en BUS, que complica la realización de cualquier cambio en la red. También deja mucho que desear en cuestión de fiabilidad. Por todo esto, se introdujo un nuevo tipo de tecnología llamada 10 Base-T, que aumenta la movilidad de los dispositivos y la fiabilidad.

El cable usado se llama UTP que consiste en cuatro pares trenzados sin apantallamiento. El propio trenzado que llevan los hilos es el que realiza las funciones de aislar la información de interferencias externas. También existen cables similares al UTP pero con apantallamiento que se llaman Par trenzado blindado (Shielded Twisted Pair) STP.

10 Base-T usa una topología en estrella consistente en que desde cada nodo va un cable a un concentrador común que es el encargado de interconectarlos. Cada uno de estos cables no puede tener una longitud superior a 90m.

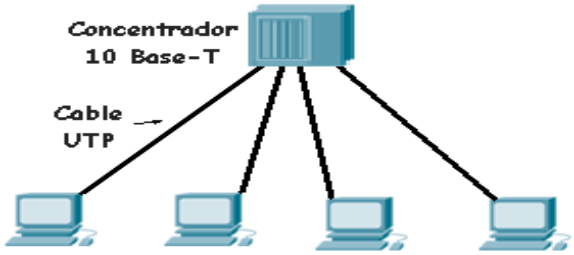

Figura 1.8.- 10base-T.

A los concentradores también se les conoce con el nombre de HUB's y son equipos que nos permiten estructurar el cableado de la red. Su función es distribuir y amplificar las señales de la red y detectar e informar de las colisiones que se produzcan. En el caso de que el número de colisiones que se producen en un segmento sea demasiado elevado, el concentrador lo aislará para que el conflicto no se propague al resto de la red.

También se puede usar una topología en árbol donde un concentrador principal se interconecta con otros concentradores. La profundidad de este tipo de conexiones viene limitada por la regla 5-4-3.

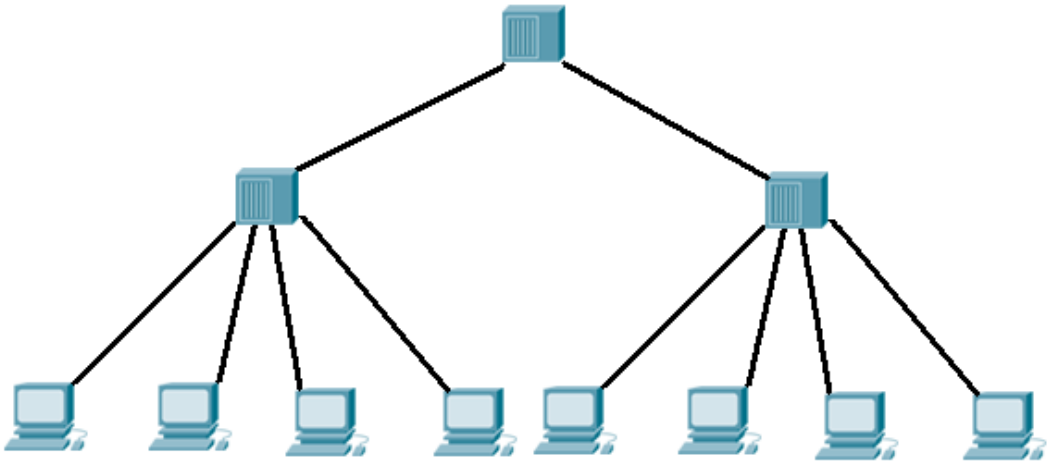

Figura 1.9.- Topología en àrbol

10 Base-T también se puede combinar con otro tipo de tecnologías, como es el caso de usar 10 Base-2 o 10 Base-5 como Backbone entre los distintos concentradores.

Cuando la distancia entre concentradores es grande, esta limitada por la longitud máxima que se puede conseguir con el cable UTP (100m). Si la distancia es mayor se puede usar la tecnología 10 Base-2 que permite hasta 185m o la 10 Base-5 con la que podríamos alcanzar los 500m. Otra solución puede ser usar cable UTP poniendo repetidores cada 100m.

De los 8 hilos de que dispone en el cable UTP, sólo se usan cuatro para los datos de la LAN (dos para transmisión y dos para la recepción) por lo que quedan otros cuatro utilizables para otros propósitos (telefonía, sistemas de seguridad, transmisión de vídeo, etc.).

El conector usado es similar al utilizado habitualmente en los teléfonos pero con 8 pines. Se le conoce con el nombre de RJ-45. Los pines usados para los datos son el 1 - 2 para un par de hilos y el 3 - 6 para el otro. La especificación que regula la conexión de hilos en los dispositivos Ethernet es la EIA/TIA T568A y T568B.

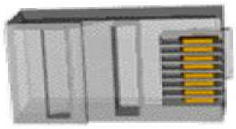

Figura 1.10.-Conector RJ-45.

Tabla 1.3 Características de una red estrella.

Características De Una Red Estrella	
Tipo de cable usado	UTP, STP y FTP
Tipo de conector usado	RJ-45
Velocidad	10 Mbits/s
Topología usada	Estrella
Máxima longitud entre la estación y el concentrador	90 m
Máxima longitud entre concentradores	100 m

Máximo de dispositivos conectados por segmento	512
Regla 5-4-3	Sí

Ventajas.

- Aislamiento de fallos. Debido a que cada nodo tiene su propio cable hasta el concentrador, en caso de que falle uno, dejaría de funcionar solamente él y no el resto de la red como pasaba en otros tipos de tecnologías.
- Fácil localización de averías. Cada nodo tiene un indicador en su concentrador indicando que está funcionando correctamente. Localizar un nodo defectuoso es fácil.
- Alta movilidad en la red. Desconectar un nodo de la red, no tiene ningún efecto sobre los demás. Por lo tanto, cambiar un dispositivo de lugar es tan fácil como desconectarlo del lugar de origen y volverlo a conectar en el lugar de destino.
- Aprovechamiento del cable UTP para hacer convivir otros servicios. De los cuatro pares (8 hilos) de que dispone, sólo se usan dos pares (4 hilos) para los datos de la LAN por lo que quedan otros dos utilizables para otros propósitos (telefonía, sistemas de seguridad, transmisión de vídeo, etc.).

Desventajas.

- Distancias. 10 Base-T permite que la distancia máxima entre el nodo y el concentrador sea de 90m. En algunas instalaciones esto puede ser un problema, aunque siempre se puede recurrir a soluciones cómo las comentadas anteriormente consistentes en combinar esta tecnología con 10 Base-2 o 10 Base-5, o el uso de repetidores para alargar la distancia.
- Sensibilidad a interferencias externas. El cable coaxial usado en otras tecnologías es más inmune a interferencias debido a su apantallamiento. En la mayoría de los casos, el trenzado interno que lleva el cable UTP es suficiente para evitarlas.

1.3.2.4.-Fast Ethernet.

En la actualidad han surgido nuevas especificaciones basadas en Ethernet que permiten transmitir datos a mayor velocidad como son:

Ethernet de 100 Mbits/s (100 BaseX o Fast Ethernet).

Esta especificación permite velocidades de transferencia de 100 Mbits/s sobre cables de pares trenzados, directamente desde cada estación. El sistema 100 BaseX tiene la misma arquitectura que 10 Base-T con la diferencia de usar componentes que son capaces de transferir la información a 100 Mbits/s.

Partiendo de una LAN montada con los requerimientos de una 10 Base-T, únicamente se requiere la sustitución de los concentradores y las tarjetas de red de las estaciones.

Casi todos los componentes usados en nuestro proyecto, soportan esta especificación. Desde el cable hasta las rosetas y conectores, pasando por las tarjetas de red. La única excepción es el concentrador. Esto en principio limita la velocidad de la LAN a 10 Mbits/s. Para convertirlo en 100 BaseX y por lo tanto aumentar la velocidad de la LAN simplemente habrá que sustituir el concentrador por uno de 100 Mbits/s. Será el uso diario, el que nos demandará o no el aumento de velocidad. Seguro que también influye la previsible bajada de precios que deben de experimentar estos dispositivos.

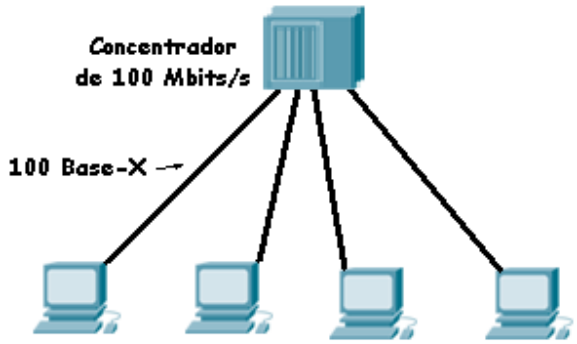

Figura 1.11. -100 Base-X.

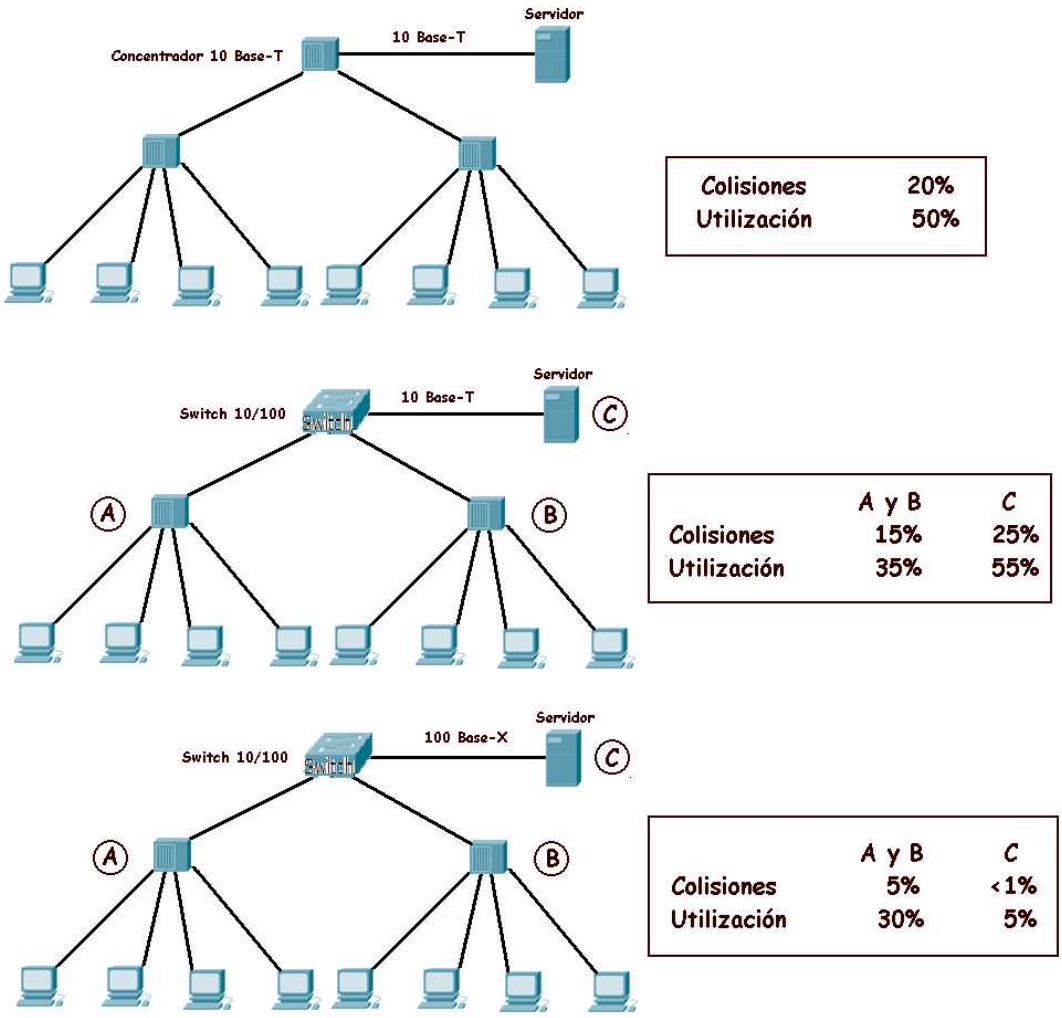

Figura 1.12..- Uso de conmutadores en lugar de concentradores.

En la figura 1.12 se puede ver como el uso de conmutadores en lugar de concentradores mejora las prestaciones de la red.

El primer caso sería una implementación típica de 10 Base-T con concentradores. Aunque no es malo el rendimiento que le saca a este montaje, veremos que es mejorable con muy pocos cambios.

El segundo caso tan solo ha cambiado el concentrador principal por un conmutador y ha conseguido disminuir considerablemente tanto el número de colisiones como la utilización de las capacidades de la red. Esto se debe a que cada puerto del conmutador es una red

separada a nivel de colisiones y además tiene para sí todo el ancho de banda disponible (10 Mbits/s en este caso).

El tercer caso es una combinación entre uso de conmutador y 100 Base-X. Como se puede observar, el switch usado tiene además de los puertos de 10 Mbits/s, dos más de 100 Mbits/s. Si el servidor de la LAN lo conectamos en uno de estos segmentos, conseguiremos una disminución muy considerable tanto del número de colisiones como del grado de utilización de la red. En definitiva mejora sustancialmente el rendimiento de la LAN.

1.3.3.-Interfaz de Datos Distribuida por Fibra (Fiber Distributed Data Interface) FDDI.

Es una LAN de anillo de token que corre con una velocidad de 100 Mbps sobre distancias de hasta 200 km con hasta 1000 estaciones conectadas. Se le puede usar como una LAN normal pero el uso más común es para conectar LANs de cobre.

· Consiste en dos anillos que transmiten en sentidos contrarios. Si tiene una ruptura (por ejemplo, debido a un fuego) se pueden conectar los dos anillos en uno.

· En vez de la codificación de Manchester usa un esquema que se llama 4 de 5: se usan cinco bits para codificar cada cuatro. Dieciséis combinaciones son datos y otras son para control. Para sincronizar se usa un preámbulo largo y se requiere que los relojes sean estables dentro de 0,005%.

· Debido a la longitud potencial del anillo una estación puede generar un nuevo marco inmediatamente después de transmitir un marco, en vez de esperar su vuelta (como en 802.5).

Pueden estar algunos marcos en el anillo a la vez.

· FDDI también tiene un modo síncrono donde cada marco contiene cuatro canales de T1; puede haber hasta 16 marcos síncronos cada 125 microsegundos.

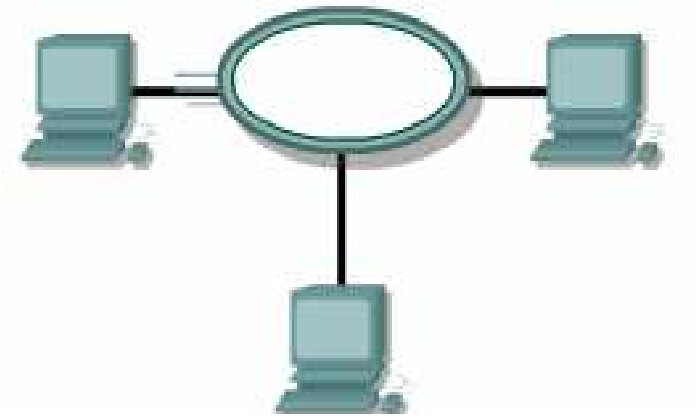

Figura 1.13.- Topología FDDI.

1.3.4.-La Interface Paralela de alto rendimiento (High-Performance Parallel Interface) (HPPI).

Fue desarrollado por Los Alamos para conectar los supercomputadores.

Principios de diseño:

- Chips estándares, ninguna opción y rendimiento.
- Tiene velocidades de 800 Mbps y 1600 Mbps. El primer es suficiente para 30 marcos por segundo de 1024×1024 pixeles de 24 bits cada uno. Usa un conmutador de crossbar.
- El cable contiene 50 pares trenzados (32 de datos, otros de control) es simplex y tiene una longitud máxima de 25 metros. Se transfiere una palabra cada 40 nsegs. Se usan dos cables para la velocidad más alta.
- Los marcos tienen 256 palabras. Se limita la detección de errores a un bit de paridad por palabra y una palabra de paridad por marco; otros checksums eran demasiado lentos.
- Fibre channel. La idea fue reemplazar los pares trenzados de HPPI con una sola fibra. Por desgracia es mucho más complicado, y por lo tanto más caro y difícil de implementar. Apoya velocidades de 100, 200, 400, y 800 Mbps.

1.4.-Encapsulamiento.

Todas las comunicaciones de una red parten de un origen y se envían a un destino. La información que se envía a través de una red se denomina datos o paquetes de datos. Si un computador (host A) desea enviar datos a otro (host B), en primer término los datos deben empaquetarse a través de un proceso denominado encapsulamiento.

El encapsulamiento rodea los datos con la información de protocolo necesaria antes de que se una al tránsito de la red. Por lo tanto, a medida que los datos se desplazan a través de las capas del modelo OSI, reciben encabezados, información final y otros tipos de información. Para ver cómo se produce el encapsulamiento, examine la forma en que los datos viajan a través de las capas como lo ilustra la figura 1.14. Una vez que se envían los datos desde el origen, viajan a través de la capa de aplicación y recorren todas las demás capas en sentido descendente. El empaquetamiento y el flujo de los datos que se intercambian experimentan cambios a medida que las capas realizan sus funciones para los usuarios finales. Como lo muestra la figura 1.15, las redes deben realizar los siguientes cinco pasos de conversión a fin de encapsular los datos:

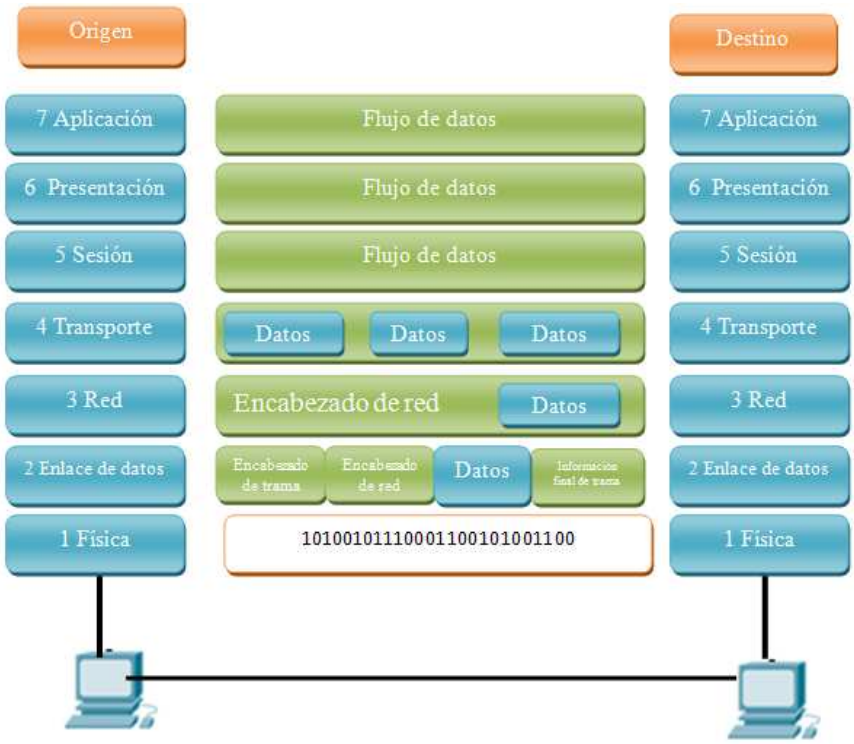

Figura 1.14.- Forma en que los datos viajan a través de las capas.

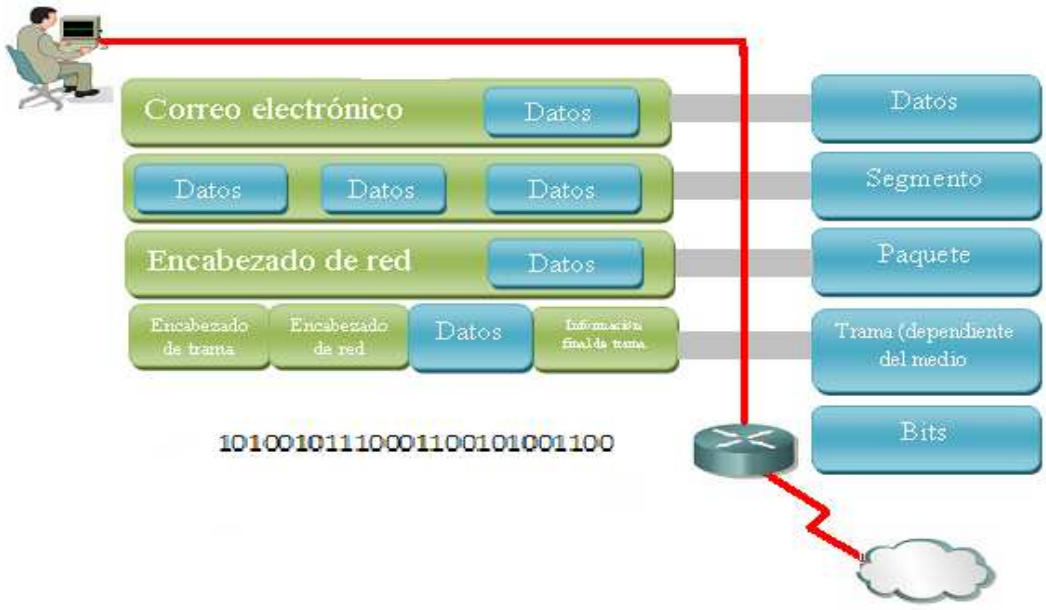

Figura 1.15.- Empaquetamiento y el flujo de los datos.

1. Crear los datos. Cuando un usuario envía un mensaje de correo electrónico, sus caracteres alfanuméricos se convierten en datos que pueden recorrer la internetwork.
2. Empaquetar los datos para ser transportados de extremo a extremo. Los datos se empaquetan para ser transportados por la internetwork. Al utilizar segmentos, la función de transporte asegura que los hosts de mensaje en ambos extremos del sistema de correo electrónico se puedan comunicar de forma confiable.
3. Agregar la dirección de red IP al encabezado. Los datos se colocan en un paquete o datagrama que contiene un encabezado de paquete con las direcciones lógicas de origen y de destino. Estas direcciones ayudan a los dispositivos de red a enviar los paquetes a través de la red por una ruta seleccionada.
4. Agregar el encabezado y la información final de la capa de enlace de datos. Cada dispositivo de la red debe poner el paquete dentro de una trama. La trama le permite conectarse al próximo dispositivo de red conectado directamente en el enlace. Cada dispositivo en la ruta de red seleccionada requiere el entramado para poder conectarse al siguiente dispositivo.

5. Realizar la conversión a bits para su transmisión. La trama debe convertirse en un patrón de unos y ceros (bits) para su transmisión a través del medio. Una función de temporización permite que los dispositivos distingan estos bits a medida que se trasladan por el medio. El medio en la internetwork física puede variar a lo largo de la ruta utilizada. Por ejemplo, el mensaje de correo electrónico se puede originar en una LAN, atravesar el backbone de una universidad y salir por un enlace WAN hasta llegar a su destino en otra LAN remota.

1.5.-Normas de Red.

Estas normas de red son creadas y administradas por una serie de diferentes organizaciones y comités.

Entre ellos se incluyen el Instituto de Ingeniería Eléctrica y Electrónica (IEEE), el Instituto Nacional Americano de Normalización (ANSI), la Asociación de la Industria de las Telecomunicaciones (TIA), la Asociación de Industrias Electrónicas (EIA) y la Unión Internacional de Telecomunicaciones (UIT), antiguamente conocida como el Comité Consultivo Internacional Telegráfico y Telefónico (CCITT).

1.6.-Modelo OSI.

En sus inicios, el desarrollo de redes sucedió con desorden en muchos sentidos. A principios de la década de 1980 se produjo un enorme crecimiento en la cantidad y el tamaño de las redes. A medida que las empresas tomaron conciencia de las ventajas de usar tecnología de networking, las redes se agregaban o expandían a casi la misma velocidad a la que se introducían las nuevas tecnologías de red.

Para mediados de la década de 1980, estas empresas comenzaron a sufrir las consecuencias de la rápida expansión. De la misma forma en que las personas que no hablan un mismo idioma tienen dificultades para comunicarse, las redes que utilizaban diferentes especificaciones e implementaciones tenían dificultades para intercambiar información. El mismo problema surgía con las empresas que desarrollaban tecnologías de networking privadas o propietarias. "Propietario" significa que una sola empresa o un pequeño grupo de empresas controlan todo uso de la tecnología. Las tecnologías de networking que

respetaban reglas propietarias en forma estricta no podían comunicarse con tecnologías que usaban reglas propietarias diferentes.

Para enfrentar el problema de incompatibilidad de redes, la Organización Internacional de Normalización (ISO) investigó modelos de networking como la red de Digital Equipment Corporation (DECnet), la Arquitectura de Sistemas de Red (SNA) y TCP/IP a fin de encontrar un conjunto de reglas aplicables de forma general a todas las redes. En base a esta investigación, la ISO desarrolló un modelo de red que ayuda a los fabricantes a crear redes que sean compatibles con otras redes.

El modelo de referencia de Interconexión de Sistemas Abiertos (OSI) lanzado en 1984 fue el modelo de red descriptivo creado por ISO. Proporcionó a los fabricantes un conjunto de estándares que aseguraron una mayor compatibilidad e interoperabilidad entre los distintos tipos de tecnología de red producidos por las empresas a nivel mundial.

Figura 1.16.-Modelo OSI.

Tabla 1.4.- Ventajas Del Modelo OSI.

Ventajas Del Modelo OSI
Reduce la complejidad

Estandariza las interfaces
Facilita el Diseño modular
Asegura la Interoperabilidad de la Tecnología
Acelera la Evolución
Simplifica la Enseñanza y el Aprendizaje
Marcador de resaltado
Tijeras

El modelo de referencia OSI se ha convertido en el modelo principal para las comunicaciones por red. Aunque existen otros modelos, la mayoría de los fabricantes de redes relacionan sus productos con el modelo de referencia de OSI. Esto es en particular así cuando lo que buscan es enseñar a los usuarios a utilizar sus productos. Se considera la mejor herramienta disponible para enseñar cómo enviar y recibir datos a través de una red.

1.6.1.- Las capas del modelo OSI.

El modelo de referencia OSI es un marco que se puede utilizar para comprender cómo viaja la información a través de una red. El modelo de referencia OSI explica de qué manera los paquetes de datos viajan a través de varias capas a otro dispositivo de una red, aun cuando el remitente y el destinatario posean diferentes tipos de medios de red.

En el modelo de referencia OSI, hay siete capas numeradas, cada una de las cuales ilustra una función de red específica. La división de la red en siete capas permite obtener las siguientes ventajas:

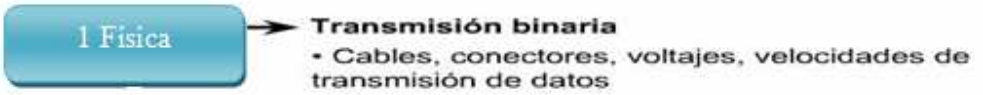

Figura 1.17.- Capa Física del modelo OSI.

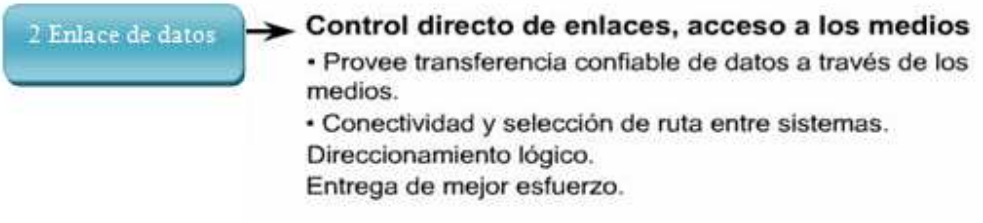

Figura 1.18.- Capa de Enlace de datos del modelo OSI.

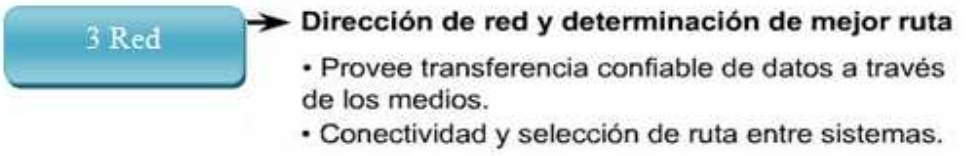

Figura 1.19.- Capa de Red del modelo OSI.

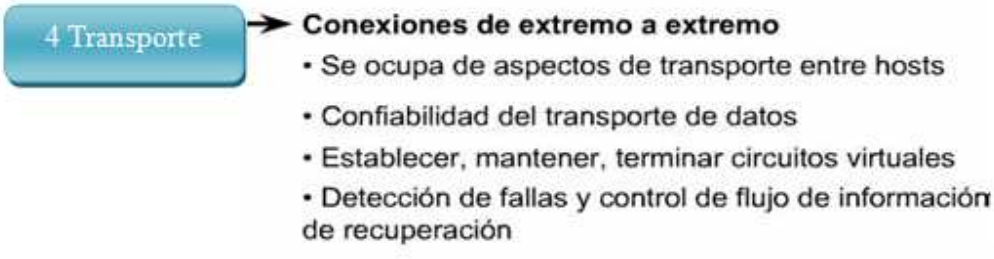

Figura 1.20.- Capa Transporte del modelo OSI.

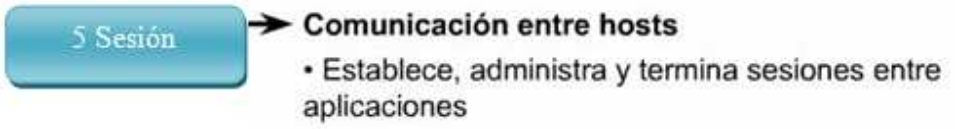

Figura 1.21.- Capa de Sesión del modelo OSI.

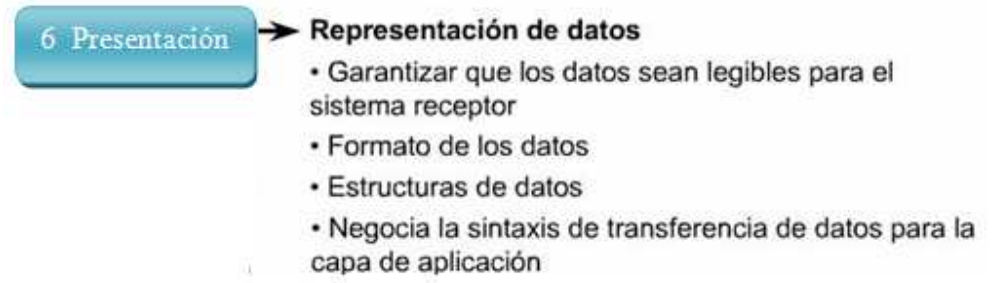

Figura 1.22.- Capa de Presentación del modelo OSI.

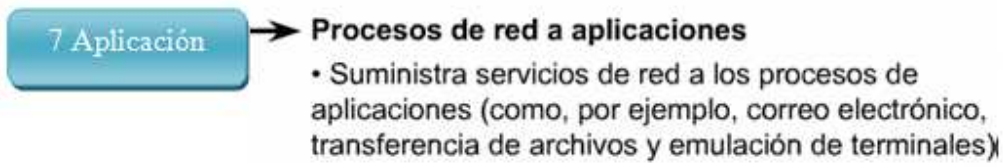

Figura 1.23.- Capa de Aplicación del modelo OSI.

- Divide la comunicación de red en partes más pequeñas y fáciles de manejar.
- Normaliza los componentes de red para permitir el desarrollo y el soporte de los productos por diferentes fabricantes.
- Permite a los distintos tipos de hardware y software de red comunicarse entre sí.
- Evita que los cambios en una capa afecten las otras capas.
- Divide la comunicación de red en partes más pequeñas para simplificar el aprendizaje.

1.7.-Modelo DOD.

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.

1.8.-Norma IEEE 802.3.

- IEEE 802.3 es un protocolo de CSMA/CD con persistencia de 1 para las LANs.
- Cuando una estación quiere transmitir, escucha al cable.
- Si el cable está ocupado, la estación espera hasta que esté desocupado; de otra manera transmite inmediatamente.
- Si hay un choque, las estaciones involucradas esperan por períodos aleatorios.
- Historia:
  - Después de ALOHA y el desarrollo del sentido de portador, Xerox PARC construyó un sistema de
  - CSMA/CD de 2,94 Mbps para conectar más de 100 estaciones de trabajo en un cable de 1 km. Se llamaba Ethernet (red de éter).
  - Xerox, DEC, e Intel crearon un estándar para un Ethernet de 10 Mbps. Esto fue el baso para 802.3, que describe una familia de protocolos de velocidades de 1 a 10 Mbps sobre algunos medios.
- Cables:

- 10Base5 (Ethernet gruesa). Usa un cable coaxial grueso y tiene una velocidad de 10 Mbps. Los segmentos pueden ser hasta 500 m en longitud con hasta 100 nodos. Se hacen las conexiones usando derivaciones de vampiro: se inserta un polo hasta la mitad del cable. La derivación es dentro un transceiver, que contiene la electrónica para la detección de portadores y choques. Entre el transceiver y el computador es un cable de hasta 50 m. A veces se pueden conectar más de un computador a un solo transceiver. En el computador hay un controlador que crea marcos, hace checksums, etc.
  - 10Base2 (Ethernet delgada). Usa un cable coaxial delgado y dobla más fácilmente. Se hacen las conexiones usando conectores de T, que son más fáciles para instalar y más confiables. La detección de derivaciones malas, rupturas, y conectores flojos es un gran problema con ambas. Un método que se usa es la medición de la propagación y la reflexión de un pulso en el cable.
  - 10Base-T. Simplifica la ubicación de rupturas. Cada estación tiene una conexión con un hub (centro). Los cables normalmente son los pares trenzados. La desventaja es que los cables tienen un límite de solamente 100 m, y también el costo de un hub puede ser alto.
  - 10Base-F. Usa la fibra óptica. Es cara pero buena para las conexiones entre edificios (los segmentos pueden tener una longitud hasta 2000 m). Para eliminar el problema con las longitudes máximas de los segmentos, se pueden instalar repetidores que reciben, amplifican, y retransmiten las señales en ambas direcciones. La única restricción es que la distancia entre cualquier par de transceivers no puede ser más de 2,5 km y no puede haber más de cuarto repetidores entre transceivers.
- Codificación de Manchester. En 802.3 no hay ningún reloj de maestro. Este produce un problema en la detección de bits distintos (por ejemplo, ¿cómo se detectan dos bits de 0 en vez de tres?). En la codificación de Manchester se usan dos señales para cada bit. Se transmite un bit de 1 estableciendo un voltaje alto en el primer intervalo y un voltaje bajo en el segundo (un bit de 0 es el inverso). Porque cada bit contiene una transición de voltajes la sincronización es sencilla.

Figura 1.24.-Codificacion Manchester.

- Marcos:
  - El preámbulo es 7 bytes de bits que se alternan. La codificación de Manchester de esto produce una onda que el recibidor puede usar para sincronizar su reloj con el mandador. Después está el inicio del marco.
  - La dirección de destino puede tener un bit alto de 1, que indica la dirección de un grupo. Todas las estaciones reciben los marcos que tienen este bit encendido, lo que permite el multicast. Una dirección de todos unos es para el broadcast. El próximo bit distingue entre las direcciones locales y las globales, que son únicas en el mundo.
  - La longitud no puede ser 0; un marco debe ser por lo menos 64 bytes. Hay dos razones. Simplifica la distinción entre marcos válidos y basura producida por choques. Más importante permite que el tiempo para mandar un marco es suficiente para detectar un choque con la estación más lejana.
  - Para una LAN de 10 Mbps con una longitud máxima de 2500 metros y cuatro repetidores, el marco mínimo debe tomar 51,2 microsegs, que corresponde a 64 bytes. Se rellena si no hay suficientes datos. Nota que con redes más rápidas se necesitan marcos más largos o longitudes máximas más cortas.
  - El checksum es CRC.
  - Algoritmo de retiro de manera exponencial binaria. Después de un choque se divide el tiempo en intervalos de 2t, que es 51,2 microsegundos. Después del choque i cada estación elige un número aleatorio entre 0 y 2i-1 (pero con un máximo de 1023) y espera por un período de este número de intervalos. Después de 16 choques el controlador falla. Este algoritmo adapta automáticamente al número de estaciones que están tratando de mandar.

- Con más y más estaciones y tráfico en una LAN de 802.3, se satura la LAN. Una posibilidad para aumentar el rendimiento del sistema sin usar una velocidad más alta es una LAN 802.3 conmutada.
- El conmutador consiste en un backplane en que se insertan 4 a 32 tarjetas que tienen uno a ocho puertas de (por lo general) 10BaseT.
- Cuando un marco llega en la tarjeta, o se reenvía a una estación conectada a la misma tarjeta o se reenvía a otra tarjeta.
- En un diseño cada tarjeta forma su propio dominio de choques. Es decir, cada tarjeta es un LAN, y todas las tarjetas pueden transmitir paralelamente.
- Otro diseño es que cada puerta forma su propio dominio de choques. La tarjeta guarda los marcos que llegan en RAM y los choques son raros. Este método puede aumentar el rendimiento de la red un orden de magnitud.
- Se pueden conectar un hub a una puerta también.
- Además de 802.3, existen 802.4 (bus de token) y 802.5 (anillo de token). La idea es que las estaciones alternan en el uso del medio (intercambiando un token, que representa el turno). La ventaja es que el tiempo máximo de espera para mandar un marco tiene un límite. En el bus de token se usa un medio de broadcast, mientras que en el anillo de token se usan enlaces de punto-a-punto entre las estaciones.

1.9.-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.

La Capa 4 del computador de origen se comunica con la Capa 4 del computador de destino, Figura 1.25. Las normas y convenciones utilizadas para esta capa reciben el nombre de protocolos de la Capa 4. Es importante recordar que los protocolos preparan datos en forma

lineal. El protocolo en una capa realiza un conjunto determinado de operaciones sobre los datos al prepararlos para ser enviados a través de la red. Los datos luego pasan a la siguiente capa donde otro protocolo realiza otro conjunto diferente de operaciones.

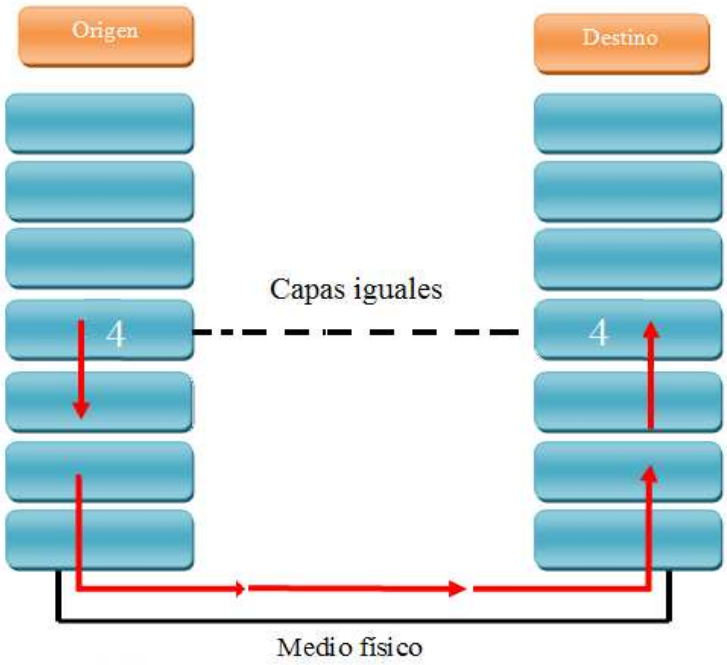

Figura 1.25.-Comunicación de computadores por medio de la capa 4 del modelo OSI.

Una vez que el paquete llega a su destino, los protocolos deshacen la construcción del paquete que se armó en el extremo de origen. Esto se hace en orden inverso. Los protocolos para cada capa en el destino devuelven la información a su forma original para que la aplicación pueda leer los datos correctamente.

1.10.-Protocolo CSMA/CD.

Ethernet es una tecnología de broadcast de medios compartidos. El método de acceso CSMA/CD que se usa en Ethernet ejecuta tres funciones:

- Transmitir y recibir paquetes de datos.
- Decodificar paquetes de datos y verificar que las direcciones sean válidas antes de transferirlos a las capas superiores del modelo OSI.
- Detectar errores dentro de los paquetes de datos o en la red

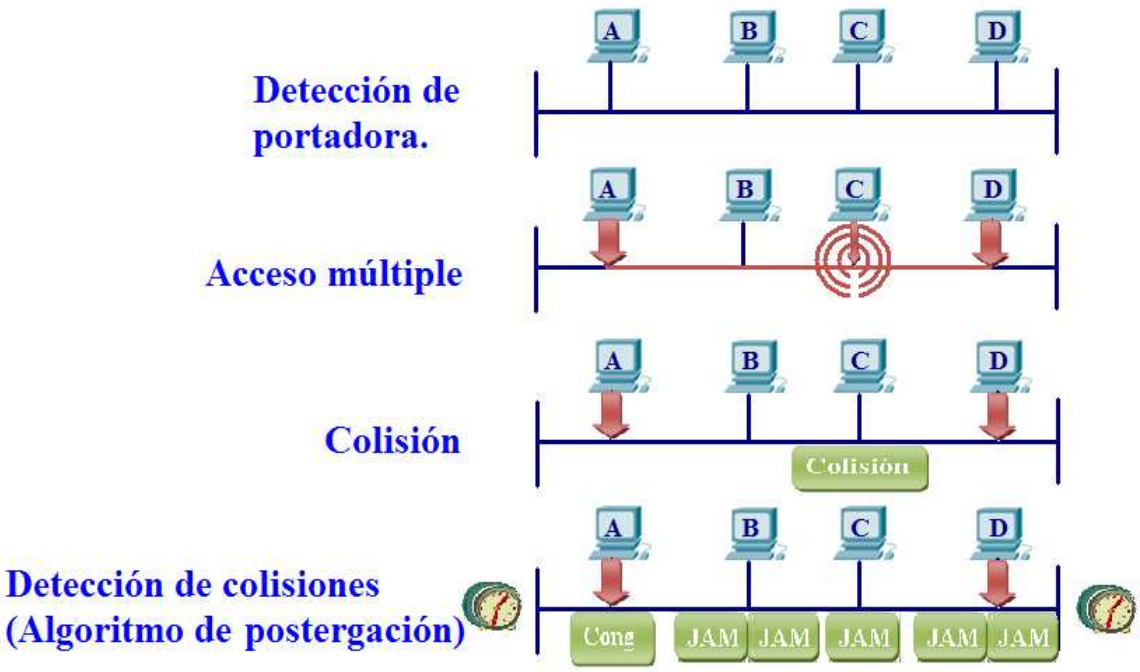

Figura 1.26.-Funcionamiento de CSMA/CD.

Ventajas Del Modelo OSI en el método de acceso CSMA/CD, los dispositivos de networking que tienen datos para transmitir funcionan en el modo "escuchar antes de transmitir". Esto significa que cuando un nodo desea enviar datos, primero debe determinar si los medios de networking están ocupados. Si el nodo determina que la red está ocupada, el nodo esperará un tiempo determinado al azar antes de reintentar. Si el nodo determina que el medio de networking no está ocupado, comenzará a transmitir y a escuchar. El nodo escucha para asegurarse que ninguna otra estación transmita al mismo tiempo. Una vez que ha terminado de transmitir los datos, el dispositivo vuelve al modo de escuchar. Figura 1.26

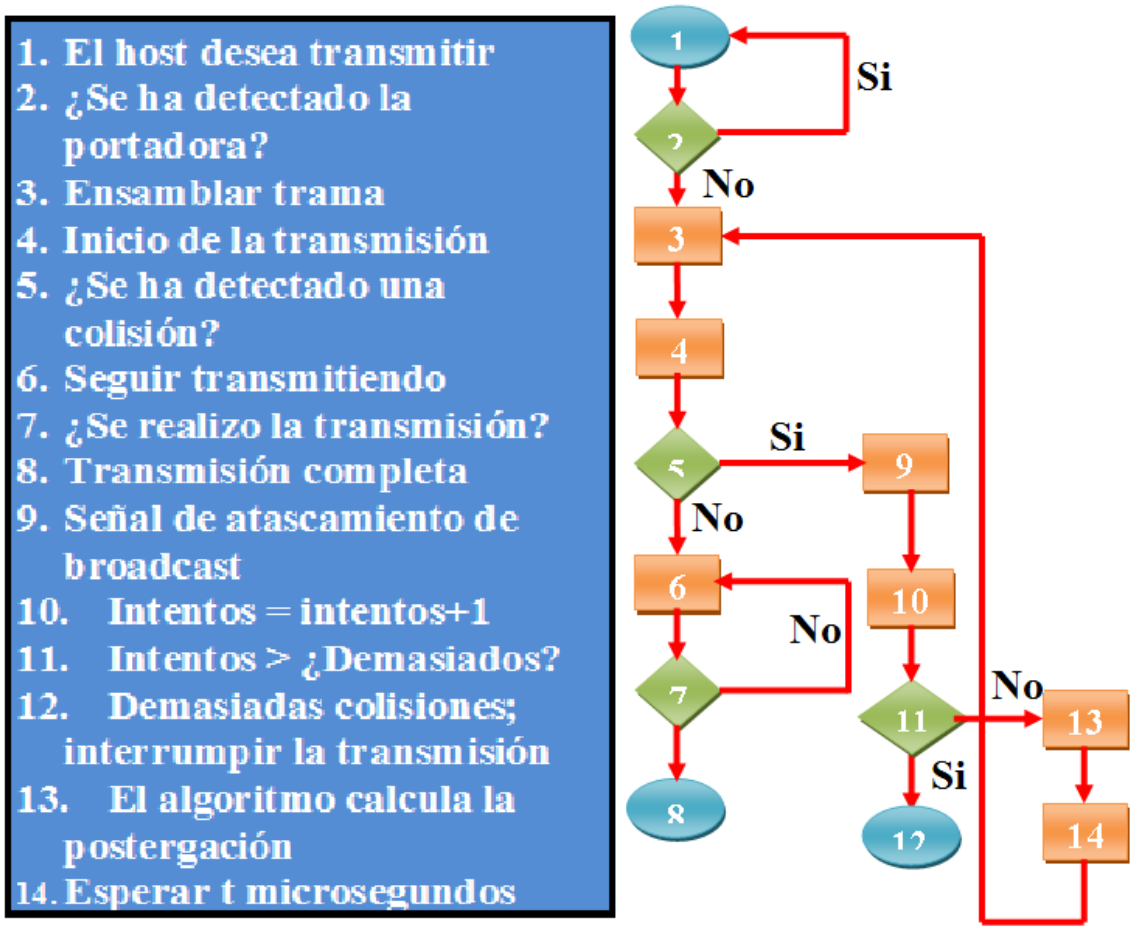

Figura 1.27.-Diagrama de flujo del protocolo CSMA/CD.

Los dispositivos de networking detectan que se ha producido una colisión cuando aumenta la amplitud de la señal en los medios de networking.

Cuando se produce una colisión, cada nodo que se encuentra en transmisión continúa transmitiendo por poco tiempo a fin de asegurar que todos los dispositivos detecten la colisión. Una vez que todos los dispositivos la han detectado, se invoca el algoritmo de postergación y la transmisión se interrumpe. Los nodos interrumpen la transmisión por un período determinado al azar, que es diferente para cada dispositivo. Cuando caduca el período de retardo cada nodo puede intentar ganar acceso al medio de networking. Los dispositivos involucrados en la colisión no tienen prioridad para transmitir datos.

1.11.-Protocolos de red.

Los conjuntos de protocolos son colecciones de protocolos que posibilitan la comunicación de red desde un host, a través de la red, hacia otro host. Un protocolo es una descripción formal de un conjunto de reglas y convenciones que rigen un aspecto particular de cómo los dispositivos de una red se comunican entre sí.

Los protocolos determinan el formato, la sincronización, la secuenciación y el control de errores en la comunicación de datos. Sin protocolos, el computador no puede armar o reconstruir el formato original del flujo de bits entrantes desde otro computador.

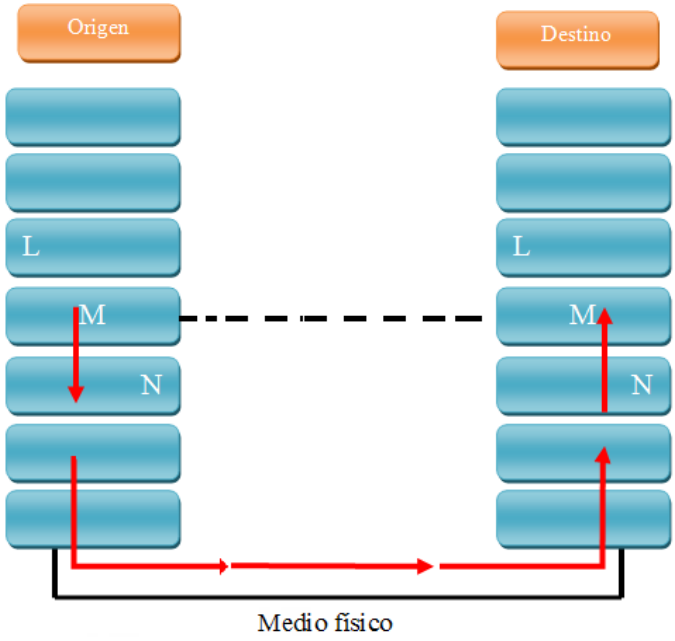

Figura 1.28.- Capas de Comunicación de Computadores.

Tabla 1.5.- Modelo físico

Modelo físico	
L.M.N	Capas de nuestro modelo de Comunicación de Computadores
Msource, Mdestination	Capas de pares
→	Comunicación entre pares
Protocolo de M capas	Las reglas mediante las cuales Msource se

	comunica con Mdestination

Los protocolos controlan todos los aspectos de la comunicación de datos, que incluye lo siguiente:

- Cómo se construye la red física
- Cómo los computadores se conectan a la red
- Cómo se formatean los datos para su transmisión
- Cómo se envían los datos
- Cómo se manejan los errores

Estas normas de red son creadas y administradas por una serie de diferentes organizaciones y comités.

Entre ellos se incluyen el Instituto de Ingeniería Eléctrica y Electrónica (IEEE), el Instituto Nacional Americano de Normalización (ANSI), la Asociación de la Industria de las Telecomunicaciones (TIA), la Asociación de Industrias Electrónicas (EIA) y la Unión Internacional de Telecomunicaciones (UIT), antiguamente conocida como el Comité Consultivo Internacional Telegráfico y Telefónico (CCITT).

1.12.-Dispositivos de red.

1.12.1.-RDSI.

RDSI ofrece conexiones conmutadas por demanda o servicios de respaldo conmutados. La interfaz de acceso básico (BRI) RDSI está compuesta de dos canales principales de 64 kbps, (canales B) para datos y un canal delta (canal D) de 16 kbps que se usa para señalizar y para otras tareas de administración del enlace.

Figura 1.29.-R.D.S.I

1.12.2.-Módem.

Las tarjetas de módem operan en la capa de acceso de red. La capa de acceso de red define los procedimientos para realizar la interfaz con el hardware de la red y para tener acceso al medio de transmisión. Los estándares del protocolo de los módem tales como el Protocolo Internet de enlace serial (SLIP) y el Protocolo de punta a punta (PPP) brindan acceso a la red a través de una conexión por módem. Debido a un intrincado juego entre las especificaciones del hardware, el software y los medios de transmisión, existen muchos protocolos que operan en esta capa. Esto puede generar confusión en los usuarios. La mayoría de los protocolos reconocibles operan en las capas de transporte y de Internet del modelo TCP/IP.

Figura 1.30.-Modem.

1.12.3.-Puente (Bridge).

Los puentes convierten los formatos de transmisión de datos de la red además de realizar la administración básica de la transmisión de datos. Los puentes, tal como su nombre lo indica, proporcionan las conexiones entre LAN. Los puentes no sólo conectan las LAN, sino que además verifican los datos para determinar si les corresponde o no cruzar el puente. Esto aumenta la eficiencia de cada parte de la red.

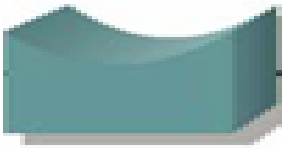

Figura 1.31.- Bridge.

1.12.4.-Switches.

Los switches de grupos de trabajo agregan inteligencia a la administración de transferencia de datos. No sólo son capaces de determinar si los datos deben permanecer o no en una LAN, sino que pueden transferir los datos únicamente a la conexión que necesita esos datos. Otra diferencia entre un puente y un switch es que un switch no convierte formatos de transmisión de datos.

Figura 1.32.- Switch.

1.12.5.-Encaminador (Router).

Los routers poseen todas las capacidades indicadas arriba. Los routers pueden regenerar señales, concentrar múltiples conexiones, convertir formatos de transmisión de datos, y manejar transferencias de datos. También pueden conectarse a una WAN, lo que les permite conectar LAN que se encuentran separadas por grandes distancias. Ninguno de los demás dispositivos puede proporcionar este tipo de conexión.

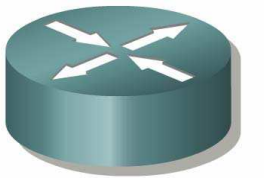

Figura 1.33.- Router.

1.13.- ¿Qué es internet?

La Internet es una red de redes. Actualmente conecta miles de redes para permitir compartir información y recursos a nivel mundial. Con la Internet los usuarios pueden compartir, prácticamente, cualquier cosa almacenada en un archivo.

Las comunicaciones en Internet son posibles entre redes de diferentes ambientes y plataformas. Este intercambio dinámico de datos se ha logrado debido al desarrollo de los protocolos de comunicación. Los protocolos son un conjunto de reglas para el intercambio de datos que permiten a los usuarios comunicarse entre diferentes redes.

1.14.- El internet y su relación con Organismos.

1.14.1.- Consorcio de Red Mundial Extensa (Word Wide Web consortium) (w3c).

Este trabaja con la comunidad global para producir software de especificaciones y referencia. El consorcio está formado por miembros de la industria, pero sus productos son gratuitos. El Web de W3C se encuentra en el Laboratorio para la Ciencia de la Computación del Instituto de Massachusetts (MIT LCS) y en el Instituto Nacional de Francia para la Investigación de la Informática y la Automatización (INRIA), en colaboración con el Concilio Europeo para la Investigación Nuclear (CERN), donde fue desarrollado originalmente el Web.

1.14.2. – El internet como un diseño de la fuerza de la tarea (Internet engineering task force) (IETF).

Este organismo se encarga del desarrollo y la ingeniería de los protocolos de Internet. La IETF es una comunidad internacional de diseñadores de red, operadores, vendedores e investigadores preocupados con la evolución de la arquitectura de Internet y su buen funcionamiento. Está abierto para cualquier interesado.

1.15.- Clasificación de los tipos de conexión.

La Internet es una red global en la cual, cada computadora actúa como un cliente y un servidor. La Internet consta de varios componentes conectados:

- Backbones: líneas de comunicación de alta velocidad y ancho de banda que unen hosts o redes.

- Redes: grupos de hardware y software de comunicación dedicados a la administración de la comunicación a otras redes. Todas las redes tienen conexiones de alta velocidad para dos o más redes.
- Proveedores del Servicio de Internet (Internet Service Provider) (ISPs): son computadoras que tienen acceso a la Internet. Varios proveedores de servicios en línea como Compuserve, MPSNet y Spin, actúan como ISPs proveyendo acceso a Internet a todos sus suscriptores.
- Hosts: computadoras cliente/servidor. En ellos es donde los usuarios ven la interacción con la Internet.

Cada computadora que se conecta directamente a una red es un host. Todos los hosts tienen una dirección de red única. Esta es comúnmente conocida como la dirección IP.
La manera en que Internet permite a las computadoras conectarse es similar a como trabaja una red de área local (Local Area Network) (LAN).
En una red simple, se tienen dos computadoras y una conexión de datos. Las computadoras se comunican enviando un paquete a través de la conexión. Un paquete es una unidad de datos que viaja entre hosts de una red específica.
Un paquete consiste de dos secciones:

- Encabezado: contiene la localización de la dirección física y otros datos de red.
- Datos: contiene un datagrama.

Los dos protocolos de Internet que trabajan en conjunto para la transmisión de datos son:

- Transmission Control Protocol (TCP)
- Internet Protocol (IP)

En conjunto estos protocolos son conocidos como TCP/IP.
Las computadoras también pueden comunicarse con otras computadoras fuera de la LAN. Al conjunto de LANs se les conoce como redes de área amplia (Wide Area Network) (WAN). Los ruteadores y gateways proveen las conexiones entre diferentes LANs. Si las LANs son del mismo tipo, se usa un ruteador. Si las LANs utilizan diferentes protocolos de comunicación, o topologías, los gateways son usados para convertir los paquetes en el formato requerido. Cuando un gateway recibe un paquete, el gateway utiliza la información de la dirección y el encabezado del datagrama para determinar la localización del

destinatario de los datos. El gateway reempaqueta el datagrama en el formato del paquete adecuado hacia la siguiente conexión. Los datos pueden cruzar varias LANs antes de llegar a su destino.

La Internet es considerada una red de área amplia, independiente a la topología. Esta independencia de las diversas topologías de LAN la realiza el protocolo estándar IP. El encabezado del paquete IP contiene una dirección de cuatro octetos que identifican a cada una de los equipos. Cuando un paquete es enviado hacia un host, la computadora determina si el paquete es local o remoto (dentro o fuera de la LAN). Si el paquete es local, el mismo lo transmite; si es remoto lo envía hacia un gateway el cual determina la dirección final. La información de la dirección también determina cómo será ruteado el paquete a través de Internet. Normalmente el gateway utiliza la localización del destinatario para determinar la mejor ruta para enviar el paquete.

Si alguna red intermedia llegara a estar demasiado ocupada o no disponible, el gateway dinámicamente selecciona una ruta alterna. Una vez que el paquete es enviado, cada red que reciba el paquete, repite el proceso redirigiéndolo cuando sea necesario. Este proceso se repite hasta que el paquete llega a su destino. Diferentes paquetes pueden tomar diferentes rutas, aún cuando contengan información del mismo archivo o mensaje. Los datos del paquete son reensamblados en el destinatario.

1.16.- Definición y fundamentos del intranet.

Una Intranet es una red informática privada dentro de una empresa u organización que está basada en los principios, normas, protocolos y herramientas usados en internet.

Podría decirse que una Intranet es una versión privada de internet. El prefijo latino “intra” significa “dentro”, mientras que “Inter” significa “entre”, lo que pone de manifiesto la idea de que una Intranet es una red enfocada hacia “dentro”, hacia el funcionamiento interno de la organización. El principal objetivo de una Intranet es compartir información entre los empleados o miembros de la organización.

Como regla general, una Intranet está compuesta de diferentes redes de área local interconectadas entre sí formando una red de área amplia (WAN) mediante líneas de comunicaciones privadas. También es habitual encontrar intranets que están conectadas con internet, permitiendo a los usuarios acceder a los servicios comunes de internet (correo

electrónico, navegación por la World Wide Web, etc...) mediante dispositivos que aportan la seguridad adecuada a esta conexión, tales como cortafuegos y servidores proxy. Cuando una parte de la Intranet se hace a su vez accesible desde el exterior, principalmente a socios, clientes y proveedores, entonces esa parte se convierte en una Extranet.

Como ya se ha indicado, una intranet utiliza los mismos esquemas de funcionamiento que internet, si bien ambos conceptos se diferencian fundamentalmente en el ámbito y propiedad de la red. Internet es una red pública, abierta a cualquier usuario a nivel mundial, mientras que una intranet es totalmente privada y solo se puede acceder a ella mediante invitación.

Las intranets se basan en la arquitectura cliente/servidor y sobre todo en el protocolo TCP/IP. Como servidor se admite cualquier máquina capaz de soportar dicho protocolo, incluso mainframes, mientras que los clientes suelen ser en la actualidad ordenadores personales (PCs) en su inmensa mayoría. Similar importancia que el protocolo TCP/IP tiene en la implantación de una intranet la tiene también el principal software usado en la parte cliente: el explorador (browser). Gracias a este componente software se consigue una total uniformidad en el uso de aplicaciones e interoperabilidad entre máquinas y usuarios.

Las redes locales y de área extensa basadas en sistemas tradicionales presentan ciertas limitaciones en cuanto a la interconexión de los sistemas que las componen, dada la variedad de protocolos existentes en el mercado y la falta de una definición de interfaz universal. La principal dificultad para los administradores era hacer que máquinas y sistemas operativos diferentes dialogaran entre sí. Pues bien, con la tecnología intranet se resuelve este problema, pues existen tanto un protocolo como un interfaz definido a nivel universal.

1.16.1.- ¿Por qué se debe considerar emplear una intranet?

Una intranet básica puede ser instalada en horas o días y puede servir como un "depósito de información" para la compañía completa.

La Intranet propone el concepto de usar el paginador de Web como la interface de información universal.

Las ventajas de este nuevo elemento de red son:

- Reduce el tiempo de aprendizaje de los usuarios.

- Simplifica la instalación de aplicaciones.
- Presenta diferentes tipos de información: texto, gráficas, sonido y video.
- Actúa como "front-end" para las aplicaciones cliente-servidor.
- Permite el acceso a bases de datos.

Una de las principales motivaciones para la adopción de la Intranet es que permite a las organizaciones evolucionar de una estrategia de publicación calendarizada a publicación en base a la demanda.
Tradicionalmente, las compañías publican una vez al año el manual del empleado. Cualquier cambio de último momento o ajuste importante, sería actualizado hasta el siguiente año. La Intranet ofrece dos soluciones a este problema:

1. El empleado decide cuando consultar la información.
2. La información puede actualizarse instantáneamente.

1.16.2.- Aplicaciones Cliente/Servidor.

Las aplicaciones cliente/servidor tradicionalmente manejan dos o tres capas:

1. Front End
2. (Middleware)
3. Back End

Actualmente el desarrollo del Front End se realiza por medio de herramientas como Visual Basic, Delphi, C++ y se instala en cada una de las computadoras. Actualizar o añadir nuevos módulos a las aplicaciones es costoso y lento.
Además las aplicaciones se deben compilar para cada plataforma.
Con el nuevo paradigma del paginador como cliente universal este problema es eliminado por varios factores:

- Las aplicaciones residen en las páginas Web.
- Los objetos y componentes se instalan automáticamente o de manera muy sencilla.

- Existen paginadores para todos los sistemas operativos.

1.16.3.- Las aplicaciones de una intranet dentro de las empresas.

Las siguientes secciones ejemplifican el uso de la Intranet en los principales departamentos de las empresas:

- Difusión y Comunicación
- Ventas y Mercadeo
- Recursos Humanos
- Educación y Capacitación

La implantación de una Intranet a nivel global para la organización tiene como objetivo mejorar la productividad, acortar el tiempo preciso para las actividades rutinarias y trazar una vía más rápida para las decisiones. En realidad, estas tecnologías suponen una transformación en la manera de hacer negocios. Hay muchas aplicaciones claves para el uso de una Intranet (o extranet), pero entre todas se pueden distinguir claramente las siguientes:

- Publicación. La publicación de documentos a través de la Intranet permite distribuir de una manera más eficiente la información entre los miembros de la organización. Hay una amplia variedad de documentos que son susceptibles de ser publicados a nivel intranet: boletines, documentación de recursos humanos, acción social, procedimientos organizativos, informes, manuales, distribución de trabajos, y un largo etcétera. Con esta tecnología se ahorran grandes cantidades de papel (las páginas web son un recurso renovable), pero lo más importante está en el acceso on-line, instantáneo y con potentes herramientas de búsqueda desde cualquier máquina del ámbito de la organización.

- Gestión de la información y el conocimiento. Las aplicaciones con tecnología Intranet permiten enlazar diferentes bases de datos y en general gestionar de una manera más eficiente los recursos de información haciendo más sencillo el acceso a los datos. Además favorece la cultura del trabajo en equipo con diferentes herramientas para teleconferencia, aplicaciones para trabajo en grupo del tipo Microsoft NetMeeting, etc.

- Formación. En una intranet se pueden implantar sistemas de formación a distancia que disminuyen los costos y amplían la disponibilidad y opciones en cuanto a horarios y alcance. Especialmente útil es este tipo de formación en intranets que incluyen sucursales en diferentes zonas horarias. La formación así concebida es un paso más de la ya conocida CBT (Computer Based Training), dando lugar a términos como WBT (Web Based Training) o WBI (Web Based Instruction)

1.16.4.- Características y Beneficios.

La Intranet tiene las siguientes características:

- Rápido Diseño.
- Escalabilidad.
- Fácil navegación.
- Accesible para la mayoría de las plataformas de cómputo.
- Integra la estrategia de cómputo distribuido.
- Adaptable a los sistemas de información propietarios.
- Uso de multimedia.

Los beneficios para la empresa son:

- Requiere poca inversión para su inicio
- Ahorra tiempo y costos en comparación de la distribución de información tradicional (papel).
- Su estrategia de cómputo distribuido utiliza los recursos de cómputo más efectivamente.
- Tiene una interfaz sencilla y flexible (vínculos).
- Independiente de la plataforma.

1.17.- ¿Qué es una extranet?

Una extranet es un puente entre organizaciones construido con los mismos protocolos de normas abiertas basados en internet que forman la base de una intranet.

El empleo de una extranet permite a las organizaciones compartir con sus asociados la información privada que se encuentra en sus intranets. Puede ser una extranet mutua,

cuando ambas organizaciones aportan una parte de sus intranets, o puede ser que solo una de ellas sea la que aporte la información.

La extranet se puede ver como una red privada que usa las normas y protocolos de internet y redes de comunicaciones (normalmente públicas) para compartir con seguridad una parte de la información de la organización con proveedores, clientes, socios, etc.

En realidad se trata de una parte de la Intranet que se extiende a usuarios externos a la compañía. La idea es aprovecharse de los beneficios de normas como Lenguaje de Marcas de Hipertexto (HyperText Markup Language) HTML, http, smtp., etc. Para mejorar la eficiencia en las relaciones entre organizaciones.

Son muchos los usos y actividades para los que una extranet puede ser aplicada:

- Intercambiar datos usando EDI (Electronic Data Interchange)
- Compartir catálogos de productos con asociados
- Colaborar con otras compañías en esfuerzos de desarrollo conjuntos
- Compartir programas de entrenamiento y formación
- Compartir noticias de interés común
- Ofrecer acceso a datos y aplicaciones

Netscape, Oracle y Sun Microsystems se encuentran desarrollando una alianza para asegurar que sus productos extranet puedan integrarse por medio de la estandarización del lenguaje Java script y la arquitectura CORBA (Common Object Request Broker Architecture).

Por su parte, Microsoft soporta en la actualidad el protocolo de túnel punto a punto (Point to Point Tunneling Protocol) (PPTP) y está trabajando con American Express y otras compañías en el standard OBI (Open Buyin on the Internet). Lotus Corporation basa su oferta extranet en el pionero y ya conocido Lotus Notes, un sistema ampliamente utilizado en el campo del groupware.

No debe confundirse una extranet con un web empresarial. Este último es un área comercial, orientada principalmente a aspectos de marketing de la empresa, información al público y, en algunos casos, con ciertas capacidades para realizar compras a través de él.

La diferencia estriba en que una extranet ofrece acceso a datos que permiten hacer negocios.

El aspecto más importante a la hora de planificar una extranet es la seguridad y privacidad, puesto que abrir una intranet al exterior conlleva riesgos evidentes. Para evitar estos riesgos se hace imprescindible el uso de sistemas de seguridad tales como cortafuegos (firewalls), así como mecanismos de certificación digital, autentificación de usuarios, encriptación, etc.

Capítulo 2.- Protocolo TCP/IP.

2.1.-Definición.

El Protocolo de control de transporte/protocolo Internet (TCP/IP) es un conjunto de protocolos o reglas desarrollados para permitir que los computadores que cooperan entre sí puedan compartir recursos a través de una red.

2.2.-Modelo TCP/IP.

El estándar histórico y técnico de la Internet es el modelo TCP/IP. El Departamento de Defensa de EE.UU. (DoD) creó el modelo de referencia TCP/IP porque necesitaba diseñar una red que pudiera sobrevivir ante cualquier circunstancia, incluso una guerra nuclear. En un mundo conectado por diferentes tipos de medios de comunicación, como alambres de cobre, microondas, fibras ópticas y enlaces satelitales, el DoD quería que la transmisión de paquetes se realizara cada vez que se iniciaba y bajo cualquier circunstancia. Este difícil problema de diseño dio origen a la creación del modelo TCP/IP.

A diferencia de las tecnologías de networking propietarias mencionadas anteriormente, el TCP/IP se desarrolló como un estándar abierto. Esto significaba que cualquier persona podía usar el TCP/IP. Esto contribuyó a acelerar el desarrollo de TCP/IP como un estándar.

El modelo TCP/IP tiene las siguientes cuatro capas:

- Capa de aplicación
- Capa de transporte
- Capa de Internet
- Capa de acceso a la red

Aunque algunas de las capas del modelo TCP/IP tienen el mismo nombre que las capas del modelo OSI, las capas de ambos modelos no se corresponden de manera exacta. Lo más notable es que la capa de aplicación posee funciones diferentes en cada modelo.

Los diseñadores de TCP/IP sintieron que la capa de aplicación debía incluir los detalles de las capas de sesión y presentación OSI. Crearon una capa de aplicación que maneja aspectos de representación, codificación y control de diálogo.

Figura 2.1.-Capas del Modelo TCP/IP.

La capa de transporte se encarga de los aspectos de calidad del servicio con respecto a la confiabilidad, el control de flujo y la corrección de errores. Uno de sus protocolos, el protocolo para el control de la transmisión (TCP), ofrece maneras flexibles y de alta calidad para crear comunicaciones de red confiables, sin problemas de flujo y con un nivel de error bajo.

TCP es un protocolo orientado a conexión. Mantiene un diálogo entre el origen y el destino mientras empaqueta la información de la capa de aplicación en unidades denominadas segmentos. Orientado a conexión no significa que existe un circuito entre los computadores que se comunican. Significa que segmentos de la Capa 4 viajan de un lado a otro entre dos hosts para comprobar que la conexión exista lógicamente para un determinado período. El propósito de la capa Internet es dividir los segmentos TCP en paquetes y enviarlos desde cualquier red.

Los paquetes llegan a la red de destino independientemente de la ruta que utilizaron para llegar allí. El protocolo específico que rige esta capa se denomina Protocolo Internet (IP). En esta capa se produce la determinación de la mejor ruta y la conmutación de paquetes.

La relación entre IP y TCP es importante. Se puede pensar en el IP como el que indica el camino a los paquetes, en tanto que el TCP brinda un transporte seguro.

El nombre de la capa de acceso de red es muy amplio y se presta a confusión. También se conoce como la capa de host a red. Esta capa guarda relación con todos los componentes, tanto físicos como lógicos, necesarios para lograr un enlace físico. Incluye los detalles de tecnología de networking, y todos los detalles de las capas físicas y de enlace de datos del modelo OSI.

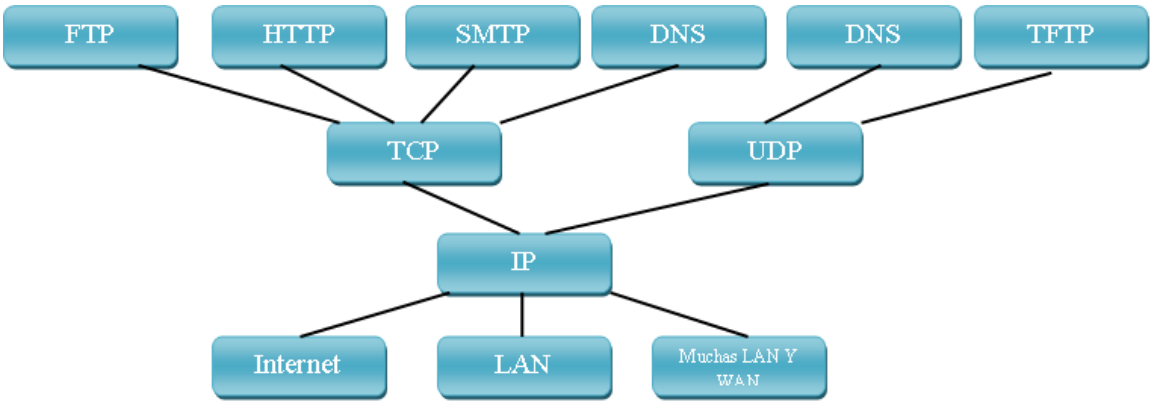

Figura 2.2.- Protocolos del modelo TCP/IP.

La figura ilustra algunos de los protocolos comunes especificados por las capas del modelo de referencia TCP/IP. Algunos de los protocolos de capa de aplicación más comúnmente usados incluyen los siguientes:

- Protocolo de Transferencia de Archivos (FTP)
- Protocolo de Transferencia de Hipertexto (HTTP)
- Protocolo simple de transferencia de correo (SMTP)
- Sistema de denominación de dominios (DNS)
- Protocolo Trivial de Transferencia de Archivos (TFTP)

Los protocolos de capa de transporte comunes incluyen:

- Protocolo para el Control del Transporte (TCP)
- Protocolo de Datagrama de Usuario (UDP)

Los protocolos de la capa Internet comunes son:

- Protocolo Internet (IP)
- Protocolo (ICMP)

Los protocolos de la capa de acceso de red màs comunes son:

- Protocolo (Address Resolution Protocol) ARP.
- Protocolo (Reverse Address Resolution Protocol) RARP.
- Protocolo (Serial-Line Internet Protocol) SLIP.
- Protocolo (Point to Point Protocol) PPP.

La capa de acceso de red se refiere a cualquier tecnología en particular utilizada en una red específica. Independientemente de los servicios de aplicación de red que se brinden y del protocolo de transferencia que se utilice, existe un solo protocolo de Internet, IP. Esta es una decisión de diseño deliberada. IP sirve como protocolo universal que permite que cualquier computador en cualquier parte del mundo pueda comunicarse en cualquier momento.

Comparando el modelo OSI con los modelos TCP/IP, surgen algunas similitudes y diferencias.

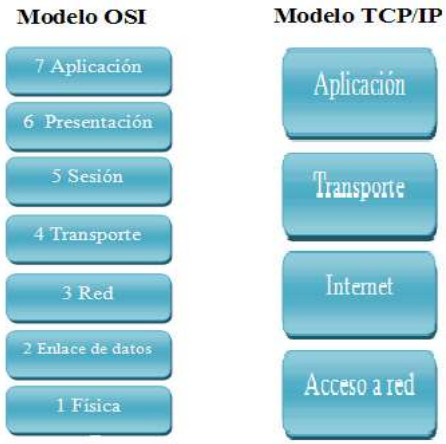

Figura 2.3.-Comparación del Modelo OSI y el Modelo TCP/IP.

Las similitudes incluyen:

- Ambos se dividen en capas.
- Ambos tienen capas de aplicación, aunque incluyen servicios muy distintos.
- Ambos tienen capas de transporte y de red similares.
- Ambos modelos deben ser conocidos por los profesionales de networking.
- Ambos suponen que se conmutan paquetes. Esto significa que los paquetes individuales pueden usar rutas diferentes para llegar al mismo destino. Esto se contrasta con las redes conmutadas por circuito, en las que todos los paquetes toman la misma ruta.

Las diferencias incluyen:

- TCP/IP combina las funciones de la capa de presentación y de sesión en la capa de aplicación.
- TCP/IP combina la capa de enlace de datos y la capa física del modelo OSI en la capa de Acceso de red.
- TCP/IP parece ser más simple porque tiene menos capas.
- Los protocolos TCP/IP son los estándares en torno a los cuales se desarrolló la Internet, de modo que la credibilidad del modelo TCP/IP se debe en gran parte a sus protocolos. En comparación, por lo general las redes no se desarrollan a partir del protocolo OSI, aunque el modelo OSI se usa como guía.

2.3.- Direccionamiento IP.

2.3.1.-Direcciones IPv4.

Un Router envía los paquetes desde la red origen a la red destino utilizando el protocolo IP. Los paquetes deben incluir un identificador tanto para la red origen como para la red destino. Utilizando la dirección IP de una red destino, un Router puede enviar un paquete a la red correcta. Cuando un paquete llega a un Router conectado a la red destino, este utiliza la dirección IP para localizar el computador en particular conectado a la red. Este sistema funciona de la misma forma que un sistema nacional de correo. Cuando se envía una carta, primero debe enviarse a la oficina de correos de la ciudad destino, utilizando el código

postal. Dicha oficina debe entonces localizar el destino final en la misma ciudad utilizando el domicilio. Es un proceso de dos pasos.

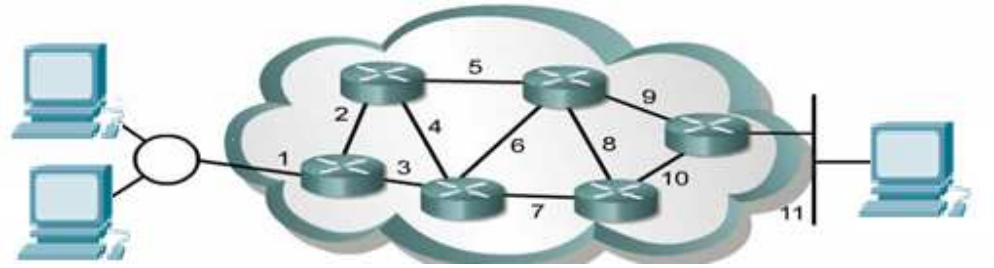

Figura 2.4.- Un Router envía los paquetes desde la red origen a la red destino utilizando el protocolo IP.

De igual manera, cada dirección IP consta de dos partes. Una parte identifica la red donde se conecta el sistema y la segunda identifica el sistema en particular de esa red. Como muestra la Figura 2.6, cada octeto varía de 0 a 255. Cada uno de los octetos se divide en 256 subgrupos y éstos, a su vez, se dividen en otros 256 subgrupos con 256 direcciones cada uno. Al referirse a una dirección de grupo inmediatamente arriba de un grupo en la jerarquía, se puede hacer referencia a todos los grupos que se ramifican a partir de dicha dirección como si fueran una sola unidad.

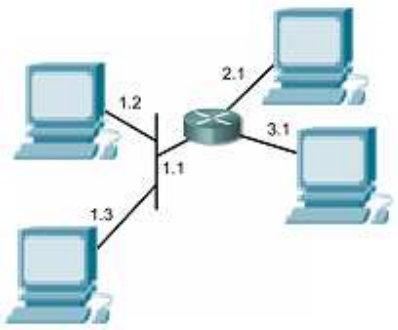

Figura 2.5.- Cada dirección IP consta de dos partes.

Tabla 2.1.-Octetos de una dirección IP.

Red	**Host**
1	1 2 3
2	1
3	1

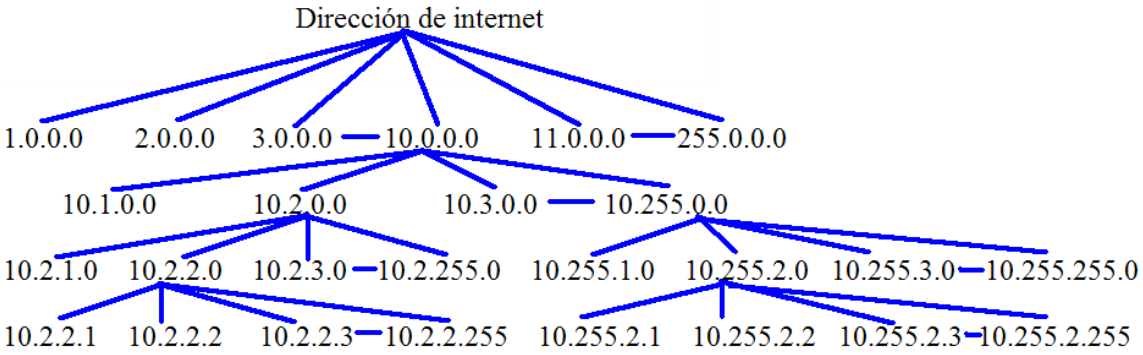

Figura 2.6.-Direccionamiento IP.

Este tipo de dirección recibe el nombre de dirección jerárquica porque contiene diferentes niveles. Una dirección IP combina estos dos identificadores en un solo número. Este número debe ser un número exclusivo, porque las direcciones repetidas harían imposible el enrutamiento. La primera parte identifica la dirección de la red del sistema. La segunda parte, la parte del host, identifica qué máquina en particular de la red.

Tabla 2.2.-Clases de Direcciones IP.

Clase de dirección	Cantidad de redes	Cantidad de host por red
A	126*	16,777,216
B	16,384	65,535
C	2,097,152	254
D (Multicast)	No es Aplicable	No es Aplicable

Las direcciones IP se dividen en clases para definir las redes de tamaño pequeño, mediano y grande. Las direcciones Clase A se asignan a las redes de mayor tamaño. Las direcciones Clase B se utilizan para las redes de tamaño medio y las de Clase C para redes pequeñas. El primer paso para determinar qué parte de la dirección identifica la red y qué parte identifica el host es identificar la clase de dirección IP.

Tabla 2.3.-Clase de direccion IP.

Clase de dirección IP	Bits de mayor peso	Primer intervalo de dirección de octeto	Número de bits en la dirección de red
Clase A	0	0-127*	8
Clase B	10	128-191	16
Clase C	110	192-223	24
Clase D	1110	224-239	28

2.3.2.-Direcciones IP Clase A, B, C, D y E.

Para adaptarse a redes de distintos tamaños y para ayudar a clasificarlas, las direcciones IP se dividen en grupos llamados clases.

Tabla 2.4.- Direccionamiento classful.

Clase A	**Red**	**Host**	**Host**	**Host**
Octeto	1	2	3	4
Clase B	**Red**	**Red**	**Host**	**Host**
Octeto	1	2	3	4
Clase A	**Red**	**Red**	**Red**	**Host**
Octeto	1	2	3	4
Clase A	**Host**	**Host**	**Host**	**Host**
Octeto	1	2	3	4

Esto se conoce como direccionamiento classful. Cada dirección IP completa de 32 bits se divide en la parte de la red y parte del host. Un bit o una secuencia de bits al inicio de cada dirección determinan su clase.

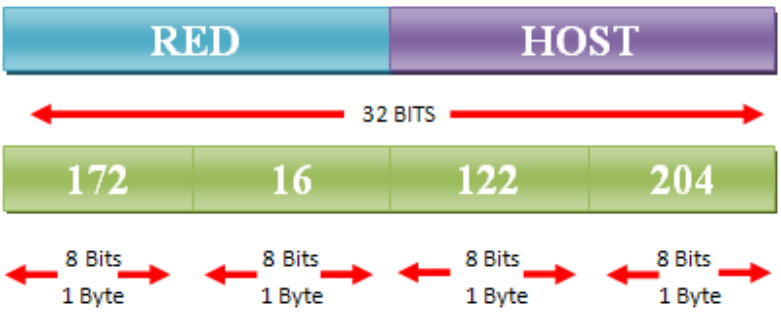

Figura 2.7.-Dirección IP.

La dirección Clase A se diseñó para admitir redes de tamaño extremadamente grande, de más de 16 millones de direcciones de host disponibles. Las direcciones IP Clase A utilizan sólo el primer octeto para indicar la dirección de la red. Los tres octetos restantes son para las direcciones host.

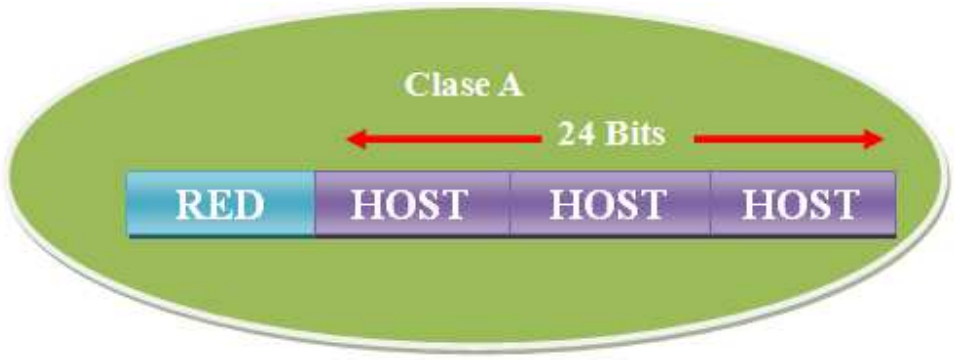

Figura 2.8.-Clase A.

El primer bit de la dirección Clase A siempre es 0. Con dicho primer bit, que es un 0, el menor número que se puede representar es 00000000, 0 decimal. El valor más alto que se puede representar es 01111111, 127 decimal. Estos números 0 y 127 quedan reservados y no se pueden utilizar como direcciones de red. Cualquier dirección que comience con un valor entre 1 y 126 en el primer octeto es una dirección Clase A.

La red 127.0.0.0 se reserva para las pruebas de loopback. Los routers o las máquinas locales pueden utilizar esta dirección para enviar paquetes nuevamente hacia ellos mismos. Por lo tanto, no se puede asignar este número a una red.

La dirección Clase B se diseñó para cumplir las necesidades de redes de tamaño moderado a grande. Una dirección IP Clase B utiliza los primeros dos de los cuatro octetos para indicar la dirección de la red. Los dos octetos restantes especifican las direcciones del host.

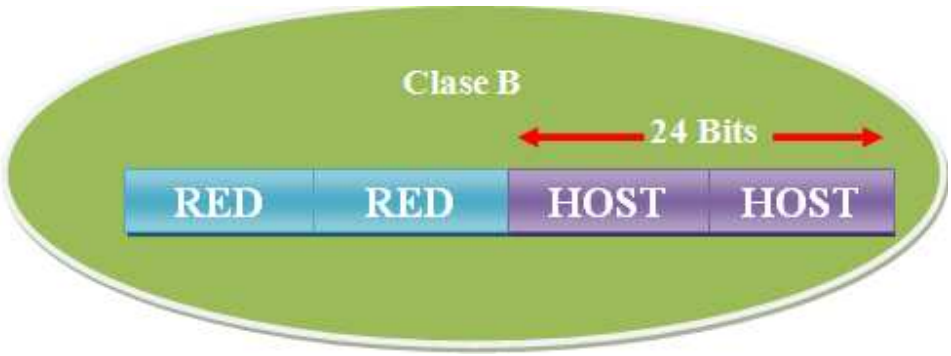

Figura 2.9.-Clase B.

Los primeros dos bits del primer octeto de la dirección Clase B siempre son 10. Los seis bits restantes pueden poblarse con unos o ceros. Por lo tanto, el menor número que puede representarse en una dirección Clase B es 10000000, 128 decimal. El número más alto que puede representarse es 10111111, 191 decimal. Cualquier dirección que comience con un valor entre 128 y 191 en el primer octeto es una dirección Clase B.

El espacio de direccionamiento Clase C es el que se utiliza más frecuentemente en las clases de direcciones originales. Este espacio de direccionamiento tiene el propósito de admitir redes pequeñas con un máximo de 254 hosts.

Una dirección Clase C comienza con el binario 110. Por lo tanto, el menor número que puede representarse es 11000000, 192 decimal. El número más alto que puede representarse es 11011111, 223 decimal. Si una dirección contiene un número entre 192 y 223 en el primer octeto, es una dirección de Clase C.

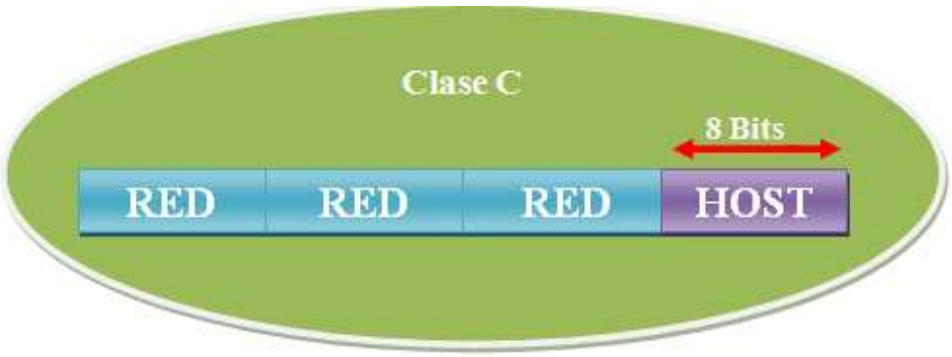

Figura 2.10.-Clase C.

La dirección Clase D se creó para permitir multicast en una dirección IP. Una dirección multicast es una dirección exclusiva de red que dirige los paquetes con esa dirección destino hacia grupos predefinidos de direcciones IP. Por lo tanto, una sola estación puede transmitir de forma simultánea una sola corriente de datos a múltiples receptores.

El espacio de direccionamiento Clase D, en forma similar a otros espacios de direccionamiento, se encuentra limitado matemáticamente. Los primeros cuatro bits de una dirección Clase D deben ser 1110. Por lo tanto, el primer rango de octeto para las direcciones Clase D es 11100000 a 11101111, o 224 a 239.

Una dirección IP que comienza con un valor entre 224 y 239 en el primer octeto es una dirección Clase D.

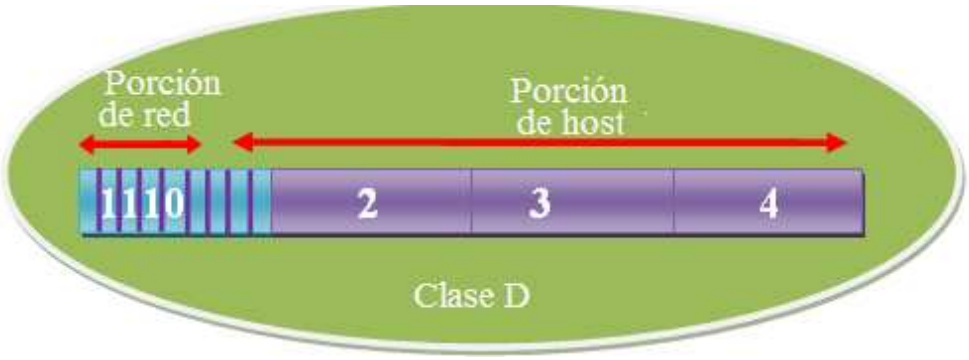

Figura 2.11.-Clase D.

Se ha definido una dirección Clase E. Sin embargo, la Fuerza de tareas de ingeniería de Internet (IETF) ha reservado estas direcciones para su propia investigación. Por lo tanto, no se han emitido direcciones Clase E para ser utilizadas en Internet. Los primeros cuatro bits de una dirección Clase E siempre son 1s.

Por lo tanto, el rango del primer octeto para las direcciones Clase E es 11110000 a 11111111, o 240 a 255.

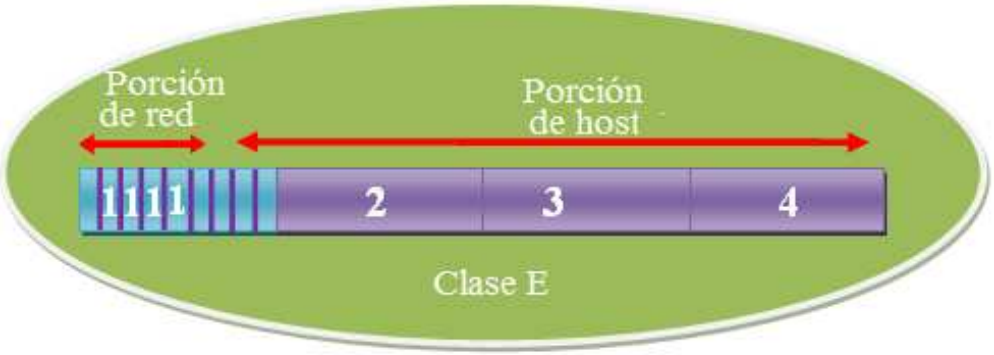

Figura 2.12.-Clase E.

La Figura muestra el rango de las direcciones IP del primer octeto tanto en decimales como en binarios para cada clase de dirección IP.

Tabla 2.5.-Intervalos de direcciones IP.

Clase de dirección IP	**Intervalo de dirección IP (Valor decimal)**
Clase A	1-126 (00000001-01111110)
Clase B	128-191 (10000000-10111111)
Clase C	192-223 (11000000-11011111)
Clase D	224-239 (11100000-11101111)
Clase E	240-255 (11110000-11111111)

2.3.3.-Direcciones reservadas.

Ciertas direcciones de host son reservadas y no pueden asignarse a dispositivos de la red. Estas direcciones de host reservadas incluyen:

• Dirección de red: Utilizada para identificar la red en sí.

En la Figura 2.13, la sección que está identificada en el casillero superior representa la red 198.150.11.0. Los datos enviados a cualquier host de dicha red (198.150.11.1- 198.150.11.254) se verá desde afuera de la red del área local con la dirección 198.150.11.0. Los números del host sólo tienen importancia cuando los datos se encuentran en una red de área local. La LAN contenida en el casillero inferior recibe el mismo tratamiento que la LAN superior, sólo que el número de la red es 198.150.12.0.

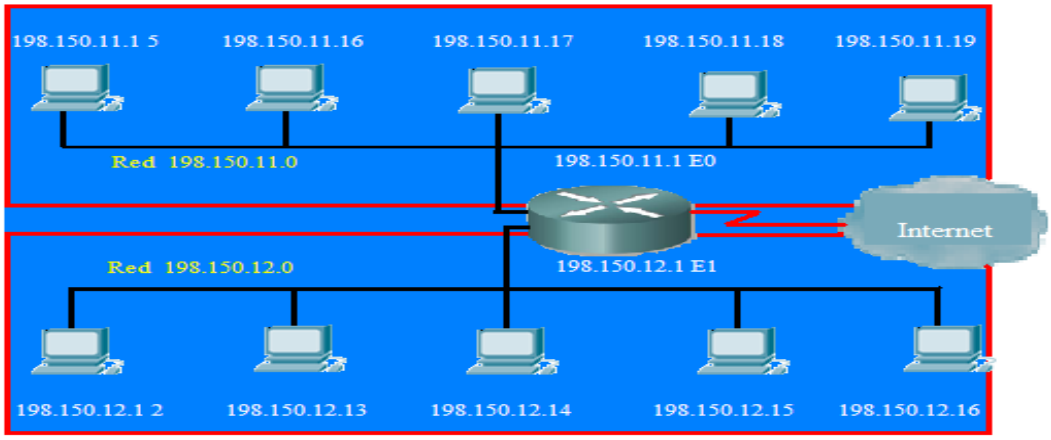

Figura 2.13.- Dirección de red.

• Dirección de broadcast: Utilizada para realizar el broadcast de paquetes hacia todos los dispositivos de una red.

En la figura 2.14, la sección que se identifica en el casillero superior representa la dirección de broadcast 198.150.11.255. Todos los hosts de la red leerán los datos enviados a la dirección de broadcast (198.150.11.1- 198.150.11.254). La LAN contenida en el casillero inferior recibe el mismo tratamiento que la LAN superior, sólo que la dirección de broadcast es 198.150.12.255.

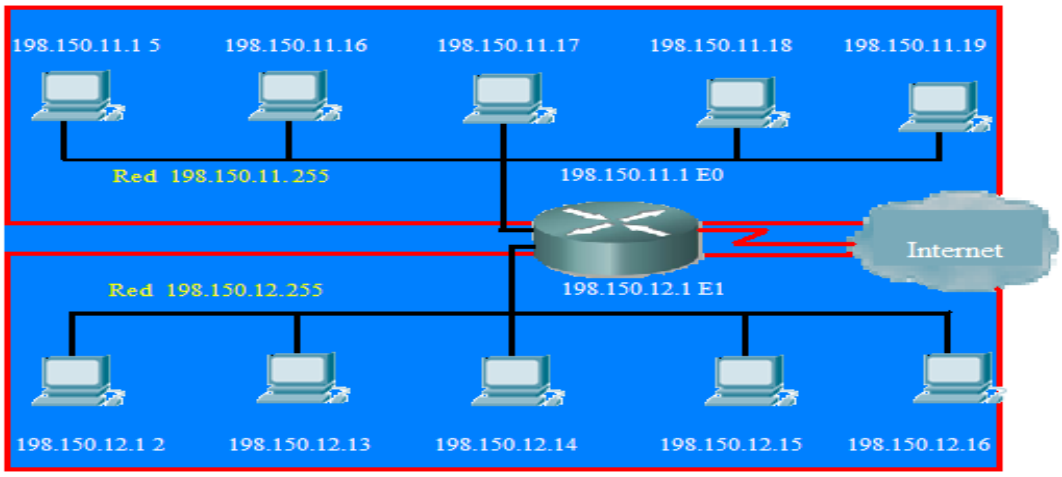

Figura 2.14.- Dirección de broadcast.

La dirección IP que tiene ceros binarios en todas las posiciones de bits de host queda reservada para la dirección de red. Tomando como ejemplo una red Clase A, 113.0.0.0 es la dirección IP de la red, conocida como el ID (identificador) de la red, que contiene el host 113.1.2.3. Un Router usa la dirección IP de red al enviar datos por Internet. En un ejemplo de red Clase B, la dirección 176.10.0.0 es una dirección de red, como muestra la Figura 2.15.

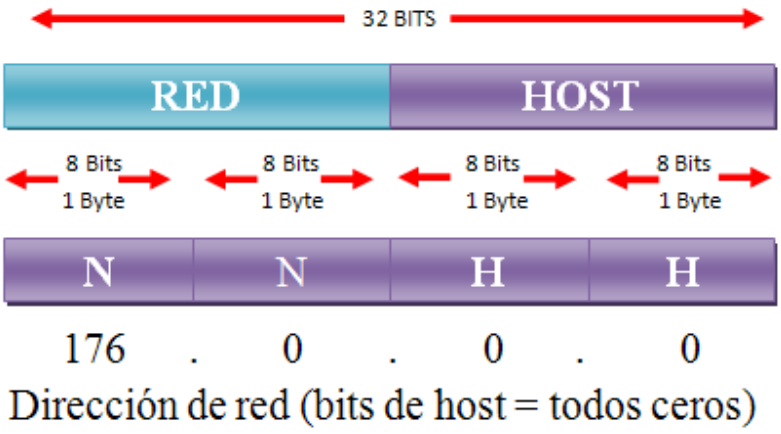

Figura 2.15.-Ejemplo de Dirección reservada de Clase B, la dirección 176.10.0.0

En una dirección de red Clase B, los primeros dos octetos se designan como porción de red. Los últimos dos octetos contienen ceros, dado que esos 16 bits corresponden a los números de host y se utilizan para identificar los dispositivos que están conectados a la red. La dirección IP, 176.10.0.0, es un ejemplo de una dirección de red. Esta dirección nunca se asigna como dirección de host. Una dirección de host para un dispositivo conectado a la red 176.10.0.0 podría ser 176.10.16.1. En este ejemplo, "176.10" es la parte de RED y "16.1" es la parte de host.

Para enviar información a todos los dispositivos de la red, se necesita una dirección de broadcast. Un broadcast se produce cuando una fuente envía datos a todos los dispositivos de una red. Para asegurar que todos los demás dispositivos de una red procesen el broadcast, el transmisor debe utilizar una dirección IP destino que ellos puedan reconocer y procesar. Las direcciones IP de broadcast terminan con unos binarios en toda la parte de la dirección que corresponde al host.

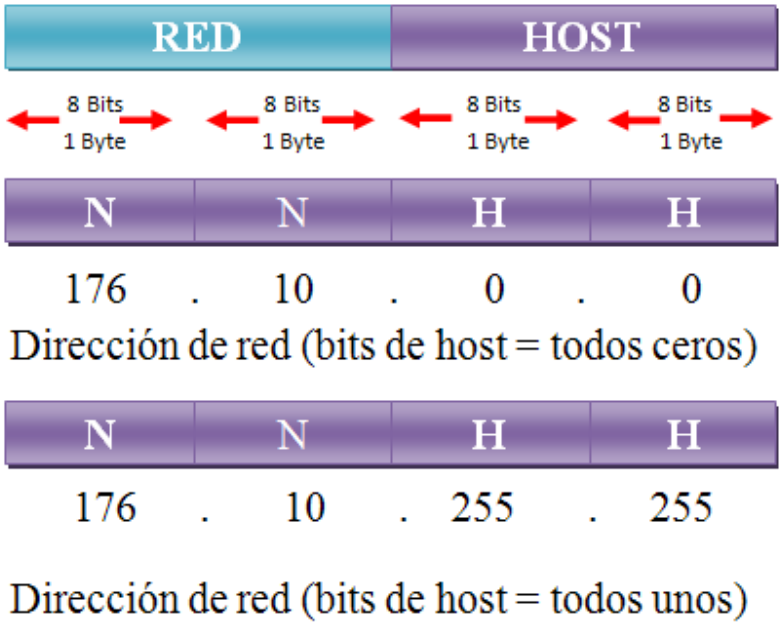

Figura 2.16.-Ejemplo de dirección de broadcast.

En el ejemplo de la red, 176.10.0.0, los últimos 16 bits componen el campo del host o la parte de la dirección del host. El broadcast que se envía a todos los dispositivos de la red incluye una dirección destino de 176.10.255.255. Esto se produce porque 255 es el valor decimal de un octeto que contiene 11111111.

2.3.4.-Direcciones públicas y privadas.

La estabilidad de la Internet depende de forma directa de la exclusividad de las direcciones de red utilizadas públicamente.

Las direcciones IP públicas son exclusivas. Dos máquinas que se conectan a una red pública nunca pueden tener la misma dirección IP porque las direcciones IP públicas son globales y están estandarizadas. Todas las máquinas que se conectan a la Internet acuerdan adaptarse al sistema. Hay que obtener las direcciones IP públicas de un proveedor de servicios de Internet (ISP) o un registro, a un costo.

Con el rápido crecimiento de Internet, las direcciones IP públicas comenzaron a escasear. Se desarrollaron nuevos esquemas de direccionamiento, tales como el enrutamiento entre dominios sin clase (CIDR) y el IPv6, para ayudar a resolver este problema. CIDR e IPv6 se tratan más adelante en este curso.

Las direcciones IP privadas son otra solución al problema del inminente agotamiento de las direcciones IP públicas. Como ya se ha mencionado, las redes públicas requieren que los hosts tengan direcciones IP únicas. Sin embargo, las redes privadas que no están conectadas a la Internet pueden utilizar cualquier dirección de host, siempre que cada host dentro de la red privada sea exclusivo. Existen muchas redes privadas junto con las redes públicas. Sin embargo, no es recomendable que una red privada utilice una dirección cualquiera debido a que, con el tiempo, dicha red podría conectarse a Internet. El RFC 1918 asigna tres bloques de la dirección IP para uso interno y privado. Estos tres bloques consisten en una dirección de Clase A, un rango de direcciones de Clase B y un rango de direcciones de Clase C. Las direcciones que se encuentran en estos rangos no se enrutan hacia el backbone de la Internet. Los Routers de Internet descartan inmediatamente las direcciones privadas. Si se produce un direccionamiento hacia una intranet que no es pública, un laboratorio de prueba o una red doméstica, es posible utilizar las direcciones privadas en lugar de direcciones exclusivas a nivel global. Las direcciones IP privadas pueden entremezclarse, como

muestra el gráfico, con las direcciones IP públicas. Así, se conservará el número de direcciones utilizadas para conexiones internas.

Tabla 2.6.-Intervalos de direcciones internas.

Clase de dirección IP	**Intervalo de internas RFC 1918**
Clase A	10.0.0.0 a 10.255.255.255
Clase B	172.16.0.0 a 172.31.255.255
Clase C	192.168.0.0 a 192.168.255.255

La conexión de una red que utiliza direcciones privadas a la Internet requiere que las direcciones privadas se conviertan a direcciones públicas. Este proceso de conversión se conoce como Traducción de direcciones de red (NAT). En general, un Router es el dispositivo que realiza la NAT.

Segmentación de la red

La división en subredes es otro método para administrar las direcciones IP. Este método, que consiste en dividir las clases de direcciones de red completas en partes de menor tamaño, ha evitado el completo agotamiento de las direcciones IP. Resulta imposible hablar sobre el TCP/IP sin mencionar la división en subredes. Como administrador de sistemas, es importante comprender que la división en subredes constituye un medio para dividir e identificar las redes individuales en toda la LAN. No siempre es necesario subdividir una red pequeña. Sin embargo, en el caso de redes grandes a muy grandes, la división en subredes es necesaria. Dividir una red en subredes significa utilizar una máscara de subred para dividir la red y convertir una gran red en segmentos más pequeños, más eficientes y administrables o subredes.

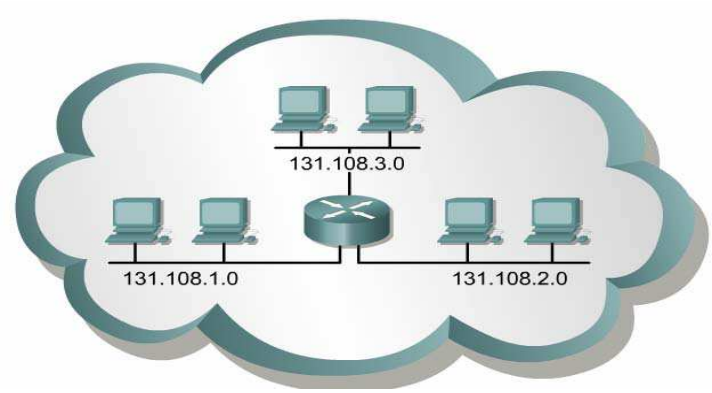

Figura 2.17.- Subredes.

El administrador del sistema debe resolver estos problemas al agregar y expandir la red. Es importante saber cuántas subredes o redes son necesarias y cuántos hosts se requerirán en cada red. Con la división en subredes, la red no está limitada a las máscaras de red por defecto Clase A, B o C y se da una mayor flexibilidad en el diseño de la red.

Las direcciones de subredes incluyen la porción de red más el campo de subred y el campo de host. El campo de subred y el campo de host se crean a partir de la porción de host original de la red entera. La capacidad para decidir cómo se divide la porción de host original en los nuevos campos de subred y de host ofrece flexibilidad en el direccionamiento al administrador de red.

Para crear una dirección de subred, un administrador de red pide prestados bits del campo de host y los designa como campo de subred. El número mínimo de bits que se puede pedir es dos. Al crear una subred, donde se solicita un sólo bit, el número de la red suele ser red .0. El número de broadcast entonces sería la red .255. El número máximo de bits que se puede pedir prestado puede ser cualquier número que deje por lo menos 2 bits restantes para el número de host.

Tabla 2.7.-Número de subredes por tipo de red.

Notación decimal del primer octeto de host	Número de subredes	Número de hosts de clase A por subred	Número de hosts de clase B por subredes	Número de hosts de clase C por subredes
.192	2	4,194,302	16,382	62
.224	6	2,097,150	8,190	30
.240	14	1,048,574	4,094	14
.248	30	524,286	2,046	6
.252	62	262,142	1,022	2
.254	126	131,070	510	-
.255	254	65,534	254	-

2.3.5.-IPv4 en comparación con IPv6.

Cuando se adoptó TCP/IP en los años 80, dependía de un esquema de direccionamiento de dos niveles. En ese entonces, esto ofrecía una escalabilidad adecuada. Desafortunadamente, los diseñadores de TCP/IP no pudieron predecir que, con el tiempo, su protocolo sostendría una red global de información, comercio y entretenimiento. Hace más de veinte años, la Versión 4 del IP (IPv4) ofrecía una estrategia de direccionamiento que, aunque resultó escalable durante algún tiempo, produjo una asignación poco eficiente de las direcciones.
Las direcciones Clase A y B forman un 75 por ciento del espacio de direccionamiento IPv4, sin embargo, se pueden asignar menos de 17 000 organizaciones a un número de red Clase A o B. Las direcciones de red Clase C son mucho más numerosas que las direcciones Clase A y B aunque ellas representan sólo el 12,5 por ciento de los cuatro mil millones de direcciones IP posibles.

Figura 2.18.-Porcentaje del espacio de direccionamiento IPv4.

Lamentablemente, las direcciones Clase C están limitadas a 254 hosts utilizables. Esto no satisface las necesidades de organizaciones más importantes que no pueden adquirir una dirección Clase A o B. Aún si hubiera más direcciones Clase A, B y C, muchas direcciones de red harían que los Routers se detengan debido a la carga del enorme tamaño de las tablas de enrutamiento, necesarias para guardar las rutas de acceso a cada una de las redes.

Ya en 1992, la Fuerza de tareas de ingeniería de Internet (IETF) identificó las dos dificultades siguientes:

• Agotamiento de las restantes direcciones de red IPv4 no asignadas. En ese entonces, el espacio de Clase B estaba a punto de agotarse.

• Se produjo un gran y rápido aumento en el tamaño de las tablas de enrutamiento de Internet a medida que las redes Clase C se conectaban en línea. La inundación resultante de nueva información en la red amenazaba la capacidad de los Routers de Internet para ejercer una efectiva administración.

Durante las últimas dos décadas, se desarrollaron numerosas extensiones al IPv4. Estas extensiones se diseñaron específicamente para mejorar la eficiencia con la cual es posible utilizar un espacio de direccionamiento de 32 bits. Dos de las más importantes son las

máscaras de subred y el enrutamiento entre dominios sin clase (CIDR), que se tratan con mayor detalle en lecciones posteriores

Mientras tanto, se ha definido y desarrollado una versión más extensible y escalable del IP, la Versión 6 del IP (IPv6). IPv6 utiliza 128 bits en lugar de los 32 bits que en la actualidad utiliza el IPv4. IPv6 utiliza números hexadecimales para representar los 128 bits. IPv6 proporciona 640 sextillones de direcciones. Esta versión del IP proporciona un número de direcciones suficientes para futuras necesidades de comunicación.

Esta versión de IP debe proporcionar suficientes direcciones para las necesidades de comunicación futuras.

La figura muestra las direcciones IPv4 e IPv6. Las direcciones de IPv4 miden 32 bits de longitud, se escriben con números decimales separados por puntos. Las direcciones IPv6 miden 128 bits y son identificadores de interfaces individuales y conjuntos de interfaces. Las direcciones IPv6 se asignan a interfaces, no a nodos. Como cada interface pertenece a un solo nodo, cualquiera de las direcciones unicast asignada a las interfaces del nodo se pueden usar como identificadores del nodo. Las direcciones IPv6 se escriben en hexadecimal, separados por comas. Los campos IPv6 tienen una longitud de 16 bits. Para que las direcciones sean más fáciles de leer, es posible omitir los ceros iníciales de cada campo. El campo: 0003: se escribe :3: La representación taquigráfica del IPv6 de los 128 bits utiliza números de 16 dígitos, que se muestran en forma de cuatro dígitos hexadecimales.

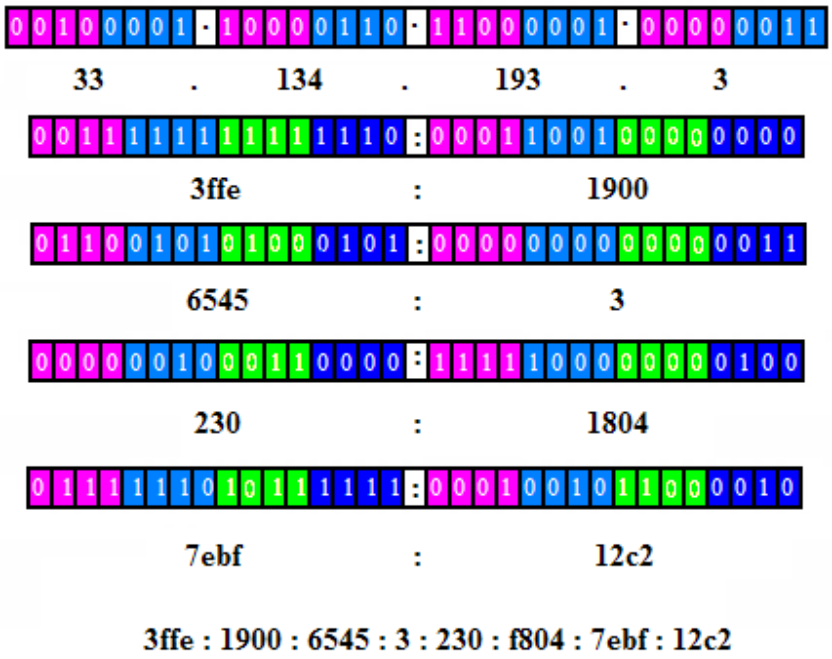

Figura 2.19.-Direccionamiento IPv6.

Después de diez años de planificación y desarrollo, el IPv6 lentamente comienza a implementarse en redes selectas. Con el tiempo, el IPv6 podrá reemplazar el IPv4 como el protocolo de Internet dominante.

2.3.6.-Asignación dinámica de direcciones IP.

Un host de red necesita obtener una dirección exclusiva a nivel global para poder funcionar en Internet. La dirección MAC o física que posee el host sólo tiene alcance local, para identificar el host dentro de la red del área local. Como es una dirección de Capa 2, el Router no la utiliza para realizar transmisiones fuera de la LAN.

Las direcciones IP son las direcciones que más frecuentemente se utilizan en las comunicaciones en la Internet. Este protocolo es un esquema de direccionamiento jerárquico que permite que las direcciones individuales se asocien en forma conjunta y sean tratadas como grupos. Estos grupos de direcciones posibilitan una eficiente transferencia de datos a través de la Internet.

Los administradores de redes utilizan dos métodos para asignar las direcciones IP. Estos métodos son el estático y el dinámico. Más adelante, en esta lección, se tratará el direccionamiento estático y las tres variantes del direccionamiento dinámico. Independientemente del esquema de direccionamiento elegido, no es posible tener dos interfaces con la misma dirección IP. Dos hosts con la misma dirección IP pueden generar conflictos que hacen que ambos no puedan operar correctamente. Como muestra la Figura 2.20, los hosts tienen una dirección física ya que cuentan con una tarjeta de interfaz de red que les permite conectarse al medio físico.

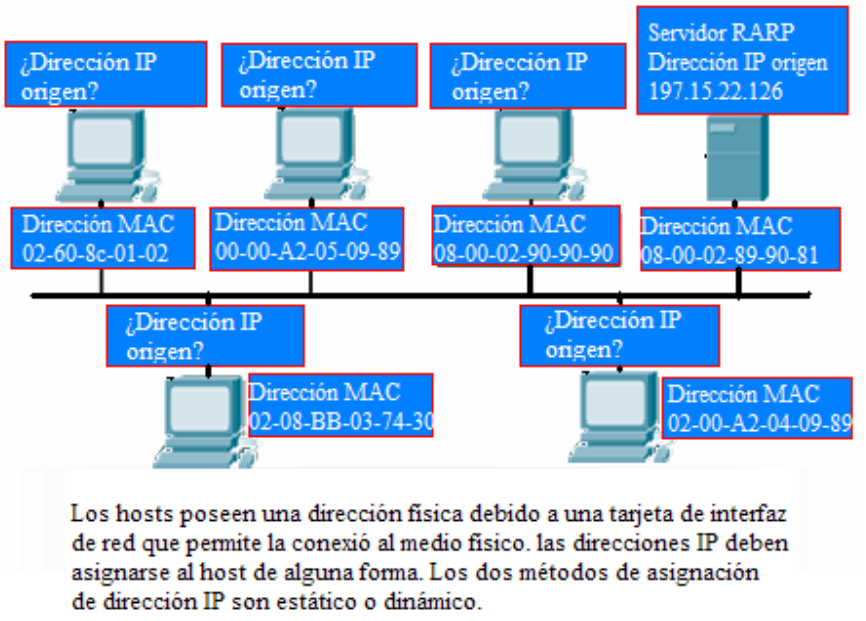

Figura 2.20.-Relacion de dirección IP con dirección MAC.

Asignación estática de una dirección IP.

La asignación estática funciona mejor en las redes pequeñas con poca frecuencia de cambios. De forma manual, el administrador del sistema asigna y rastrea las direcciones IP para cada computador, impresora o servidor de una red interna. Es fundamental llevar un buen registro para evitar que se produzcan problemas con las direcciones IP repetidas. Esto es posible sólo cuando hay una pequeña cantidad de dispositivos que rastrear.

Los servidores deben recibir una dirección IP estática de modo que las estaciones de trabajo y otros dispositivos siempre sepan cómo acceder a los servicios requeridos. Considere lo difícil que sería realizar una llamada telefónica a un lugar que cambiara de número todos los días.

2.4.-Protocolos TCP/IP.

TCP/IP es una familia de protocolos desarrollados para permitir la comunicación entre ordenadores de cualquier tipo de red o fabricante, respetando los protocolos de cada red individual.

Los protocolos TCP/IP se estructuran en 5 niveles funcionales:

Tabla 2.8.- Modelo TCP/IP.

TCP/IP
APLICACIÓN
TRANSORTE
INTERNET
RED
FISICO

- El nivel físico corresponde al hardware. Puede ser un cable coaxial, un cable par trenzado, cable de fibra óptica o una línea telefónica. TCP/IP no considera oficialmente el nivel físico como componente específico de su modelo y tiende a agrupar el nivel físico con el nivel de red. Los protocolos principales de este nivel son: ARP y RARP.

- El nivel de red. Independientemente del medio físico que se utilice, necesitará una tarjeta de red específica que, a su vez, dependerá de un software llamado controlador de dispositivo proporcionado por el sistema operativo o por el fabricante. Proporciona fiabilidad (aunque no necesariamente) en la distribución de

datos que pueden adoptar diferentes formatos. Aunque TCP/IP no especifica ningún protocolo para este nivel, los protocolos más notables son: SLIP, PPP Y PPTP.

- El nivel Internet se superpone a la red física creando un servicio de red virtual independiente de aquélla. No es fiable ni orientado a conexión. Se encarga del direccionamiento y encaminamiento de los datos hasta 12 estación receptora. El protocolo específico de este nivel es IP.

- El nivel de transporte suministra a las aplicaciones servicios de comunicaciones desde la estación emisora a la receptora. Utiliza dos tipos de protocolos: TCP que es fiable y orientado a conexión y UDP que es no fiable y no orientado a conexión.

- El nivel de aplicación corresponde a las aplicaciones disponibles para los usuarios como pueden ser: FTP, SNMP, TELNET, etc.

Estos niveles se corresponden con los niveles del modelo de referencia OSI de la siguiente manera:

Tabla 2.9.-Modelos TCP/IP y OSI.

TCP/IP
APLICACION
TRANSPORTE
INTERNET
RED
FISICO

OSI
APLICACIÓN
PRESENTACON
SESION
TRANSPORTE
RED
ENLACE DE DATOS
FISICO

Esta correspondencia es teórica porque, como los protocolos TCP/IP fueron desarrollados antes que el modelo de referencia OSI, existen sustanciales diferencias, como son:

- El concepto de jerarquía en relación a los niveles. Indica que una tarea de comunicaciones se divide en entidades que pueden comunicar con otras pares en otro sistema. Una entidad dentro de un sistema proporciona servicios a otras entidades y, a su vez, utiliza los servicios de otras. Éstas deben tener una relación jerárquica, de manera que una entidad sólo utilice los servicios de las jerárquicamente inferiores. La diferencia entre ambos modelos es consecuencia del pragmatismo con el que se desarrollaron los protocolos TCP/IP, ya que éstos proporcionan a los diseñadores mayor grado de libertad para la utilización de uno u otro; mientras que OSI es más prescriptivo, ya que dicta los protocolos de un nivel determinado que deben realizar unas funciones específicas.

- La interoperación de redes, ya que los protocolos TCP/IP se han concebido para interconectar sistemas no conectados a la misma red.

- La fiabilidad extremo a extremo. El protocolo IP no es fiable, es decir, no garantiza que los paquetes entregados sean correctos y que conserven la secuencia con que fueron emitidos, ya que supone que son los protocolos de transporte los que deben garantizarlo.

- Los servicios no orientados a conexión. El protocolo IP tampoco es orientado a conexión, ya que ésta debe proporcionarse en niveles superiores.

- La gestión de red. En los primeros documentos del modelo OSI no se contemplaban las funciones de gestión y, aunque actualmente ya se contemplan, no alcanzan el nivel de aceptación de los de TCP/IP.

2.5.-Protocolos del nivel físico (Nivel de Acceso a la Red).

Aunque TCP/IP no considera oficialmente el nivel físico como componente específico de su modelo y tiende a agrupar el nivel físico con el nivel de red, se van a describir en este apartado los protocolos ARP, RARP, SLIP, PPP Y PPTP.

2.5.1.-ARP.

ARP (Address Resolution Protocol) es un protocolo que se utiliza para convertir las direcciones IP en direcciones físicas que puedan ser utilizadas por los manejadores.
Para poder realizar esta conversión, existe en cada ordenador un módulo ARP que utiliza una tabla de direcciones ARP, que en la mayoría de los ordenadores trata como si fuera una memoria intermedia (caché), de forma que la información que lleva mucho tiempo sin utilizarse se borra.
Si encuentra la correspondencia entre la dirección 1P y la dirección física, se procede a la transmisión.
Si no la encuentra en la tabla, se genera una petición ARP que se difunde por toda la red. Si alguno de los ordenadores de la red reconoce su propia dirección 1P en la petición ARP, envía un mensaje de respuesta que indica su dirección física y se graba en la Tabla de Direcciones ARP.

2.5.2.-RARP.

RARP (Reverse Address Resolution Protocol) se utiliza cuando al producirse el arranque inicial, los ordenadores no conocen su dirección IP.
Requiere que exista en la red, al menos, un servidor RARP. Cuando un ordenador desea conocer su dirección IP envía un paquete que contiene su propia dirección física.
El servidor RARP, al recibir el paquete, busca en su tabla RARP la dirección IP correspondiente a la dirección física inicial indicada en el paquete y envía un paquete al ordenador origen con dicha información.
A diferencia del protocolo ARP que se incorpora normalmente en todos los productos TCP/IP, el protocolo RARP sólo se incorpora en unos pocos productos.

2.5.3.-SLIP.

SLIP (Serial-Line Internet Protocol) es un protocolo antiguo desarrollado para el entorno UNIX. Opera sin control de errores, control de flujo o seguridad, pero consigue un buen rendimiento con pequeños bloques de datos.

2.5.4.-PPP.

PPP (Point-to-Point Protocol) es un protocolo SLIP mejorado con control y recuperación de errores.
A diferencia de SLIP, que sólo puede ser usado con TCP/IP, los enlaces PPP pueden ser compartidos simultáneamente por diferentes protocolos, incluido IPX

2.5.5.-PPTP.

Aunque PPTP (point to Point Tunneling Protocol) no es un protocolo propio de TCP/IP, se va a describir en esta sección, ya que es un nuevo protocolo de red incorporado en Windows NT, que utiliza redes privadas multiprotocolo para permitir a los usuarios remotos tener acceso de forma segura, a través de Internet, a redes de empresas (Extranet).
Ofrece las siguientes ventajas:

- Costos de transmisión más bajos. Ya que usa Internet para la conexión en lugar de una llamada normal a través de la línea telefónica.
- Menores costos de hardware. Ya que permite separar los módems y las tarjetas RDSI, así como colocarse en un servidor de comunicaciones.
- Mayor nivel de seguridad. Funciona con cifrado de datos y actúa con cualquier protocolo.

Los datos enviados con PPTP se encapsulan en paquetes PPP cifrados que se envían a través de Internet. Pero también, puede ser usado para transportar el tráfico de acceso remoto IPX y NetBEUI.

2.6.-Protocolos de nivel de internet

En este nivel se encuentran los protocolos ICMP e IP.

2.6.1.-ICMP.

ICMP (Internet Control Message Protocol) es un protocolo de mantenimiento y gestión de red que ayuda a supervisar la red.
Se utiliza para poder encontrar una ruta a través de la cual los datagramas viajen por la red y alcancen su destino.

El objetivo principal de ICMP es proporcionar la información de error o control entre nodos. La implementación de ICMP es obligatoria como un subconjunto lógico del protocolo IP.

Los mensajes de error de este protocolo normalmente los genera y los procesa TCP/IP y no el usuario.

Existen cuatro tipos de mensajes ICMP:

- Mensajes de destino no alcanzable.
- Mensajes de control de congestión.
- Mensajes de redireccionamiento.
- Mensajes de tiempo excedido.

Una de las utilidades de diagnóstico que utiliza este protocolo es PING (se utiliza para comprobar si un ordenador está conectado a la red).

2.6.2.-IP

IP (Internet Protocol) se encarga de seleccionar la trayectoria a seguir por los datagramas, es decir, por dónde se deben encaminar los datagramas salientes, puede llevar a cabo tareas de fragmentación y reensamblado.

Este protocolo, que no es fiable ni está orientado a conexión, no garantiza el control de flujo, la recuperación de errores ni que los datos lleguen a su destino.

IP no se encarga de controlar que sus datagramas, que envía a través de la red, puedan perderse, llegar desordenados o duplicados. Para ello, estas opciones tendrán que ser contempladas por protocolos del nivel de transporte.

Los datagramas IP contienen una cabecera con información para el nivel IP y datos. Estos datagramas se encapsulan en tramas que, dependiendo de la red física utilizada, tienen una longitud determinada.

Cuando los datagramas viajan de unos equipos a otros pueden atravesar diferentes tipos de redes. El tamaño máximo de estos paquetes puede variar de una red a otra dependiendo del medio físico que se emplee para su transmisión. A este tamaño máximo se le denomina MTU (Unidad Máxima de Transmisión) y ninguna red puede transmitir ningún paquete cuya longitud exceda el MTU de dicha red.

Debido a este problema, es necesario reconvertir los datagramas IP en el formato requerido

por cada una de las redes que va atravesando. Esto es lo que se denomina fragmentación y reensamblado.

La fragmentación divide los paquetes en fragmentos de menor longitud (se realiza en el nivel más inferior posible y de forma transparente al resto de niveles) y el reensamblado realiza la operación contraria.

2.7.-Protocolos de nivel de transporte.

En este nivel se encuentran los protocolos TCP y UDP.

2.7.1.-TCP.

TCP (Transmission Control Protocol) es un protocolo orientado a conexión que utiliza los servicios del nivel Internet.

Al igual que cualquier protocolo orientado a conexión consta de tres fases:

- Establecimiento de la conexión. Se inicia con el intercambio de tres mensajes, garantiza que los dos extremos de la transmisión estén preparados para la transferencia de datos y permite que ambos acuerden los números iníciales de secuencia (cada extremo elige un número de forma aleatoria).
- Transferencia de los datos. La unidad de datos que utiliza es el segmento y su longitud se mide en octetos. La transmisión es fiable ya que permite la recuperación ante datos perdidos, erróneos o duplicados, además garantiza la secuencia de entrega, para lo que se añade a la cabecera del segmento de datos un número de secuencia y un código de control. La fiabilidad de la recepción se consigue mediante la confirmación de la recepción, los temporizadores de espera de confirmación y la retransmisión de segmentos.
- Liberación de la conexión. Cuando una aplicación comunica que no tiene más datos que transmitir, TCP finaliza la conexión en una dirección. Desde ese momento, TCP no vuelve a enviar datos en ese sentido, y permite que los datos circulen en el sentido contrario hasta que el emisor cierra también esa conexión.

TCP permite multiplexación, es decir, una conexión TCP puede ser utilizada simultáneamente por varios usuarios.

Como normalmente existe más de un proceso de usuario o aplicación que utiliza TCP de

forma simultánea, es necesario identificar los datos asociados a cada proceso. Para ello, se emplean los puertos. Un puerto es una palabra de 16 bits que identifica hacia qué aplicación o proceso han de dirigirse los datos.

Hay aplicaciones que tienen asignado el mismo número de puerto, ya que realizan funciones de servidores normalizados que utilizan los servicios TCP/IP. Estos puertos reservados se encuentran en el archivo SERVICES que está en el directorio ETC y corresponden a números superiores al que se debe especificar si corresponden al protocolo TCP o UDP.

Un socket está compuesto por un par de números que identifican de manera única a cada aplicación. Cada socket se compone de dos campos:

- La dirección IP del ordenador en el que se está ejecutando la aplicación.
- El puerto a través del cual la aplicación se comunica con TCP/IP.

2.7.2.-UDP.

UDP (User Datagram Protocol/Protocolo de datagramas de usuario) es un protocolo que se basa en el intercambio de datagramas. UDP permite el envío a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera.

El inconveniente de esta forma de actuación es que no hay confirmación de recepción ni de haber recibido los datagramas en el orden adecuado, debe ser la aplicación la que se encargue de controlado.

Al igual que el protocolo TCP, utiliza puertos y sockets y, también, permite la multiplexación.

2.8.-Protocolos del nivel de aplicación

Todas las aplicaciones TCP/IP utilizan el modelo cliente/servidor.

En este nivel se encuentran un buen número de protocolos, de los cuales se van a describir los siguientes: FTP, HTTP, NFS, NTP, RPC, SMTP, SNMP, TELNET y TFTP.

2.8.1.-FTP.

FTP (File Transfer Protocol/Protocolo de transferencia de archivos) es el más utilizado de todos los protocolos de aplicación y uno de los más antiguos.

Se utiliza para la transferencia de archivos y proporciona acceso interactivo, especificaciones de formato y control de autentificación (aunque es posible conectarse como el usuario anónimo que no necesita contraseña).

2.8.2.-HTTP.

HTTP (Hyper Text Transfer Protocol/Protocolo de transferencia de hipertexto) es uno de los protocolos más recientes. Se utiliza para manejar la consulta de hipertexto y el acceso de datos con World Wide Web (WWW). El tráfico generado por este protocolo ha pasado, debido a la influencia de Internet, a ser muy grande.

2.8.3.-NFS.

NFS (Network File System/Sistema de archivos de red) ha sido desarrollado por Sun Microsystems Incorporated y autoriza a los usuarios el acceso en línea a archivos que se encuentran en sistemas remotos (accede a un archivo remoto como si se tratara de un archivo local). La mayoría del tráfico NFS es ahora un caso especial del protocolo RPG.

2.8.4.-NTP.

NTP (Network Time Protocol/ Protocolo de tiempo de red) permite que todos los sistemas sincronicen su hora con un sistema designado como servidor horario.

2.8.5.-RPC.

RPC (Remote Procedure Call/Llamada remota) es una llamada a un procedimiento que se ejecuta en un sistema diferente del que realiza la llamada.

El proceso cliente envía un mensaje al proceso servidor y espera una respuesta. Este, al recibir la llamada, estudia los procedimientos del proceso llamado, obtiene los resultados y los envía de vuelta al proceso cliente mediante un mensaje de respuesta.

Existen dos tipos de servidores:

- El servidor interactivo que recibe una llamada proporciona el servicio y vuelve al

estado de espera.

- El servidor concurrente que recibe la llamada contesta al mensaje enviando al cliente un número de puerta, arranca un proceso paralelo para prestar el servicio requerido por el cliente y vuelve al estado de espera. Cuando el proceso paralelo haya finalizado el servicio requerido, acaba su ejecución.

2.8.6.-SMTP.

SMTP (Simple Mail Transfer Protocol/Protocolo sencillo de transferencia de correo electrónico) es un protocolo de correo electrónico. Especifica el formato exacto de los mensajes que un cliente debe enviar desde un ordenador al servidor de otro, pero no especifica cómo debe almacenarse el correo ni con qué frecuencia se debe intentar el envío de los mensajes.

2.8.7.-SNMP.

SNMP (Simple Network Management Protocol/Protocolo sencillo de gestión de red) sirve para administrar los sistemas de forma remota. También se puede utilizar para supervisar el tráfico de la red desde una o varias estaciones de trabajo llamadas administradores SNMP.
Los elementos de la red que puede administrar y monitorizar son dispositivos como ordenadores, puertas de enlace (gateways), encaminadores (routers), mainframes, miniordenadores, hubs, etc.
SNMP minimiza el número y la complejidad de las funciones realizadas por el administrador y cuenta con las siguientes ventajas:

- Reduce el costo de desarrollo del software del agente de administración necesario para soportar este protocolo.
- Aumenta el grado de las funciones de administración utilizadas de forma remota, permitiendo un uso completo de los recursos de Internet en dichas tareas.
- Permite que las funciones de administración sean de fácil comprensión y uso por parte de los desarrolladores de herramientas de administración de la red.

Utiliza una arquitectura distribuida que consiste en agentes y sistemas de administración.

- Un agente es un ordenador que ejecuta el software de agente SNMP o un encaminador.

  La obligación principal de un agente es ejecutar las tareas iniciadas por los comandos SNMP que han sido requeridas por un sistema de administración.

  Los comandos SNMP que se utilizan pertenecen a los tipos siguientes:
- GetRequest: Éste es el comando que usa el sistema de administración para solicitar información a un agente.
- GetNextRequest: También es empleado por el sistema de administración para solicitar información al agente y se utiliza si la información deseada se encuentra en forma de tabla o matriz (se usa de forma repetitiva hasta que se hayan conseguido todos los datos de la matriz).
- GetResponse: El agente consultado utiliza este comando para contestar una solicitud hecha por el sistema de administración.
- SetRequest: El sistema de administración lo utiliza para cambiar el valor de un parámetro del MIB (Management Information Base).
- Trap: Este comando lo utiliza un agente para informar al sistema de administración de un suceso determinado que se ha producido.
- Un sistema de administración es un ordenador que ejecuta un software de administración SNMP. Puede iniciar las operaciones de los comandos GetRequest, GetNextRequest y SetRequest.

Un agente únicamente puede iniciar el comando Trap para informar al sistema de administración de un suceso extraordinario y contestar al sistema de administración con el comando GetResponse.

La forma en que actúa el protocolo SNMP es la siguiente:

1. El sistema de administración envía primero una solicitud al agente para obtener el valor de una variable del MIB.
2. El agente contesta a la solicitud en función del nombre de la comunidad que acompaña a la solicitud.

Una comunidad comprende un grupo de ordenadores que ejecutan el servicio SNMP. El uso de un nombre de comunidad proporciona una seguridad mínima para los agentes que reciben solicitudes e inician capturas (traps) así como para las tareas iniciadas por los

sistemas de administración.

Un agente no responderá a una solicitud de un sistema de administración distinto de aquéllos que tenga configurados (un agente puede pertenecer a varias comunidades a la vez).

El MIB describe los objetos que están incluidos en la base de datos de un agente SNMP.

Los objetos que haya en un MIB deben estar definidos para que los desarrolladores de software para la administración de las estaciones de trabajo los conozcan, así como sus valores respectivos.

Un MIB registra y almacena información sobre el ordenador en el que se está ejecutando. Un administrador SNMP puede solicitar y recoger información de un agente MIB así como revisar o alterar los objetos que contiene.

2.8.8.-TELNET.

TELNET permite que un usuario desde un terminal acceda a los recursos y aplicaciones de otros ordenadores.

Una vez que la conexión queda establecida, actúa de intermediario entre ambos ordenadores.

Se fundamenta en tres principios:

- El concepto de terminal virtual de red (NVT). Corresponde a la definición de cómo han de ser los datos, caracteres de control y las secuencias de los mandatos que han de circular por la red para permitir una heterogeneidad de los sistemas.
- La simetría entre terminales y procesos. La comunicación puede ocurrir entre dos terminales, dos procesos o entre un terminal y un proceso.
- Permite que el cliente y el servidor negocien sus opciones. La conexión comienza con una fase de negociación de opciones en la que se utilizan cuatro mandatos: *WILL, WONT, DO* y *DONT*.

  WILL se envía para mostrar el deseo de comenzar una opción (que se ha de indicar) y se contesta con *DO* (respuesta positiva) o *DONT* (respuesta negativa).

  WONT se envía para mostrar el deseo de no comenzar una opción (que se ha de indicar) y se contesta con *DONT* (mostrando el acuerdo de no utilización).

  DO se envía para indicar que comience a utilizar una opción (que se ha de

indicar) y se contesta con *WILL* (respuesta positiva) o *WONT* (respuesta negativa).

DONT se envía para indicar que no comience a utilizar una opción (que se ha de indicar) y se contesta con *WONT* (mostrando el acuerdo de no utilización).

2.8.9.-TFTP.

TFTP (Trivial File Transfer Protocol/Protocolo de transferencia de archivos trivial) es un protocolo destinado a la transferencia de archivos aunque sin permitir tanta interacción entre cliente y servidor como la que existe en FTP. Además, existe otra diferencia, en lugar de utilizar el protocolo TCP, utiliza UDP.

Sus reglas son muy sencillas. En el envío del primer paquete se establece una interacción entre el cliente y el servidor. Se empieza una numeración de los bloques (iniciando desde 1). Cada paquete de datos contiene una cabecera que especifica el bloque que contiene. Un bloque de menos de 512 bytes indica que es el último y corresponde al final del archivo.

2.9.- Seguridad de TCP/IP.

La seguridad es una preocupación importante siempre que se conecta una red al exterior.

El software básico de TCP/IP no cifra los datos por sí mismo, debe realizarlo la aplicación. Si no se cifran los datos, la contraseña se enviará en texto ASCII y podrá ser leída fácilmente durante el trayecto por personas que disponga de medios y conocimientos. Es importante que los datos (sobre todo la contraseña) vayan cifrados para evitar que sean examinados por personas ajenas.

Otra opción es mantener alejadas del sistema a todas aquellas personas ajenas. Para ello, lo mejor es instalar un cortafuegos (firewall). Su función es filtrar los intentos de establecimiento de conexión de forma que se pueda detectar e impedir el acceso al sistema a posibles intrusos sin que ni siquiera se haya llegado a establecer un enlace directo entre ellos.

El cortafuegos puede ser configurado para permitir que sólo determinadas direcciones, origen y destino, puedan acceder a su red (o desde ella).

Las funciones de cortafuegos se pueden realizar por:

- Ordenadores dedicados exclusivamente al filtrado de paquetes (servidor proxy).
- Encaminadores de red (routers) configurados para esta tarea.
- Programas de software para distintos sistemas operativos.
- Cualquier otro dispositivo intercalado entre la red y el exterior que soporte el filtrado de paquetes según unos parámetros previamente definidos.

  Entre los posibles beneficios de utilizar cortafuegos se encuentran:
- Acceso controlado a la red.
- Protección para servicios de Internet que sean vulnerables.
- Administración de seguridad centralizada.
- Estadísticas de las conexiones a la red. Filtrado sofisticado de paquetes. Los filtros de paquetes controlan qué tipos de paquetes IP pueden acceder a los servicios de la red interna. Así, puede denegar paquetes, bloquear paquetes de un ordenador determinado de Internet, rechazar direcciones fantasmas, evitar ataques FRAG (un ataque FRAG se produce cuando se provoca un fallo en el algoritmo de reensamblado de los paquetes IP que se reciben debido al envío de fragmentos de paquetes trucados) o evitar ataques SYN (un ataque SYN se produce cuando se inunda un servidor con requerimientos de conexiones falsas que evitan el procesamiento de requerimientos verdaderos).
- Configuración desde un sistema de hardware independiente que no dependa de ningún otro sistema de hardware y software.

  Entre las posibles razones para no utilizar un cortafuegos se encuentran:
- El acceso a los servicios deseados puede llegar a ser más complejo de lo normal.
- El peligro de acceso por una puerta trasera a la red se incrementa si no se tiene prevista su inuti1ización.
- Es necesario una administración suplementaria de la red.
- El costo económico es mayor.
-

La configuración se hace demasiado compleja para realizarla de forma adecuada.

2.10.-Los comandos TCP/IP.

Tabla 2.10.- Comandos TCP/IP.

Comandos	Descripción
Arp	Muestra o modifica entradas en la caché ARP que contiene una o varias tablas utilizadas para almacenar la traducción de las direcciones IP a direcciones físicas Ethernet o Token Ring.
Finger	Muestra información sobre un usuario conectado a un equipo que está ejecutando el servicio Finger. En Windows Server 2003 no se proporciona el servicio Finger.
Ftp	Transfiere archivos entre una estación de trabajo y un servidor FTP, y viceversa (pueden ejecutar sistemas operativos distintos).
Hostname	Indica el nombre del equipo actual.
Ipconfig	Muestra todos los valores actuales de la configuración TCP/IP. Es especialmente útil en los sistemas que ejecutan DHCP ya que permite averiguar las direcciones IP que se han adjudicado.
Lpq	Muestra el estado de la cola de impresión indicada en un equipo que ejecuta el dominio LPD
Lpr	Envía un archivo a una impresora de un equipo que ejecute el dominio LPD
Nbtstat	Muestra las estadísticas de protocolo y las conexiones TCP/IP actuales que utilizan NBT (NetBIOS sobre TCP/IP).
Netstat	Muestra las estadísticas de protocolo y las conexiones actuales de la red TCP/IP.
Slookup	Muestra información de los servidores de nombres DNS.
Ping	Envía una llamada a un equipo remoto e informa si se puede establecer conexión o no con él. También muestra determinadas estadísticas sobre el estado de la conexión establecida.

Rcp	Realiza una copia de archivos entre equipos Windows Server 2003 y un sistema que ejecute un shell remoto.
Tftp	Transfiere archivos entre un equipo local y un equipo remoto que está ejecutando el servicio TFTP sin necesidad de autentificación del usuario.
Tracert	Determina el camino tomado hacia un destino y envía paquetes del protocolo ICMP con valores variables de Tiempo de duración (TTL) para el destino. Cada enrutador disminuirá TTL al menos en una unidad antes de reenviardo. Cuando TTL llegue a cero, el enrutador devolverá al sistema de origen un mensaje de tiempo excedido

Capítulo 3.- Conceptos previos antes de construir una Intranet.

3.1.-Necesidades para montar una intranet.

Para montar una Intranet es necesario contar con una red local instalada.

En dicha red local deberá haber un servidor con una capacidad de proceso y almacenamiento suficiente, así como también estaciones de trabajo desde las que se pueda acceder al servidor.

El servidor deberá contar con un sistema operativo de red con utilidades que permitan crear y administrar un sitio Web, proporcione servicios de seguridad y administración e incorpore el protocolo TCP/IP (para el ejemplo que se va a desarrollar en el libro, se va a utilizar una red local con un servidor que dispone de un procesador Pentium II a 350 Mhz, con 128 MB de RAM, 10 GB de espacio en disco y cuenta con el sistema operativo Windows 2000 Server con el protocolo TCP/IP correctamente instalado).

Las estaciones de trabajo pueden utilizar el sistema operativo Windows 95/98, Windows NT Workstation o Windows 2000 Professional (en todos los casos, ha de estar instalado correctamente el protocolo TCP/IP en cada estación de trabajo).

3.2.-Directorio Activo.

El Directorio Activo es la implementación para Windows de los Servicios de Directorio. Su objetivo fundamental es ampliar las funciones del sistema de dominios para facilitar la gestión y administración de las redes.

Su estructura se basa en los siguientes conceptos:

- Dominio. Es la estructura fundamental. Permite agrupar todos los objetos que se administrarán de forma estructurada y jerárquica.
- Unidad organizativa. Es una unidad jerárquica inferior del dominio que puede estar compuesta por una serie de objetos y por otras unidades organizativas.
- Grupos. Son conjuntos de objetos del mismo tipo y se utilizan fundamentalmente para la asignación de derechos de acceso a los recursos.
- Objetos. En una representación de un recurso de red (usuarios, ordenadores, impresoras, etc.).

Entre sus características principales se encuentran:

- Al crear un nuevo dominio en un árbol ya existente, las relaciones de confianza que se establecen de forma automática son transitivas y bidireccionales con los demás dominios.

• Multidominio. Permite que un servidor albergue más de un dominio.

- Réplica multimaestro. Permite que una modificación que se realice en el directorio de cualquier servidor se replique automáticamente a los restantes servidores del dominio.
- Soporte de herencia. Permite que cualquier cambio en los derechos de acceso se propague automáticamente a todos los niveles inferiores.
- Administración de privilegios flexible. Con ello se puede asignar de forma más precisa los privilegios, ya que permite dar derechos de administración sobre un subconjunto determinado de objetos en lugar de sobre la totalidad.

Hay tres categorías de datos que pueden replicarse entre los dominios:

• Datos del dominio. Contiene datos de los objetos del dominio.

• Datos de configuración. Describen la topología del directorio.

- Datos del esquema. Es la definición de todos los objetos y sus atributos que pueden ser almacenados en el directorio.
- Control de acceso del usuario a recursos entre dominios o bosques.

  Se puede bloquear el acceso de usuarios de un dominio o bosque a recursos de otros dominios o bosques, y, después, permitir un acceso selectivo al establecer

la entrada de control de acceso (ACE) Permitir autenticación en un recurso local del objeto de usuario o grupo.

3.3.-Las unidades organizativas.

Las unidades organizativas son contenedores del Directorio Activo en los que se pueden colocar usuarios, grupos, equipos y otras unidades organizativas (una unidad organizativa no puede contener objetos de otros dominios).

Es el ámbito o unidad más pequeña a la que se puede asignar configuraciones de Directiva de grupo y en la que se puede delegar el control administrativo (otras posibilidades para ambas cosas son los sitios y los dominios). Con las unidades organizativas, se pueden crear contenedores dentro de un dominio que representen las estructuras lógicas y jerárquicas existentes dentro de una organización (de esta manera, se puede administrar la configuración y el uso de cuentas y recursos en función de un modelo organizativo determinado).

Utilizando las unidades organizativas se pueden ver más fácilmente los objetos del directorio de un dominio y simplificar su administración. El control administrativo de cada unidad organizativa se puede delegar en personas específicas (asi se podrán distribuir las tareas administrativas del dominio entre varios administradores, de forma que sus responsabilidades coincidan en la mayor medida posible con las que tienen asignadas en la organización).

Las unidades organizativas no son principios de seguridad y por tanto no tienen miembros. Su único propósito consiste en organizar y contener objetos del directorio (para conceder derechos y permisos a los usuarios, se ha de realizar a través de los grupos, pero se pueden utilizar las unidades organizativas para contener a los objetos grupo y asignarles configuraciones de Directiva de grupo). .

Cada dominio puede implementar su propia jerarquía de unidades organizativas. Si la organización tiene varios dominios, se pueden crear estructuras de unidades organizativas totalmente independientes en cada uno de ellos.

Si se necesita decidir la división de una parte determinada de la red en dominios y unidades organizativas, se han de tener en cuenta las siguientes recomendaciones:

- Si se trata de una organización descentralizada en la que los distintos usuarios y

recursos son administrados por grupos totalmente diferentes de administradores, es conveniente dividir la red en dominios independientes.

- Si dos partes de la misma red estén separadas por un vínculo lento que hace prácticamente imposible que el tráfico de una replicación completa pueda atravesarlo, es conveniente dividir la red en dominios independientes.
- Si se necesita reflejar la estructura de la organización, es recomendable dividir el dominio en unidades organizativas en lugar de crear dominios independientes.
- Si se desea delegar el control administrativo en pequeños conjuntos de usuarios, grupos y recursos, es conveniente dividir el dominio en unidades organizativas (dicho control administrativo puede ser completo, como la capacidad de crear usuarios y cambiar contraseñas, o limitado, como el mantenimiento de las colas de impresión).
- Si la estructura de esa parte específica de la organización puede sufrir modificaciones en el futuro, es conveniente dividir el dominio en unidades organizativas.

Al crear unidades organizativas en los dominios, se establecen dos tipos de jerarquías en el árbol del dominio:

- La jerarquía de los dominios en un árbol de dominio.
- La jerarquía de las unidades organizativas en el dominio.

Esta doble jerarquía permite una mayor flexibilidad en la administración de los árboles de dominio. Por ejemplo, si una organización dispone de una red administrada por un grupo central de administradores, se pueden crear unidades organizativas que contengan las cuentas y recursos de cada uno de sus dominios (cada dominio puede tener una unidad organizativa de administradores que contenga las cuentas de usuario de los administradores de ese dominio). El grupo central de administradores puede delegar el control administrativo a cada una de dichas unidades organizativas, al mismo tiempo que conserva el control administrativo global sobre ellas.

3.3.1.- Cómo trabajar con las unidades organizativas.

Para trabajar con las unidades organizativas en un dominio se utilizan usuarios y equipos

de Active Directory desde Herramientas administrativas del menú Inicio.

3.4.-Bosques y árboles de dominio.

Cuando varios dominios comparten un esquema y un catálogo global comunes se forma un bosque. Si varios dominios cuentan con nombres de dominio DNS contiguos, se les denomina árbol de dominios.

3.4.1.-Arboles de dominio.

El primer dominio de un árbol de dominio se denomina dominio raíz. Los dominios adicionales del mismo árbol son dominios secundarios. Un dominio que se encuentra inmediatamente encima de otro dominio del mismo árbol se denomina dominio principal del dominio secundario.

Todos los dominios que comparten el mismo dominio raíz forman un árbol de dominio y constituyen un espacio de nombres contiguo, es decir, el nombre de un dominio secundario consta del nombre de dicho dominio secundario más el nombre el dominio principal (por ejemplo principal.empresa.com es un dominio secundario de empresa.com que a su vez es el dominio principal de principal.empresa.com; el dominio empresa.com es el dominio principal de principal.empresa.com que además es el dominio raíz de este árbol de dominio).

Los dominios de Windows Server 2003 que forman parte de un árbol están unidos entre sí mediante relaciones de confianza transitivas y bidireccionales. Dado que estas relaciones de confianza son bidirecciona1es y transitivas, un dominio recién creado en un bosque o árbol de dominio tiene establecidas inmediatamente relaciones de confianza con todos los demás dominios existentes en dicho bosque o árbol de dominio. Estas relaciones de confianza permiten que un único proceso de inicio de sesión sirva para autenticar a un usuario en todos los dominios del bosque o del árbol de dominio.

3.4.2.- Bosques.

Un bosque está formado por uno o varios árboles de dominio. Los árboles de dominio de un bosque no constituyen un espacio de nombres contiguo. Por ejemplo, aunque dos árboles de dominio (empresa.com y empresal.com) pueden tener ambos dominio secundario denominado contabilidad, los nombres DNS de esos dominios secundarios

serán contabilidad.empresa.com y contabilidad.empresal.com.

Sin embargo, un bosque no tiene ningún dominio raíz propiamente dicho. El dominio raíz del bosque es el primer dominio que se creó en el bosque. Los dominios raíz de todos los árboles de dominio del bosque establecen relaciones de "confianza transitivas con el dominio raíz del bosque.

Todos los dominios de todos los árboles de dominio de un bosque comparten las siguientes características:

- Relaciones de confianza transitivas entre los dominios.
- Relaciones de confianza transitivas entre los árboles de dominio.
- Un esquema común.
- Información de configuración común.
- Un catálogo global común.

Al utilizar bosques y árboles de dominio se obtiene la flexibilidad que ofrecen los sistemas de espacios de nombres contiguos y no contiguos (puede ser útil en el caso de organizaciones que tienen divisiones independientes que necesitan conservar sus propios nombres DNS).

3.4.3.-Relaciones de confianza.

En los equipos que ejecutan Windows Server 2003, la autentificación de las cuentas entre dominios es posible realizarla gracias a las relaciones de confianza bidireccionales y transitivas basadas en el protocolo de seguridad Kerberos V5; en caso de que un equipo implicado en una transacción no admita Kerberos V5, se utilizará el protocolo NTLM NT LAN Manager.

Las relaciones de confianza se crean automáticamente entre dominios adyacentes (dominio principal y sus secundarios) cuando se crea un dominio en un árbol de dominios.

En un bosque, se crea automáticamente una relación de confianza entre el dominio raíz del bosque y el dominio raíz de cada árbol de dominio que se agrega al bosque (como dichas relaciones de confianza son transitivas, los usuarios y equipos podrán autentificarse en cualquier dominio del bosque o del árbol de dominios).

3.4.4.- Confianza entre dominios.

Una confianza entre dominios es una relación que se establece entre los dominios y que permite a los usuarios de un dominio ser autentificados por un controlador de dominio de otro dominio.

Las solicitudes de autenticación siguen una ruta de confianza que es la serie de relaciones de confianza que deben seguir las solicitudes de autentificación entre los dominios. Para que un usuario pueda tener acceso a un recurso de otro dominio, el sistema de seguridad de los controladores de dominio debe determinar -si el dominio de confianza o confianza de salida (el dominio donde inicia la sesión el usuario) tiene una relación de confianza con el dominio que confía o confianza de entrada (el dominio que contiene el recurso al que el usuario intenta obtener acceso). Para determinarlo, el sistema de seguridad calcula la ruta de confianza entre un controlador del dominio que confía y un controlador del dominio de confianza.

Una relación de confianza entre dominios puede ser:

- Unidireccional.
- Bidireccional.
- Transitiva.
- Intransitiva.

3.4.4.1.- Confianza unidireccional

Una confianza unidireccional es una ruta de autenticación unidireccional creada entre dos dominios. De esta manera, si existe una confianza unidireccional entre dos dominios A y B, los usuarios del dominio A pueden tener acceso a los recursos del dominio B, pero los usuarios del dominio B no pueden tener acceso a los recursos del dominio A.

Las relaciones unidireccionales pueden ser transitivas o intransitivas dependiendo del tipo de confianza que se desea crear.

Las solicitudes de autentificación en una relación de confianza unidireccional intransitiva sólo se pueden transmitir desde el dominio que confía al dominio en el que se confía. Esto significa que si el dominio A tiene una confianza unidireccional intransitiva con el dominio B y éste la tiene con el dominio C, el dominio A no tiene una relación de confianza con el dominio C.

Sin embargo, las solicitudes de autentificación en una relación de confianza unidireccional transitiva se pueden extender más allá de los dos dominios en los que se Ó. Esto significa que si el dominio A tiene una confianza unidireccional transitiva con el dominio B y éste la tiene con el dominio C, el dominio A tiene una relación de confianza con el dominio C.

Un dominio de Windows Server 2003 establece una confianza unidireccional

- Los dominios de Windows Server 2003 de un bosque diferente.
- Los dominios de Windows NT 4.0.
- Los territorios de Kerberos V5.

Aunque, si se establecen confianzas unidireccionales en los dos sentidos entre dominios y territorios indicados, se dispone de una confianza bidireccional.

3.4.4.2.- Confianza bidireccional.

En una relación de confianza bidireccional entre dos dominios A y B, los usuarios del dominio A pueden tener acceso a los recursos del dominio B y, así mismo, los usuarios del dominio B pueden tener acceso a los recursos del dominio A. De esta manera, las solicitudes de autentificación entre los dos dominios se pueden realizar en ambas direcciones.

Cuando se crea un nuevo dominio secundario, automáticamente se crea una confianza bidireccional entre el nuevo dominio secundario y el dominio principal.

De forma predeterminada, todos los dominios de Windows Server 2003 pertenecientes a un mismo bosque están vinculados mediante una confianza bidireccional transitiva.

3.4.4.3.- Confianza transitiva.

Todas las confianzas entre los dominios de un bosque de Windows Server 2003 son

transitivas. Es decir, la confianza entre dominios de la relación se puede extender más allá de los dos dominios en los que se formó. Esto significa que si el dominio A tiene una confianza transitiva con el dominio B y éste la tiene con el dominio C, el dominio A tiene una relación de confianza con el dominio C.

Cuando se crea un nuevo dominio secundario, automáticamente se crea una relación de confianza transitiva bidireccional entre el dominio principal y el nuevo dominio secundario. De esta forma, las relaciones de confianza transitivas fluyen hacia arriba a través del árbol de dominios a medida que éste se forma, con lo que se crean relaciones de confianza transitivas entre todos los dominios del árbol.

Cuando se crea un árbol de dominios en un bosque, se crea una relación de confianza transitiva bidireccional entre el dominio raíz del bosque y el nuevo dominio (la raíz del nuevo árbol de dominios). Si no se agrega ningún dominio secundario al dominio nuevo, la ruta de confianza estará entre este nuevo dominio raíz y el dominio raíz del bosque. Si se agregan dominios secundarios al dominio nuevo, la confianza fluye hacia arriba a través del árbol de dominios hasta el dominio raíz del árbol de dominios y, de este modo, se extiende la ruta de confianza inicial creada entre la raíz del dominio y el dominio raíz del bosque.

Si el nuevo dominio agregado al bosque es un único dominio raíz (es decir, no tiene dominios secundarios) o un árbol de dominios, la ruta de confianza se extiende desde el nuevo dominio raíz hasta cualquier otro dominio raíz del bosque. De esta forma, las relaciones de confianza transitivas fluyen a través de todos los dominios del bosque.

Las solicitudes de autenticación siguen estas rutas de confianza y, de esta manera, las cuentas de cualquier dominio del bosque se pueden autentificar en cualquier otro (es decir, con un único proceso de inicio de sesión, las cuentas que poseen los permisos adecuados pueden tener acceso a los recursos en cualquier dominio del bosque).

Igualmente, se pueden crear de forma manual relaciones de confianza transitivas entre los dominios de Windows Server 2003 del mismo árbol o bosque de dominios. Estas relaciones de confianza de acceso directo se pueden utilizar para acortar la ruta de confianza entre árboles o bosques de dominios grandes y complejos.

3.4.4.4.- Confianza intransitiva.

Una confianza intransitiva está limitada por los dos dominios de la relación y no fluye a cualquier otro dominio del bosque (de forma predeterminada, las confianzas intransitivas son unidireccionales, aunque también se puede crear una relación unidireccional si se crean dos unidireccionales).

En la mayor parte de los casos, se debe crear las confianzas intransitivas igualmente (para ello, se deben crear dos confianzas unidireccionales entre los dominios implicados).

Debido a la necesidad de flujos de confianza, no es posible tener relaciones intransitivas entre dominios del mismo bosque de Windows Server 2003.

3.5.- Los Sitios.

Un sitio es un conjunto de subredes (cada subred dispone de su propio identificador de red único dentro de su dirección IP) correctamente conectadas. Es conveniente que las redes de área extensa (WAN) empleen múltiples sitios, ya que si no lo hacen así, la atención de las solicitudes o la replicación de información del directorio pueden ser muy poco eficientes.

3.5.1.-Cómo se relacionan los sitios con los dominios.

En el Directorio Activo, los sitios representan la estructura física (topología) de la red mientras que los dominios representan la estructura lógica de la organización.

La estructura lógica y la estructura física son independientes la una de la otra, por ello:

- No es necesaria ninguna correlación entre la estructura física de la red y su estructura de dominios.
- Es posible que haya múltiples dominios en un único sitio, así como múltiples sitios en un único dominio.
- No es necesaria ninguna conexión entre los espacios de nombres de sitios y de dominios.

El Directorio Activo utiliza la información de topología, almacenada como objetos de sitio y vínculos de sitio en el directorio, para crear la topología de replicación mejor y más eficaz.

3.5.2.- ¿Cómo se utilizan los sitios?

Los sitios facilitan diversas operaciones:

- Autenticación. Cuando un cliente inicia una sesión en un dominio, en primer lugar se dirige a un controlador de dominio del mismo sitio para autenticarse (de esta manera, se reduce el tráfico en las conexiones WAN).
- Replicación. Los sitios optimizan la replicación de información del directorio. La información de configuración y del esquema del directorio se distribuye por todo el bosque y los datos del dominio se distribuyen entre todos los controladores de dominio. La información del directorio se replica dentro de un sitio con mayor frecuencia que con los demás sitios (de esta forma, los controladores de dominio que con más probabilidad necesitarán información especial del directorio, son los que primero reciben las replicaciones). Los controladores de dominio de otros sitios reciben todos los cambios efectuados en el directorio, pero con menor frecuencia, con lo que se reduce el consumo de ancho de banda de red.

La pertenencia a un sitio se determina de manera diferente para los controladores de dominio y para los clientes.

Un cliente determina en qué sitio está cuando se conecta, ya que obtiene su dirección IP y su máscara de subred del servidor DHCP (de modo que la ubicación de su sitio se actualiza dinámicamente).

La ubicación de un controlador de dominio se establece por el sitio al que pertenece en el directorio (ya que obtiene su dirección IP y su máscara de subred de forma estática y, por tanto, no se modificará a no ser que se desplace a un sitio distinto).

Si un controlador de dominio o un cliente tiene una dirección que no este incluida en ningún sitio, el cliente o el controlador de dominio estará contenido dentro del sitio inicial creado (Default-First-Site, Nombre-predeterminado-primer-sitio Toda la actividad se controla, entonces, como si la actividad del cliente o del controlador de dominio fuera un miembro del Default-First-Site (sin tener en cuenta la dirección IP o la ubicación de la subred real). Por tanto, todos los sitios siempre tendrán un controlador de dominio asociado, ya que el controlador de dominio mas próximo se asocia a sí mismo a un sitio

que no tenga ningún controlador de dominio (amenos que se elimine Default-First-Site).

3.6.-Configuración y gestión del servidor.

La responsabilidad de configurar y gestionar el servidor de la red corresponde al administrador.

Una vez instalado el sistema operativo, se ha de proceder a la configuración la red, que incluye los siguientes pasos:

- Desarrollar la estructura de directorios.
- Copiar los programas de aplicaciones y los datos.
- Dar de alta a los usuarios y grupos.
- Establecer la administración de seguridad.
- Localización de problemas.
- Establecer la seguridad del servidor.

3.7.-El desarrollo de la estructura de directorios.

Sin duda, se puede emplear un número ilimitado de estructuras de directorios en un servidor y se debe estudiar cuidadosamente la que mejor se adapta a las necesidades de cada empresa.

Cuando se planea la disposición de los directorios, se deben considerar tres circunstancias importantes:

- La simplicidad de la estructura. No se debe hacer que la estructura de directorios sea tan complicada que los usuarios no puedan encontrar los programas ni los archivos de datos.
- La seguridad. Muchas de las previsiones de seguridad de un sistema operativo de red son relativas a los directorios y subdirectorios.
- La lógica. Los archivos deben estar agrupados lógicamente para aumentar la eficiencia de la red.

3.7.1.- Los usuarios.

Las cuentas de usuario representan a una persona y se denominan principales de seguridad

dentro del Directorio Activo, ya que son objetos del directorio a los que se asignan automáticamente identificadores de seguridad para iniciar sesiones en la red y tener acceso a los recursos.

Una cuenta de usuario permite que un usuario inicie sesiones en equipos y dominios con una identidad que se puede autentificar y autorizar para tener acceso a los recursos del dominio. Cada usuario que se conecta a la red debe tener su propia cuenta de usuario y su propia contraseña única. Por tanto, una cuenta de usuario se utiliza para:

- Autentificar la identidad del usuario.
- Autorizar o denegar el acceso a los recursos del dominio.
- Administrar otros principales de seguridad.
- Auditar las acciones realizadas con la cuenta de usuario.

En Windows Server 2003, los usuarios pueden ser de dos tipos:

- Usuarios globales. Estas cuentas se crean en equipos controladores de dominio y pueden usarse para conectarse a los dominios en que están creadas y a otros dominios en los que se confía.
- Usuarios locales. Estas cuentas se crean en equipos que no sean controladores de dominio y, por tanto, no pueden usarse para conectarse a ningún dominio.

Windows Server 2003 proporciona dos cuentas de usuario predefinidas que se crean en el proceso de la instalación y pueden usarse para iniciar una sesión y tener acceso a los recursos (además, crea otra cuenta local para los servicios de ayuda y soporte técnico remoto denominada SUPPORT_388945AO que está deshabilitada por defecto y que, posteriormente, desaparece cuando se instala el Directorio Activo). Estas cuentas son:

La cuenta de usuario del Administrador le permite administrar el equipo en el que se creó. Esta cuenta puede ser renombrada o deshabilitada pero no puede ser borrada ni quitada del grupo local de Administradores. Es importante renombrar y proteger esta cuenta con una contraseña especial, así como crear otras cuentas de administradores para proteger mejor la seguridad del servidor. Todos los administradores son miembros de los grupos siguientes: grupo local de Administradores, grupo global de Administradores del dominio, grupo global de Administradores de organización, grupo global de Administradores de esquema, grupo global de Propietarios del creador de directivas de grupo y grupo global de Usuarios del dominio (ver apartado siguiente para tener información de estos grupos).

La cuenta de usuario del Invitado. Normalmente, esta cuenta está deshabilitada (y debería permanecer de esta manera) pero puede habilitarse si se desea que alguien pueda conectarse al equipo o dominio con ella (tenga en cuenta que no precisa ninguna contraseña). Esta cuenta puede borrarse y renombrarse. Todos los invitados son miembros de los siguientes grupos: grupo local de Invitados y grupo global de Invitados de dominio (ver apartado siguiente para tener información de estos grupos).

3.7.2.- Perfil de usuario.

Un perfil de usuario es una de las herramientas más potentes de Windows Server 2003 para configurar el entorno de trabajo de los usuarios de red.

Se puede especificar el aspecto del escritorio, la barra de tareas, el contenido del menú Inicio, etc. (incluidos programas o aplicaciones).

Cada usuario puede tener un perfil que está asociado a su nombre de usuario y que se guarda en la estación de trabajo (aquellos usuarios que acceden a varias estaciones pueden tener un perfil en cada una de ellas). Este perfil se denomina perfil local porque sólo es accesible desde la estación en que está creado.

Los usuarios que se conectan a un servidor Windows Server 2003 pueden tener también perfiles en dicho servidor. De esta manera, se puede acceder al perfil independientemente de la estación en que se esté conectado. Este perfil se denomina perfil de red porque se puede acceder a él desde cualquier estación de la red.

Hay dos tipos de perfiles de red:

- Perfil móvil. Este tipo de perfil es asignado a cada usuario por los administradores pero puede ser modificado por el usuario y los cambios permanecen después de finalizar la conexión.
- Perfil obligatorio. Este tipo de perfil es igual que el perfil móvil pero asegura que los usuarios trabajen en un entorno común. Por tanto, puede ser modificado por el usuario pero los cambios realizados se pierden al finalizar la conexión. Sólo puede ser modificado (y guardados sus cambios) por los administradores.

Además, existe un perfil temporal que se crea cuando se produce un error en la carga del perfil del usuario (se elimina al final de la sesión y no se almacenan los cambios realizados por el usuario en la configuración del escritorio y los archivos).

Todos los perfiles locales se guardan por defecto en \Documents and settings\<nombre de usuario> (únicamente en el caso de una actualización desde Windows NT, los archivos se guardarían en IPROFILES\<nombre de usuario». En dicha ubicación se encuentran los subdirectorios de los usuarios que se crearon en el momento de la instalación (además de los que se hayan creado posteriormente) que son: Administrador, All Users y Default User.

- El perfil del Administrador es el que corresponde a dicho usuario.
- El perfil de All Users contiene las entradas que se incluirán en los perfiles de todos los usuarios del presente equipo e incluyen los iconos del escritorio y programas del menú Inicio, comunes a todos los usuarios.
- El perfil de Default User es el que corresponde a todo usuario que se conecta por vez primera o que no tenga asignado un perfil específico para él.

En cada uno de los perfiles puede haber las siguientes carpetas:

- Configuración local. Almacena los archivos de datos de programas, historial y archivos temporales.
- Cookies. Almacena información sobre las preferencias del usuario.
- Datos de programa. Almacena los datos específicos de los programas.
- Entorno de red. Guarda los accesos directos a elementos de Mis sitios de red.
- Escritorio. Guarda los elementos que aparecen en el escritorio del usuario incluidos archivos, carpetas y accesos directos.
- Favoritos. Guarda los accesos directos a las ubicaciones favoritas de Internet.
- Impresoras. Guarda los accesos directos a los elementos de la carpeta Impresoras.
- Menú Inicio. Guarda los accesos directos de los programas.
- Mis documentos. Guarda los documentos y subcarpetas del usuario.
- Recent. Guarda los accesos directos a los documentos y carpetas usados recientemente.
- SendTo. Guarda los accesos directos a las utilidades de control de los documentos.

- Templates. Contiene los accesos directos a las plantillas del usuario.

En Windows Server 2003, las carpetas Configuración local, Datos de programa, Entorno de red, Impresoras, Recent, SendTo y Templates aunque son ocultas se muestran por defecto. En Windows 2000 y XP, no se ven a no ser que se indique expresamente, marcando Mostrar todos los archivos y carpetas ocultos de la ficha Ver de Opciones de carpeta del menú Herramientas.

Así mismo, pueden tener hasta tres archivos llamados: ntuser.dat (contiene los datos del registro del usuario), ntuser.dat.LOG (que es un archivo donde se guardan los cambios realizados en el registro del usuario hasta que son guardados en el disco) y ntuser.man (contiene los datos del registro del usuario pero es un archivo de sólo lectura y, por tanto, no se guardarán los cambios realizados por el usuario en él).

Para asignar un perfil de usuario, una secuencia de comandos de inicio de sesión o un sub directorio particular para la cuenta del usuario, está la ficha Perfil de la pantalla de Propiedades de cada usuario (tanto si son usuarios locales como globales).

3.7.3.- Los perfiles móviles.

Como ya se indicó anteriormente, estos perfiles son asignados a cada usuario, pueden ser modificados por ellos mismos y los cambios permanecen después de finalizar la conexión.

Para ello, se guardan los datos del Registro del usuario en un archivo llamado ntuser.dat (dentro de un sub directorio con su nombre que se encuentra en la carpeta \Documents and Settings, a no ser que sea una actualización de Windows NT). Cuando el usuario se conecta, este archivo se copia a la categoría HKEY_CURRENT_USER del Registro (ver apartado correspondiente). Cuando el usuario realice cambios en su perfil, éstos se guardarán en el archivo NTuser.DAT al finalizar su conexión (de esa manera los cambios permanecerán para la próxima vez que inicie una sesión).

También, cuenta con el archivo ntuser.dat.LOG, que es un archivo donde se guardan los cambios realizados en el registro del usuario hasta que son guardados en el disco.

3.7.4.- Perfiles obligatorios.

Como ya se indicó anteriormente, este tipo de perfiles tienen la misma estructura que los

perfiles móviles, pero asegura que los usuarios trabajen en uno común. Por tanto los usuarios pueden modificarlos pero los cambios realizados se pierden al finalizar la conexión (los cambios sólo se guardan cuando se realizan por los administradores).

Para ello, se guardan los datos del Registro del usuario en un archivo llamado er.man (dentro de un sub directorio con su nombre que se encuentra en la carpeta documents and Settings, a no ser que sea una actualización de Windows NT). Cuando el usuario se conecta, este archivo se copia a la categoría HKEY _ CURRENT _ USER registro (ver apartado correspondiente). Cuando el usuario realice cambios en su perfil, éstos no se guardarán en el archivo al finalizar su conexión (de esa manera los cambios realizados no permanecerán para la próxima vez que inicie una sesión).

3.7.5.- La ruta de acceso local.

Indica el directorio local privado de cada usuario, donde puede almacenar sus archivos y programas. Así mismo, es el directorio predeterminado que se utilizará en el Símbolo del sistema y en todas las aplicaciones que no tienen definido un directorio de trabajo.

Facilita la tarea de hacer copias de seguridad de los archivos de cada usuario y su eliminación cuando se quite la cuenta de dicho usuario.

Deberá crearlo antes de especificar su ruta y su utilización es incompatible con Conectar.

3.7.6.-Conectar a una unidad de red.

Indica la letra deseada que estará conectada al directorio de red (compartido) privado de cada usuario, donde puede almacenar sus archivos y programas, así mismo, es el directorio predeterminado que se utilizará en el Símbolo del sistema y en todas las aplicaciones que no tienen definido un directorio de trabajo.

Facilita la tarea de hacer copias de seguridad de los archivos de cada usuario y su eliminación cuando se quite la cuenta de dicho usuario.

Deberá crearlo antes de especificar su ruta y su utilización es incompatible con Ruta de acceso local.

3.7.7.- Los grupos.

Las cuentas de grupo representan a un grupo y se denominan principales de seguridad dentro del Directorio Activo, ya que son objetos del directorio a los que se asigna automáticamente identificador de seguridad. En Windows Server 2003 se pueden dar dos tipos de grupos:

- Los grupos de seguridad. Este tipo de grupos se muestran en las listas de control de acceso discrecional (DACL) que es el lugar donde están definidos los permisos sobre los recursos y los objetos. Los grupos de seguridad se utilizan para asignar derechos y permisos y también como entidades de correo electrónico; de esta manera al enviar un mensaje de correo electrónico al grupo, el mensaje se envía a todos los miembros del grupo.
- Los grupos de distribución. En este tipo de grupos no es posible habilitar la seguridad ya que no aparecen en las listas de control de acceso discrecional (DACL). Los grupos de distribución sólo se pueden utilizar con aplicaciones de correo electrónico (como Microsoft Exchange) para enviar correo electrónico a los grupos de usuarios para asignar derechos y permisos.

Un grupo de seguridad puede convertirse en grupo de distribución (y viceversa) en cualquier momento si todos los controladores del dominio se actualizan a Windows Server 2003 y el administrador ha habilitado funcionamiento en modo nativo (si esto no es así, estarán en modo mixto y podrá realizar esta conversión).

Cada grupo de seguridad o de distribución tiene un ámbito que identifica el alcance de aplicación del grupo. Existen cuatro tipos de grupos en función de su ámbito de aplicación:

- Grupos de ámbito universal, o grupos universales. Este tipo de grupos (que únicamente pueden crearse en servidores que tengan instalado el Directorio Activo y que se encuentren en modo nativo) puede tener de miembros a otros grupos universales, grupos globales y cuentas de cualquier dominio y se le puede conceder permisos en cualquier dominio.
- Grupos de ámbito global, o grupos globales. Este tipo de grupos (solo puede crearse en servidores que tengan instalado el Directorio Activo) pueden tener como miembros a grupos globales y cuentas únicamente del dominio en el que

se ha definido el grupo y se le pueden conceder permisos en cualquier dominio.

- Grupos de ámbito local de dominio, grupos de dominio local o integrado local. Este tipo de grupos (que únicamente puede crearse en servidores que tengan instalado el Directorio Activo) pueden tener como miembros a grupos universales, grupos globales, grupos locales de dominio de su propio dominio y cuentas de cualquier dominio y sólo se puede utilizar para conceder permisos en el dominio que contiene el grupo.
- Grupos locales. Este tipo de grupos únicamente puede crearse en equipo que no tienen instalado el Directorio Activo. Puede tener como miembro a cuentas locales del equipo en el que se crean y si el equipo forma parte de un dominio podrá tener también cuentas y grupos del propio dominio y de los dominios de confianza y se puede utilizar para conceder permisos en el equipo en el que se crea el grupo.

3.8.- La seguridad del servidor.

Dentro del concepto de seguridad del servidor se pueden distinguir dos apartados:

- La seguridad física.
- La seguridad de los datos.

3.8.1.- La seguridad física del servidor.

El lugar donde esté colocado el servidor es sumamente importante para su estabilidad. El servidor necesita estar protegido contra distintos factores externos que pueden alterar el funcionamiento de la red.

Estos factores externos son: la electricidad estática, el calor, los ruidos eléctricos, los altibajos de tensión y los cortes de corriente.

La protección contra la electricidad estática y el calor:

Se han de tomar algunas precauciones para proteger al servidor de las cargas estáticas ya que el rendimiento de éste afecta a toda la red.

Entre las precauciones que se han de tomar está la de tratar regularmente las alfombras y maquetas con productos antiestáticos, utilizar fundas protectoras para ambas e instalar el servidor sobre una superficie conectada a una toma de tierra.

No utilizar plásticos ni material sintético ya que generan electricidad estática.

El calor y el frío excesivos son riesgos potenciales para el buen funcionamiento del servidor. Se ha de mantener la temperatura de la habitación del servidor entre 18° y 26° y asegurar una buena ventilación.

La protección contra los ruidos eléctricos, los altibajos de tensión y los cortes de corriente:

Los ruidos eléctricos son causados por las inconsistencias del suministro de la corriente del ordenador. Para proteger al servidor contra los ruidos eléctricos, puede recurrirse a la instalación de una línea dedicada de suministro eléctrico.

No hay que conectar otros dispositivos a este suministro de corriente, porque pueden generar ruidos que anulen las ventajas de la protección ofrecida por la fuente de corriente dedicada.

La conexión a la fuente de energía se ha de hacer con cable estándar de tres hilos, con el hilo de masa conectado a tierra.

Debe prevenirse contra los altibajos de tensión y contra el corte de la corriente. Para esto, lo mejor es completar la instalación con un Sistema de Alimentación Ininterrumpida o SAI (UPS, Uninterrumpible Power Suply). El SAI permite al servidor continuar activo durante cierto tiempo ante un eventual corte de la corriente.

Puede también tomarse la precaución de instalar un SAI en cada una de las estaciones que trabajen con aplicaciones críticas para protegerse de los daños producidos por la pérdida de datos durante un corte de energía.

La suciedad:

Aquí interviene tanto la suciedad de la sala donde se encuentra el servidor como la suciedad que pueden generar los propios usuarios.

Hay que mantener la sala en un estado de perfecta limpieza para evitar que el polvo pueda concentrarse dentro del servidor y altere su correcto funcionamiento.

Referente a los usuarios y administradores se ha de tener en cuenta que cualquier vertido de líquidos o de restos de alimentos sobre la pantalla y el teclado del servidor pueden producir distintos daños potenciales en el servidor. También, se ha de tener precaución con la ceniza

de los cigarros tanto dentro del teclado como en la pantalla y la CPU porque pueden producir daños importantes.

La seguridad contra incendios y agua:

De qué vale tener bien protegido el servidor si no se cuenta con una buena protección contra incendios. En la sala donde se encuentre instalado el servidor debe haber detectores de humo de alta sensibilidad y un sistema contra incendios a base de gas halón a presión. Este sistema debe producir un aviso previo a su utilización porque provoca el apagado del incendio de forma inmediata por consumo del oxígeno de la sala y, por tanto, todas las personas deberán salir de dicha sala porque podrían correr riesgo de asfixia.

También deberá estar protegido el servidor contra peligros de inundaciones y goteras que podrían provocar cortocircuitos eléctricos.

La protección contra robo y destrucción:

Es muy importante que en la sala donde se encuentra el servidor haya una protección efectiva que imposibilite tanto el robo del equipo o de alguno de sus componentes como la posibilidad de algún atentado que provoque la destrucción de todo o de alguna parte importante del servidor (tanto a nivel de hardware como de software).

La sala deberá estar protegida con sistemas antirrobo (tanto a nivel de las puertas como de las ventanas), las puertas que conducen a la sala deberán permanecer cerradas y se deberá identificar a cualquier persona que tenga acceso al servidor.

La información y el software han de estar guardados en otras habitaciones cerradas y los disquetes se han de encontrar cerrados con llave en los cajones de los archivos o de las mesas.

3.8.2.- La seguridad de los datos.

Es importante que los datos que están ubicados en el servidor de la red se encuentren bien protegidos. Para ello hay que considerar tres apartados:

- La seguridad del almacenamiento en el disco duro.
- La configuración de seguridad.
- La copia de seguridad de los datos.

3.8.2.1.- La seguridad del almacenamiento en el disco duro.

La unidad básica de almacenamiento de la información es el disco duro. Su capacidad está en constante incremento (desde 40 GB en adelante).

La forma más común de organizar el almacenamiento de la información es a través de un único disco duro (cuenta con la ventaja de la simplicidad de su configuración) aunque, dependiendo del tamaño de la empresa, se debe considerar la posibilidad de trabajar con más de un disco duro asociado.

Cada disco duro del sistema tiene asignado un número (comienza en el cero) y se asignan de forma diferente en función del tipo de disco:

- SCSI. En una controladora primaria de este tipo, los números van del cero al seis en el caso de SCSI-lo SCSI-2, y del cero al catorce en el caso del SCSI-3 de 16 bits (aunque todas poseen otra dirección que suele estar reservada para el adaptador del bus). Además, pueden tener varios canales por lo que, en caso de tener 4 canales pueden llegar a tener hasta sesenta dispositivos.
- IDE, EIDE Y ESDI. En una controladora primaria de estos tipos, los números van del cero al uno. Cuando esta controladora se completa puede recurrirse a una segunda controladora (lo que permitiría disponer hasta de un total de cuatro discos).

Todos los discos duros deben estar formateados a bajo nivel para poderse utilizar con Windows Server 2003.

3.8.2.2.- Particiones.

En un disco básico, la partición hace que un disco duro (o una parte de él) pueda ser utilizado como medio de almacenamiento.

Son la manera en que se divide el disco físico de forma que cada una de ellas funcionan como si fueran unidades separadas.

Las particiones pueden ser de dos tipos:

- Particiones primarias que son reconocidas por la BIOS del ordenador como capaces de iniciar el sistema operativo desde ellas. Para ello, disponen de un sector de arranque (BOOT SECTOR) que es el que se encarga de cargar el sistema operativo y una de las particiones primarias debe estar declarada como activa.

- Particiones secundarias que se forman en las áreas del disco duro (que no tienen particiones primarias) y que están contiguas.

  Las particiones extendidas deben estar configuradas en unidades lógicas para poderse utilizar para almacenar información

El número de particiones que se puede crear en un disco básico depende del estilo de partición del disco que es el método que Windows XP Professional y Windows Server 2003 utilizan para organizar las particiones del disco. Todos los equipos basados en los procesadores x86 utilizan el estilo de partición conocido como Registro de Inicio Maestro (MBR). MBR contiene una tabla de particiones que indica el lugar del disco donde se encuentran las particiones (como MBR es el único estilo de partición disponible para los equipos x86, no es necesario elegirlo, se aplicará automáticamente). En los discos con MBR se pueden crear hasta cuatro particiones primarias por disco o, bien, hasta tres particiones primarias y una partición extendida.

Los equipos basados en el procesador Itanium, como la versión de 64 bits de Windows Server 2003 Enterprise Edition o Datacenter Edition, utilizan un nuevo estilo denominado Tabla de Particiones GUID (GPT). En los discos con GPT se pueden crear hasta 128 particiones primarias (como no existe la limitación a cuatro particiones, no es necesario crear particiones extendidas ni unidades lógicas).

Requieren un disco GPT que contenga una partición de sistema con Interfaz de Firmware Extensible (EFI) y los archivos necesarios para iniciar el equipo. También, se pueden instalar discos MBR en sistemas basados en Itanium, pero no se podrá iniciar el sistema desde ellos.

Existen algunas diferencias entre los estilos de partición GPT y MBR, pero la mayoría de las tareas relacionadas con los discos no cambian. Los discos básicos y dinámicos funcionan de la misma manera que en Windows 2000 y ambos tipos de almacenamiento están disponibles tanto en los discos que utilizan un estilo de partición como en los que usan el otro.

3.8.2.3.- Unidades lógicas.

Las particiones secundarias se pueden dividir en una o varias unidades lógicas (puede haber un número ilimitado de unidades lógicas en un disco) que son partes más pequeñas de la partición.

3.8.2.4.- Volúmenes.

En un disco dinámico, un volumen es una parte de un disco físico que funciona igual que una unidad separada. Es equivalente a las particiones primarias de versiones anteriores.

3.8.2.5.- Espacio libre de almacenamiento.

Con este término se designa el espacio del disco duro que no pertenece a ninguna partición o volumen y puede utilizarse para crearlos.

3.8.2.6.- Sistemas de archivos.

Es posible escoger entre tres sistemas de archivos distintos para un disco duro que se utilice con Windows Server 2003:

- FAT (File Allocation System). Se puede acceder a este sistema de archivos desde MS-DOS y todas las versiones de Windows. Permite trabajar con particiones menores de 2 GB Y no soporta dominios.
- FAT32. Se puede accesar a este sistema de archivos desde Windows 95 OSR2, Windows 98, Windows 2000, Windows XP y Windows Server 2003.

Permite trabajar con particiones mayores de 2 GB, el tamaño máximo de un archivo es de 4 GB, los volúmenes pueden llegar hasta 2 TB (en Windows 2000 sólo hasta 32 GB) Y no soporta dominios.

- NTFS (NT FUe System) Es el sistema desarrollado para Windows NT 4 que permite nombres de archivo de hasta doscientos cincuenta y seis caracteres, ordenación de directorios, atributos de acceso a archivos, reparto de unidades en varios discos duros, reflexión de discos duros y registro de actividades. En Windows 2000 Server se incluyeron mejoras que permitía utilizar el Directorio Activo, dominios, cuotas en disco para cada usuario, cifrado y compresión de

archivos, almacenamiento remoto, una herramienta de fragmentación y utilización de enlaces de archivos similares a los realizados en UNIX. Sus volúmenes pueden llegar hasta 16 TB menos 64 KB Y el tamaño máximo de un archivo sólo está limitado por el tamaño del volumen.

3.8.2.7.- Discos básicos y dinámicos.

Windows Server 2003 soporta discos básicos y dinámicos.

Ambos pueden existir en un mismo sistema pero un volumen (formado por uno o más discos físicos) debe utilizar únicamente uno de los dos tipos.

Un disco básico es un disco físico que contiene particiones primarias (son aquellas que son reconocidas por la BIOS del ordenador como capaces de iniciar el sistema operativo desde ella ya que dispone de un sector de arranque), particiones extendidas o dispositivos lógicos (las particiones y las unidades lógicas de los discos básicos se conocen como volúmenes básicos). Pueden contener conjuntos de volúmenes, conjunto de espejos, conjunto de bandas con o sin paridad creados con Windows NT 4 o anterior, y se puede acceder a ellos desde MS-DOS (no es posible crear estos conjuntos desde Windows Server 2003, únicamente se pueden borrar, extender o convertirlos a tipos de volúmenes de los discos dinámicos). Es el que se establece por defecto en la instalación.

Se han de utilizar volúmenes básicos en los equipos que disponen de MSDOS, Windows 95, Windows 98, Windows Millennium, Windows NT 4.0 o Windows XP Home Edition configurados para inicio múltiple con Windows XP Professional o Windows Server 2003, ya que estos sistemas operativos no tienen acceso a los datos almacenados en los volúmenes dinámicos. I

Windows XP Professional y Windows Server 2003 no soportan los volúmenes básicos multidisco creados con Windows NT 4.0 o versiones anteriores (como son los conjuntos de volúmenes, conjunto de espejos, conjuntos de bandas sin paridad o conjuntos de bandas con paridad). Es necesario hacer una copia de seguridad y eliminar estos volúmenes o convertidos en discos dinámicos antes de instalar Windows Server 2003 (si no se hace una copia de seguridad de los volúmenes antes de la actualización a Windows Server 2003, se puede hacer posteriormente con la utilidad FT Online que se encuentra en la carpeta \Support\Tools de los discos de instalación).

Un disco dinámico es un disco físico que contiene volúmenes dinámicos creados por Windows Server 2003. Un volumen dinámico es una parte de un disco físico que funciona igual que una unidad separada, es equivalente a las particiones primarias de versiones anteriores. No puede contener particiones o discos lógicos, y no se puede acceder a ellos desde MS-DOS. Puede contener volúmenes distribuidos, volúmenes seccionados, volúmenes reflejados y volúmenes RAID-5.

Un conjunto de volúmenes puede existir en los discos básicos (aunque no en Windows Server 2003) y es la unión de una o más áreas de espacio disponibles (que pueden estar en uno o varios discos duros) que, a su vez, puede dividirse en particiones y unidades lógicas (no es reconocido por MS-DOS y sólo funciona con NTFS). Habrá una letra de unidad que representará al conjunto de volúmenes. Cuando se amplía, los datos previamente existentes no se ven afectados. Sin embargo, no es posible reducirlos si no que deberá eliminar el conjunto completo (con la pérdida de los datos). El equivalente en los discos dinámicos, es un volumen distribuido.

Un conjunto de espejos puede existir en los discos básicos (aunque no en Windows Server 2003) e indica dos particiones de dos discos duros distintos que se configuran para que una sea idéntica a la otra. La partición espejo no aparece en el Administrador de discos y sólo sirve para reflejar los datos de la otra partición (que entrará en funcionamiento cuando la primera partición falle). Este método hace que el nivel de seguridad sea alto (aunque no se evitan los virus ya que estarían grabados en ambas particiones). Se corresponde con RAID 1. El equivalente en los discos dinámicos, es un volumen reflejado.

Un conjunto de bandas puede existir en los discos básicos (aunque no en Windows Server 2003) y es la unión de dos o más áreas de espacio disponibles (que pueden estar en dos o más discos duros) que a su vez se dividirán en bandas. En cada disco duro se creará una partición y todas ellas tendrán aproximadamente el mismo tamaño (no es reconocido por MS-DOS y sólo funciona con NTFS). Habrá una letra de unidad que representará al conjunto de bandas. Pueden ser de dos tipos:

- Sin paridad. Un conjunto de bandas sin paridad dividirá cada uno de los discos duros en partes pequeñas llamadas bandas (así, si tiene cuatro discos duros y cada uno tiene diez bandas, diremos que hay diez filas de cuatro bandas cada una). Al guardar un archivo no lo hará como se describió en el conjunto de volúmenes si no

que lo distribuirá en las bandas de todos los discos duros (ocupando la primera fila de bandas disponible de cada disco duro antes de pasar a la segunda). De esa manera, el acceso será más rápido ya que se elimina parte del tiempo que tarda el cabezal en buscar los sectores y las pistas donde se encuentra el archivo pero tiene el inconveniente que si se estropea un disco duro se pierde toda la información del conjunto de bandas. Ofrece mayor velocidad en el almacenamiento de los datos ya que los datos se copian al mismo tiempo en los diferentes discos pero el nivel de seguridad es menor ya que cuando falla una banda se perderán todos los datos. Se corresponde con RAID 0. El equivalente en los discos dinámicos, es un volumen seccionado.

- Con paridad. Un conjunto de bandas con paridad utilizará una banda de cada fila del disco duro para guardar información de paridad de todas las bandas de esa fila (así, si tiene cinco discos duros y cada uno tiene diez bandas, diremos que hay diez filas de cinco bandas cada una y en cada fila hay una banda denominada de paridad). La información se guarda igual que en el conjunto de bandas sin paridad pero guardando, en la banda de paridad de cada fila, información que permitirá recuperar los datos de cualquier banda de dicha fila si dejará de funcionar. Cuando falla una banda se pueden recuperar los datos defectuosos que contenía aunque pierde velocidad de almacenamiento. Otro inconveniente que tiene es la disminución del espacio libre para guardar información en un porcentaje igual al número de discos duros que forman parte del conjunto de bandas con paridad (así, si hay cinco discos duros se perderá un 20% y si hay cuatro discos duros se perderá un 25%) y, también, que necesita mayor cantidad de memoria RAM para no ver disminuir el rendimiento del equipo (aproximadamente, un 25% más de memoria). Se corresponde con RAID 5. El equivalente en los discos dinámicos, es un volumen RAID-5.

3.9.- La configuración de seguridad.

La configuración de seguridad define el comportamiento del sistema en temas de seguridad y está constituida por los siguientes elementos:

- Directivas de cuenta que están formadas por:

- Directiva de contraseñas. Permite definir las directivas por la que se regirán las contraseñas. Entre ellas se encuentran los siguientes apartados: Longitud mínima de la contraseña, Vigencia máxima de la contraseña, Vigencia mínima de la contraseña, etc.
- Directiva de bloqueo de cuentas. Permite definir las directivas a seguir para el bloqueo de cuentas cuando se ha intentado iniciar una sesión y no se ha introducido correctamente la contraseña. Cuenta con los siguientes apartados: Duración del bloqueo de cuenta, Restablecer la cuenta de bloqueos después de y Umbral de bloqueos de la cuenta.
- Directiva Kerberos. Permite definir las directivas por las que se regirá este protocolo de autentificación. Entre ellas se encuentran los siguientes apartados: Edad máxima de renovación de tíquets de usuario, Vigencia máxima del vale de servicio, Vigencia máxima del vale de usuario, etc.

- Directivas locales que están formadas por:
  - Directiva de auditoría. Permite definir las directivas a seguir para el establecimiento de las auditorías. Entre ellas se encuentran los siguientes apartados: Auditar el acceso a objetos, Auditar sucesos de inicio de sesión, Auditar el cambio de directivas, etc.
  - Asignación de derechos de usuario. Permite asignar derechos a los usuarios. Entre ellos se encuentran los siguientes: Hacer copia de seguridad de archivos y directorios, Restaurar archivos y directorios, Permitir el inicio de sesión local, Agregar estaciones de trabajo al dominio, Denegar el acceso desde la red a este equipo, Apagar el sistema, etc.
  - Opciones de seguridad. Permiten definir actuaciones a seguir referentes a la seguridad del sistema. Entre ellas se encuentran las siguientes: Dispositivos: impedir que los usuarios instalen controladores de impresora, Inicio de sesión interactivo: no mostrar el último nombre de usuario, Apagado: permitir apagar el sistema sin tener que iniciar sesión, Dispositivos: restringir el acceso al CD-ROM sólo al usuario con sesión iniciada localmente, Dispositivos: restringir el acceso a la unidad de disquete sólo al

usuario con sesión iniciada localmente, Servidores de red Microsoft: desconectar a los clientes cuando termine el tiempo de sesión, etc.

- Registro de sucesos que define las directivas a seguir para los registros de sucesos. Entre ellas se encuentran las siguientes: Tamaño máximo de los distintos registros, Conservar los distintos registros, etc.
- Grupos restringidos que permiten la administración de miembros de grupos locales.
- Servicios del sistema que define los permisos y modo de inicio para los distintos servicios locales.
- Registro que permite definir permisos de acceso (en las listas de control de acceso discrecional DACL) y la configuración de auditoría (en las listas de control de acceso al sistema SACL) para las claves del Registro.
- Sistema de archivos que permite definir permisos de acceso (en las listas de control de acceso discrecional DACL) y la configuración de auditoría (en las listas de control de acceso al sistema SA CL) para los objetos del sistema de archivos.
- Directivas de red inalámbrica que permiten añadir una directiva de red inalámbrica para los clientes. En dicha directiva se ha de especificar el tipo de red inalámbrica a la que pueden tener acceso los clientes y el tiempo que ha de pasar para comprobar los cambios en la directiva.
- Directivas de claves públicas que están formadas por el Sistema de archivo de cifrado para la creación de agentes de recuperación de datos, la Configuración de la petición de certificados automática, la Entidades emisoras raíz de confianza y la Confianza empresarial.
- Directivas de restricción de software que tratan de regular el software desconocido o en el que no se confía.
- Directivas de seguridad IP en Active Directory que definen las reglas de seguridad IP para establecer la comunicación entre los equipos.

Se puede modificar la configuración de la seguridad de una de las formas siguientes (depende de la función que realice el servidor):

- Si el servidor Windows 2003 es un controlador de dominio y desea modificar la configuración de seguridad para todos los miembros de la seguridad de dominio. Ha de utilizar la Directiva de dominio.
- Si el servidor Windows 2003 es un controlador de dominio y desea modificar la configuración de seguridad sólo para los controladores del dominio. Ha de utilizar la Directiva de seguridad del controlador de dominio.
- Si el servidor Windows 2003 no es un controlador de dominio. Ha de utilizar la Directiva de seguridad local.

También, se puede establecer la configuración de seguridad utilizando las siguientes herramientas:

- Para definir y modificar las plantillas de seguridad personalizadas, se utiliza el complemento Plantillas de seguridad de la Consola de Administración de Microsoft.
- Para configurar el equipo y analizar su seguridad de forma local, se utiliza el complemento Configuración y análisis de seguridad de la Consola de Administración de Microsoft.
- Para editar los objetos de grupo que pueden ser vinculados a un sitio o departamento en el Directorio Activo, o almacenados en un equipo, se utiliza el complemento Editor de objetos de directiva de grupo de la Consola de Administración de Microsoft o la directiva de seguridad correspondiente.
- Para ver el conjunto resultante de directivas para un usuario en un equipo, se utiliza el complemento Conjunto resultante de directivas de la Consola de Administración de Microsoft o la directiva de seguridad correspondiente.

3.9.1.-Las directivas de seguridad.

Como se indicó anteriormente, puede haber tres tipos de directivas de seguridad:

- Directiva de seguridad del controlador de dominio. Es la que se debe utilizar si el servidor Windows 2003 es un controlador de dominio y se desea modificar la configuración de seguridad para todos los controladores de dominio.

- Directiva de seguridad local. Es la que se debe utilizar si el servidor Windows 2003 no tiene instalado el Directorio Activo y se desea modificar su configuración de seguridad (cuenta con menos nodos de configuración que las dos anteriores).
- Como las dos primeras opciones cuentan con los mismos nodos de configuración y algunos de dichos nodos se encuentran disponibles en la tercera, se va a describir únicamente la Directiva de seguridad de dominio.

3.9.2.- Las Plantillas de seguridad.

Una Plantilla de seguridad es un archivo donde se almacena un grupo de configuraciones de seguridad. Windows 2003 incluye una serie de plantillas de seguridad basadas en la función de un equipo que van desde configuraciones de seguridad para los clientes de un dominio de baja seguridad hasta controladores de dominio de alta seguridad. Estas plantillas se pueden utilizar tal como se proporcionan y también se pueden modificar o servir como base para crear plantillas de seguridad personalizadas.

3.10.- Kerberos V5.

Kerberos V5 es el protocolo de seguridad principal para la autenticación dentro de un dominio. Comprueba la identidad del usuario y los servicios de red. Esta comprobación doble se denomina autenticación mutua.

El mecanismo de autentificación de Kerberos V5 emite vales para tener acceso a los servicios de red. Estos vales contienen datos cifrados que incluyen una contraseña cifrada para confirmar la identidad del usuario al servicio solicitado.

Exceptuando la escritura de una contraseña o las credenciales de tarjeta inteligente, todo el proceso de autenticación es transparente para el usuario.

El Centro de distribución de claves (KDC) que se ejecuta en cada controlador de dominio como parte del Directorio Activo, se utiliza para almacenar todas las contraseñas del cliente y otros datos de su cuenta.

El proceso de autentificación Kerberos V5 funciona de la manera siguiente:

1. Un usuario de un sistema cliente se autentifica en el KDC mediante una contraseña o tarjeta inteligente.

2. El KDC emite al cliente un vale especial (TGT). El sistema de cliente utiliza este TGT para tener acceso al servicio de concesión de vales (TGS) que forma parte del mecanismo de autenticación Kerberos V5 en el controlador de dominio.
3. El TGS emite a continuación un vale de servicio al cliente.
4. El cliente presenta este vale de servicio al servicio de red solicitado. El vale de servicio prueba la identidad del usuario al servicio y la identidad del servicio al usuario.

3.10.1.- Kerberos V5 y los controladores de dominio.

Los servicios de Kerberos V5 se instalan en cada controlador de dominio y se instala un cliente de Kerberos en cada estación de trabajo o servidor.
Cada controlador de dominio funciona como un KDE. Cada cliente utiliza NS para localizar el controlador de dominio disponible más cercano. Este controlador de dominio funcionará como el KDC preferido para ese usuario durante el inicio de sesión del usuario. Si el KDC preferido deja de estar disponible, el sistema localizará otro KDC alternativo para proporcionar la autenticación.

3.10.2.- Interoperabilidad de Kerberos V5.

Windows Server 2003 admite dos tipos de interoperabilidad de Kerberos V5.

- Se puede establecer una relación de confianza entre un dominio y un dominio Kerberos basado en MIT (de esta manera, un cliente de un dominios de Kerberos se puede autentificar en un dominio del Directorio Activo para tener acceso a los recursos de red del dominio).
- En un dominio, los clientes y los servidores UNIX pueden tener cuentas del Directorio Activo y por tanto pueden ser autenticados desde un controlador de dominio.

3.11.-Domain Name System (DNS).

El Sistema de Nombres de Dominios (DNS) es un conjunto de protocolos y servicios sobre una red TCP/IP, permite a los usuarios de red utilizar nombres jerárquicos sencillos para comunicarse con otros equipos en vez de memorizar y usar sus direcciones IP. Este sistema es muy usado en Internet y en muchas de las redes privadas actuales. Las utilerías como: browsers, servidores de Web, FTP y Telnet; utilizan DNS.

La función más conocida de los protocolos DNS es convertir nombres a direcciones IP por la mayor facilidad de aprenderlos y la flexibilidad de cambiar la dirección IP. Antes de la implementación de DNS, el uso de nombres de computadoras era hecha a través de listas de nombres y sus direcciones IP correspondientes almacenados en archivos HOSTS. En Internet, este archivo estaba administrado centralizadamente y debía ser periódicamente actualizado en las diferentes redes. A medida que el número de máquinas en Internet crecía, esto comenzó a ser una solución impráctica; DNS fue la manera de resolver este problema.
De acuerdo al Dr. Paul Mockapetris principal diseñador de DNS, el propósito original de DNS fue reemplazar los problemas de administrar archivos HOSTS por medio de una simple base de datos distribuida que permitiera a través de una estructura de nombres jerárquica, la distribución de la administración, tipos de datos extensibles, una base de datos virtualmente ilimitada, y un rendimiento razonables.
DNS es un protocolo de aplicación y usa tanto UDP como TCP. Los clientes solicitan a los servidores de DNS sus consultas por medio de UDP para hacer más rápida la comunicación y utilizan TCP sólo en caso de que llegara a ocurrir una respuesta truncada.
La más popular implementación del protocolo DNS es BIND (Berkeley Internet Name Domain).

3.11.1.- Definición.

Un Sistema de Nombres de Dominio está compuesto de una base de datos distribuida de nombres. Los nombres en la base de datos DNS generan una estructura lógica en forma de árbol conocida como domain name space. Cada nodo o dominio en el domain name space es nombrado y puede contener subdominios.
Los dominios y subdominios están agrupados en zonas que permiten la administración distribuida del name space. El nombre de dominio identifica la posición del dominio en el árbol lógico de DNS en relación a su dominio padre, separando cada rama del árbol con un punto ".".

3.11.2.- Servidores DNS y la Internet.

La raíz de la base de datos de DNS en Internet es administrada por el Internet Network Information Center. Los dominios de más alto nivel fueron asignados por tipo de organización y país. Los nombres de dominios siguen el estándar internacional 3166. Abreviaturas de dos y tres letras son usadas para los países, otras están reservadas para el uso de organizaciones, como:

Tabla 3.1.-Nombres de Dominios.

Nombre del Dominio	DNS Tipo de Organización
.com	Comercial
.edu	Educacional
.int	Internacional
.mil	Militar
.net	Organizaciones de red
.org	Organizaciones no comerciales

3.11.3.- Dominios y Zonas.

3.11.3.1.- Dominios.

Cada nodo en el árbol de la base de datos de DNS junto con todos sus nodos hijo es llamado un dominio. Los dominios pueden contener computadoras y otros dominios (subdominios). Por ejemplo el dominio Cibernética ciber.com puede contener otras computadoras como servidor.ciber.com y subdominios como desarrollo.ciber.com que puede contener a otros nodos como html.desarrollo.ciber.com. Los nombres de dominios y

de host tienen restricciones permitiendo solamente el uso de los caracteres "a-z", "A-Z", "0-9" y "-". El uso de caracteres como "/", "." y "_" no son permitidos.

3.11.3.2.- Zonas.

Una zona es un archivo físico para almacenar y administrar un conjunto de registros del name space de DNS. A este archivo se le llama: archivo de zona. Un solo servidor DNS puede ser configurado para administrar uno o varios archivos de zona. Cada zona esta ligada a un nodo de dominio específico conocido como dominio raíz de la zona.
Distribuir el dominio entre varios archivos de zona puede ser necesario para distribuir la administración del dominio a diferentes grupos o por eficiencia en la replicación de datos.

3.11.4.- Servidores de Nombres.

Los servidores de nombres DNS (NS) almacenan la información acerca del espacio de nombres de dominio. Los servidores de nombres generalmente "tienen autoridad" (administran) una o mas zonas.
Al configurar el servidor de nombres DNS se le informan de los otros servidores de nombres DNS del mismo dominio.

3.11.4.1.- Nombres de Servidores: Primarios, Secundarios y Maestros.

Un nombre de servidores primario obtiene los datos de sus zonas de sus archivos locales. Los cambios a la zona, como añadir otros dominios o nodos, se hacen en el NS Primario.
Un nombre de servidor secundario obtiene los datos de sus zonas del NS autoridad de la zona. El proceso de obtener la información del archivo de la base de datos de la zona por medio de la red se conoce como una transferencia de zona. Hay dos razones para tener NS secundarios. Estas razones son:

- Redundancia. Se necesitan al menos dos NS en cada zona, un primario y al menos un secundario por redundancia. Como cualquier sistema de tolerancia a fallas, las máquinas deben ser independientes, por ejemplo diferentes redes.

- Localidades Remotas. Para reducir la cantidad de trabajo en el servidor primario.

Como la información de cada zona es almacenada en archivos independientes, la designación de primario o secundario, está definida a un nivel de zona. En otras palabras, un NS puede ser primario para ciertas zonas y secundario para otras. Cuando se define una zona con un NS como secundario, se debe especificar un NS del cual obtener la información de la zona.

A la fuente de información de la zona para un NS secundario se le llama: servidor de nombres maestro. Un NS maestro puede ser primario o secundario. Cuando un NS secundario se inicializa, este se comunica con el NS maestro e inicia una transferencia de zona con el servidor.

El uso de servidores secundarios como servidores maestros ayuda mucho cuando el servidor primario esta muy ocupado o cuando la forma de comunicación es más eficiente.

3.11.5.-Forwarders y Esclavos.

Cuando un NS DNS recibe una solicitud DNS, el intenta localizar la información dentro de sus propios archivos de zona. Si falla porque el servidor no tiene autoridad por el dominio solicitado, el se debe comunicar con otros NS para satisfacer la solicitud.

Para resolver este problema, DNS utiliza el concepto de forwarders. Ciertos NS son seleccionados como forwarders y solamente ciertos forwarders determinados realizan comunicaciones en Internet. Esta configuración se hace por servidor, no por zonas.

Cuando un servidor configurado para usar forwarders recibe una solicitud DNS que es incapaz de resolver, transfiere la solicitud a uno de sus forwarders determinados. El forwarder entonces lleva a cabo cualquier comunicación necesaria para satisfacer la solicitud y regresar el resultado.

Los esclavos son servidores configurados para utilizar forwarders y para regresar un mensaje de falla si el forwarder no puede satisfacer la solicitud. Los esclavos no intentan contactar a otros NS si el forwarder es incapaz de satisfacer la solicitud.

3.11.6.-Caching-only Servers.

Aunque todos los NS almacenan temporalmente (caché) las consultas contestadas, los servidores de Caching-only son NS cuyo único trabajo es ejecutar consultas, almacenar las respuestas y regresar resultados. En otras palabras, ellos no tienen autoridad sobre ningún dominio y solamente contienen información que han almacenado al satisfacer consultas.
Para determinar cuándo usar un servidor caching-only, se debe pensar que el servidor al inicializarse no tiene información de nombres y la irá adquiriendo. Sin embargo para redes muy lentas, se genera menos tráfico que en una transferencia de zona.

3.11.7.-Resolución de Nombres.

Hay tres tipos de consultas que un cliente puede hacer a un servidor DNS: recursiva, interactiva e inversa. Estas consultas no solo se realizan entre clientes DNS y servidores DNS sino también entre servidores.

3.11.8.- Consultas Recursivas.

En una consulta recursiva, el NS responde con el dato solicitado o un estado de error. El NS no puede transferir la consulta a otro NS.
Este tipo de consulta es típicamente hecha por un cliente DNS a un servidor DNS.

3.11.9.- Consultas Interactivas.

En una consulta interactiva, el servidor consultado trata de dar la mejor respuesta. Este tipo de consulta es típicamente hecha por un servidor DNS a otro, después de recibir una consulta recursiva desde el resolver (cliente).

3.11.10.- Consulta Inversa.

Cuando un resolver tiene una dirección IP y desea conocer el nombre del nodo, utiliza una consulta inversa. Debido a que no hay una relación directa entre el espacio de nombres

DNS y sus direcciones IP asociadas, solamente una búsqueda en todos los dominios podría garantizar una respuesta correcta.

Para remediar este problema, un dominio especial "in-addr.arp." en el espacio DNS fue creado. Los nodos en el dominio "in-addr.arpa" son nombrados después de sus números en la representación IP de octetos.

Sin embargo como las direcciones IP son más específicas de derecha a izquierda y los dominios los son de izquierda a derecha, el orden de los octetos de las direcciones IP debe escribirse al revés. Así, la administración de las "ramas inferiores" del árbol DNS in-addr.arp pueden otorgarse a las compañías en base a sus clases A, B, o C.

Cuando el árbol de dominios es construido en la base de datos DNS, un registro apuntador especial es añadido a la dirección IP asociada al nombre del nodo correspondiente. En otras palabras, para encontrar un nombre de nodo en base a una dirección IP, el resolver preguntará por un registro apunto a una dirección IP. Si esta dirección IP esta fuera del dominio local, el servidor DNS comenzará a resolver a otros nodos del dominio.

3.11.11.- Cache y Tiempo de Vida.

Cuando un servidor de nombres esta procesando una consulta recursiva, posiblemente envíe varias consultas para encontrar una respuesta. El NS almacena en cache toda la información que recibe durante el proceso por cierto tiempo especificado en los datos regresados. Esta cantidad de tiempo se conoce como el: Tiempo de Vida (Time To Live, TTL). El administrador del NS de una zona decida el TTL para sus datos. Valores pequeños de TTL ayudarán a asegurar la consistencia de los datos, sin embargo, incrementa el trabajo para el NS.

Cuando los datos se almacenan en la cache del servidor DNS, él comienza a decrementar su TTL para saber cuando eliminarlo. Si una consulta se satisface en base a los datos en cache, el TTL devuelto será la cantidad de tiempo restante en la cache del servidor DNS. Así, los clientes también conocen cuando expira un dato.

3.12.- DHCP

DHCP (Dynamic Host Configuration Protocol) es un protocolo desarrollado para asignar direcciones IP a los clientes que lo soliciten.

Cada equipo de una red TCP/IP debe tener un nombre y una dirección IP únicos. La dirección IP junto con su máscara de subred relacionada identifica al equipo y a la subred a la que está conectada. Al mover un equipo a otra subred diferente, se debe cambiar la dirección IP. DHCP asigna dinámicamente una dirección IP a un cliente, a partir de una base de datos del servidor DHCP de la red local.

Proporciona las siguientes ventajas:

- Una configuración segura y fiable, ya que evita los errores de configuración producidos al escribir manualmente valores en cada equipo. Así mismo, ayuda a evitar los conflictos de direcciones causados al asignar direcciones lP que ya están siendo utilizadas en la red.
- Reduce la administración de la configuración. La utilización de servidores DHCP puede reducir significativamente el tiempo necesario para configurar y reconfigurar los equipos de la red.

El proceso a seguir por un cliente DHCP es el siguiente:

l. Manda un mensaje al servidor DHCP solicitando una dirección IP.

2. El servidor DHCP responde ofreciendo las direcciones IP que tiene disponibles.

3. El cliente selecciona una y envía una solicitud de uso de la dirección al servidor DHCP.

4. El servidor DHCP admite la solicitud y garantiza al cliente la concesión del uso de la dirección durante el tiempo determinado.

5. El cliente utiliza la dirección para conectarse a la red.

Las direcciones se conceden por un periodo de tiempo determinado. Cuando dicho periodo ha finalizado, el cliente deberá solicitar la renovación de la concesión o la dirección pasará al estado de disponible. Si solicita la renovación y no puede renovársela, se le asignará otra.

Todo el proceso de instalación y configuración de DHCP tiene que hacerlo habiendo iniciado una sesión como un usuario miembro del grupo Administradores.

3.12.1.- BOOTP y DHCP.

El Protocolo de inicio (BOOTP) es un protocolo de configuración de equipos desarrollado con anterioridad a DHCP. DHCP supera a BOOTP y resuelve limitaciones específicas de éste, como el servicio de configuración de equipos.

3.12.2.- Similitudes entre BOOTP y DHCP.

Debido a las relaciones entre BOOTP y DHCP, ambos protocolos comparten algunas características. Sus elementos comunes son:

- La estructura de formato utilizada para intercambiar mensajes entre el servidor y los clientes. Los mensajes de solicitud que envían los clientes y mensajes de respuesta que envían los servidores son casi idénticos, utilizan un datagrama UDP (User Datagram Protocol) de 576 bytes que contiene el mensaje del protocolo. Los encabezados de los mensajes son los mismos en BOOTP y DHCP con la excepción de el campo de encabezado de mensaje final utilizado para contener datos opcionales (en BOOTP, este campo opcional se llama área específica del fabricante y está limitada a 64 octetos, mientras que en DHCP recibe el nombre de campo de opciones y puede contener hasta 312 octetos de información de opciones).
- El uso de puertos UDP conocidos para la comunicación entre cliente y servidor. Ambos utilizan los mismos puertos de protocolo reservado para el envío y recepción de mensajes entre servidores (puerto UDP 67) y clientes (puerto UDP 68).
- La distribución de direcciones IP como parte integral del servicio de configuración. Aunque BOOTP y DHCP asignan direcciones IP a los clientes durante el inicio, utilizan distintos métodos de asignación. Normalmente BOOTP proporciona la asignación fija de una dirección IP para cada cliente y reserva definitivamente esta dirección en la base de datos del servidor BOOTP. Mientras que DHCP proporciona la asignación dinámica de concesiones de las direcciones IP disponibles y reserva temporalmente la dirección del cliente DHCP en la base de datos del servidor DHCP.

3.12.3.- Diferencias entre BOOTP y DHCP.

Hay importantes diferencias en la forma en que ambos realizan la configuración del equipo.

Tabla 3.2.- Diferencias entre BOOTP y DHCP.

BOOTP	DHCP
Diseñado antes que DHCP.	Diseñado después que BOOTP.
Pensado para configurar estaciones de trabajo sin disco con capacidades de inicio limitadas.	Diseñado para configurar equipos de la red que cambian frecuentemente de ubicación, tienen discos duros locales y capacidades de inicio completas.
Admite un número limitado de parámetros de configuración de los clientes llamados extensiones de fabricante.	Admite un conjunto mayor y extensible de parámetros de configuración de los clientes llamados opciones.
Durante su proceso de configuración, los clientes se comunican con servidores BOOTP para realizar la determinación de direcciones y la selección del inicio, utilizando TFTP para realizar la transferencia del archivo de imagen de inicio.	Durante su proceso de configuración, los clientes se comunican con servidores BOOTP, los cliente DHCP negocian con un servidor DHCP para determinar su dirección IP y nombre. Pueden obtener otros detalles de configuración del archivo inicial que necesitan para funcionar en la red.
Los clientes BOOTP no reenlazan ni renuevan la configuración con el	Los clientes DHCP no requieren que el sistema se reinicie para reenlazar o renovar la

servidor BOOTP, excepto al reiniciarse el sistema.	configuración con el servidor DHCP. Por el contrario, los clientes reenlazan automáticamente en intervalos de tiempo establecidos para renovar la asignación de la dirección concedida con el servidor DHCP. Este proceso se produce en segundo plano y es transparente para el usuario.

Capítulo 4.- Construcción de la intranet.

4.1.- ¿Qué es un servidor web?

Un servidor web es un programa que se está ejecutando en un equipo, normalmente un servidor que proporciona páginas web a los "clientes" que le piden. Los clientes son los navegadores web como Internet Explorer o NetScape.

Cuando llamamos a un equipo "servidor" nos referimos a un equipo que va a proporcionar determinados servicios a los usuarios de una red local o de Internet. Lleva un equipamiento de prestaciones más avanzadas que un equipo de sobremesa y sobre todo incorpora un sistema operativo de servidor.

Por tanto si en un navegador o explorador web escribimos una dirección o una página intentará localizar el servidor escrito y buscar la página solicitada. Para que ocurra esto debemos tener instalado en nuestro servidor el programa Internet Information Server. Internet Information Server, que llamaremos IIS, es el servidor de páginas web de Microsoft. Éste viene de forma gratuita con el sistema operativo Windows NT, 2000 y XP y descargable para los demás.

Antes de continuar repasemos los sistemas operativos existentes y los recomendados para crear nuestra intranet (cliente) y para alojarla (servidor).

En nuestro equipo debemos tener:

Tabla 4.1.- Sistemas Operativos y recomendaciones para crear una intranet. (PC)

Windows 95/98/ME	**Windows NT 4.0**	**Windows 2000 Professional**	**Windows XP Professional**
Muy limitados, no trabajan con servicios y no gestionan los programas y memoria con eficacia	Aunque un poco antiguo perfectamente apto y estable.	El mejor Windows hasta el momento y el recomendado para trabajar	Revisión multimedia del Windows 2000. Todavía no ha alcanzado la "madurez"
No utilizar	Requiere PII 300, 64 Mb	Requiere PIII 600, 128 Mb	Requiere PIV 1000, 256 Mb

Tabla 4.2.- Sistemas Operativos y Recomendaciones para crear una intranet. (Servidor)

Windows NT 4.0 Server	**Windows 2000 Server/Advanced Server**
Aunque está un poco anticuado es tremendamente estable y seguro. Con el Service Pack 5.0 la estabilidad y el rendimiento es realmente bueno. Sin embargo su servidor de Internet no incorpora las últimas tecnologías.	A la espera de los nuevos server la serie 2000 es la última. Es más complejo que el NT 4.0 pero incorpora muchas funcionalidades, escalabilidad y estabilidad.
Requiere PIII 800, 256 Mb y discos SCSI	Requiere PIII 800, 512 Mb y discos SCSI

Por tanto recomendamos que en nuestro servicio de páginas web se instale Windows 2000 Server. Como equipo cliente para poder manipular el servidor y todas sus opciones utilizaremos un 2000 ó XP professional.

En nuestro equipo "cliente" o en el que vamos a trabajar sólo nos queda utilizar un buen editor de páginas web o editor de sitios web. Front Page 2000/XP es el editor que mejor sincroniza con nuestro IIS, por lo tanto en nuestro curso utilizaremos Front Page de Microsoft como editor del sitio Web. Es un producto que como opción forma parte de la

suite Office de Microsoft. Finalmente un accesorio que incorpora IIS va a conectar nuestro Front Page con el servidor web IIS. Este accesorio se llama "Extensiones de servidor de Front Page" que veremos posteriormente.

Resumiendo necesitamos instalar lo siguiente:

- Servidor:
    - Internet Information Server
    - Extensiones de servidor
- Cliente (estación de trabajo)
    - Front Page 2000 ó Front Page XP

4.2.- Instalación de IIS.

Ahora se procederá a la instalación del servidor Web. Nos basaremos en Internet Information Server 5.0 que es el incluido con Windows 2000 Server que será el sistema operativo para el servidor. Sin embargo prácticamente todo lo que se comenta y explica en este capitulo es válido para las otras versiones menores (2000 Professional y XP)
Si estamos trabajando con un Windows 2000 Server el programa ya se tiene instalado, para comprobarlo... hacemos doble clic en la opción "Agregar /Quitar programas" del panel de control de Windows. Una vez abierto seleccionamos la opción "Agregar componentes de Windows"

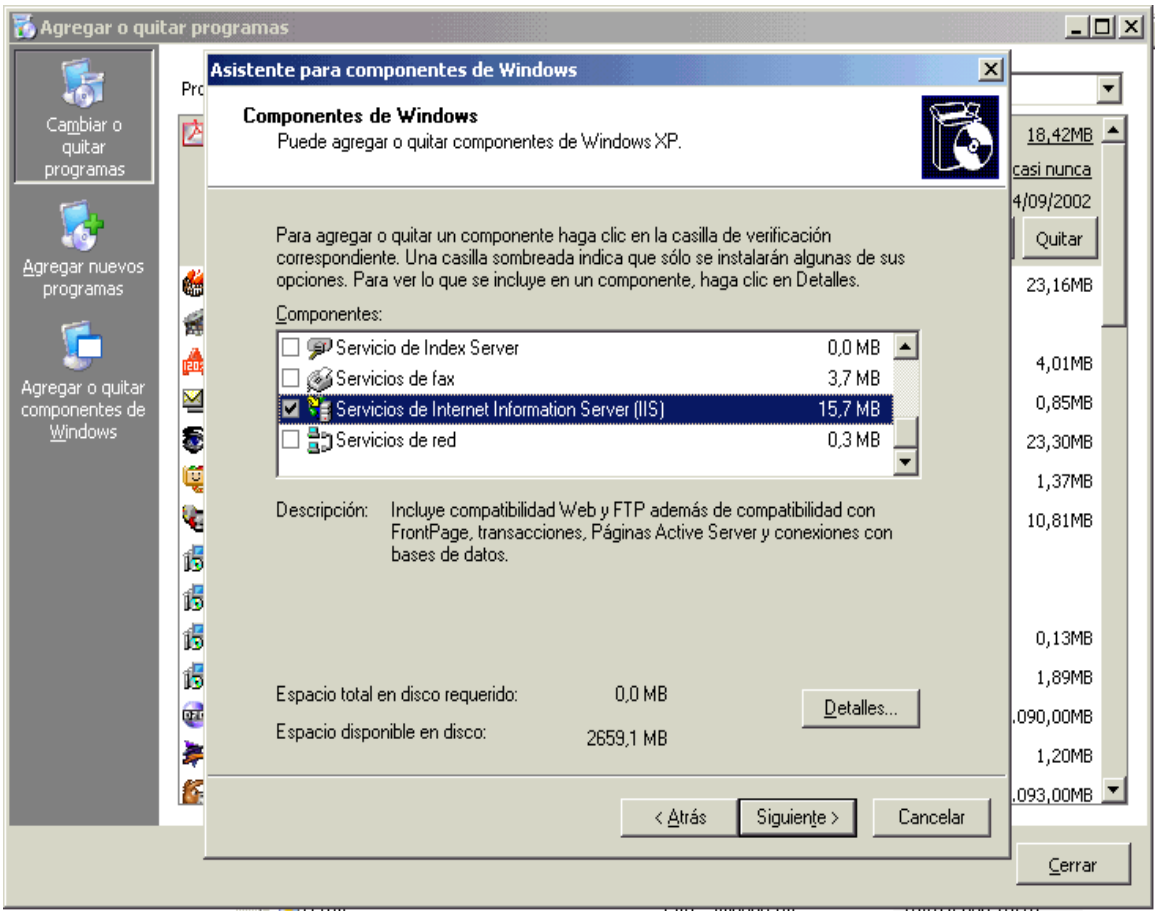

Figura 4.1.-Instalación de Internet Information Server (IIS).

Si nos desplazamos a la parte inferior podemos ver que está instalado el programa "Servicios de Internet Information Server". Si queremos instalar la versión "Professional" para desarrollo veremos que no está instalada, pulsamos en la casilla de verificación y a continuación el botón siguiente para finalizar la instalación.

Con el botón "Detalles" podemos ver los componentes de estos Servicios de IIS.

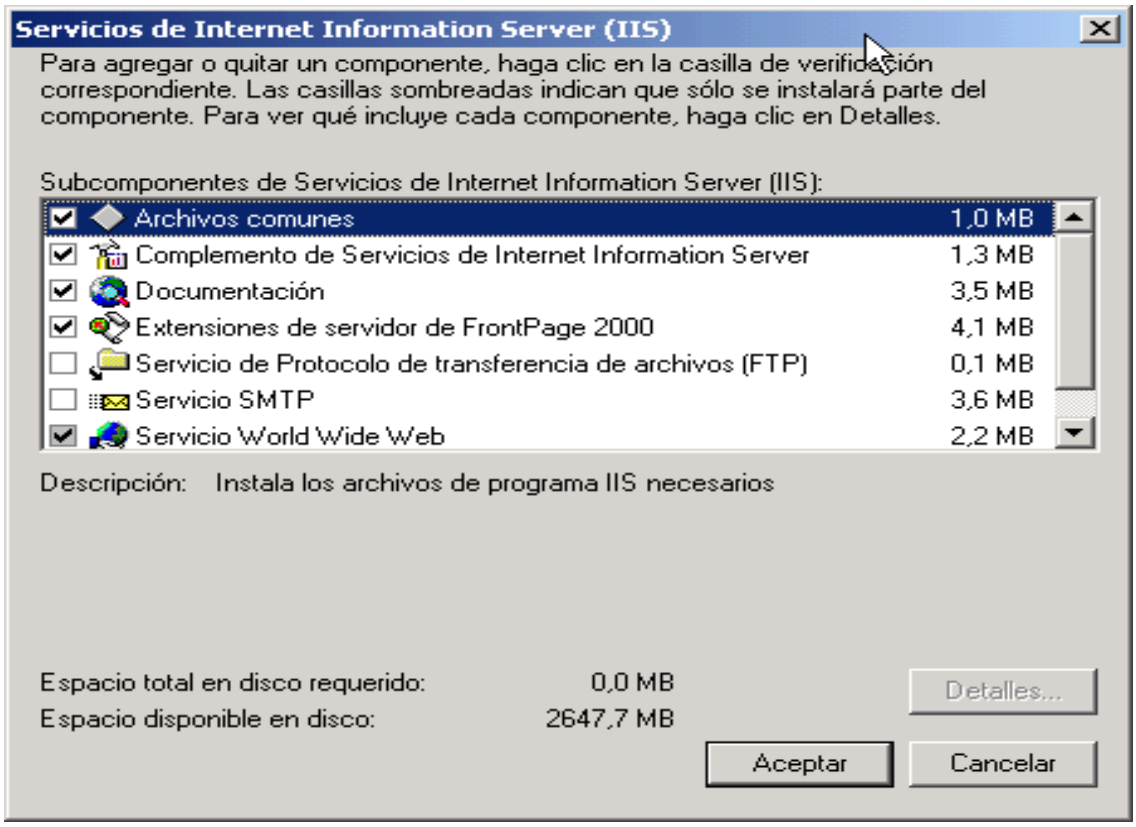

Figura 4.2.-Instalación de servicios de Internet Information Server (IIS).

Tabla 4.3.- Servicios de Internet Information Server (IIS).

Archivos comunes	Ficheros imprescindibles de Internet Information Server. Puesto que IIS además instala otros servicios éstos utilizan estos "archivos comunes". Son obligatorios.
Complemento de Servicios de Internet Information Server	Instala la interfaz administrativa o consola de administración. También es un componente imprescindible porque nos va a permitir administrar nuestra

	Intranet
Documentación	Documentación completa del IIS: Su instalación, funcionamiento, opciones, programación, ...
Extensiones de servidor de Front Page 2000	Complemento indispensable para que se comuniquen correctamente el servidor web (IIS) y nuestro editor Front Page 2000. Es imprescindible.
Servicio de Protocolo de transferencia de archivos (FTP)	Módulo adicional para crear un servidor de transferencia de archivos conocido como FTP. En nuestro paso no es necesario puesto que lo realizaremos todo desde la propia Intranet.
Servicio SMTP	Módulo adicional para crear un servicio de transferencia de mensajes o SMTP. Tampoco es necesario para nuestra Intranet
Servicio World Wide Web	Servicio de publicación de páginas web. Es decir nuestro IIS, imprescindible.
Sólo Server: Servicio NNTP	Proporciona un servicio de grupos de noticias o "newsgroup". No es necesario.
Sólo Server: Administrador de servicios Internet HTML	Páginas web con las que podemos administrar el sitio web. Es otra forma alternativa a la consola de administración. No es recomendable porque es un potencial agujero de seguridad: si alguien consigue acceder a estas páginas puede detener y romper nuestra Intranet.
Sólo Server: Visual InterDev RAD	Complemento para conectar los sitios

	web con el programa Visual Interdev para desarrollo. Este programa funciona bien con aplicaciones cliente pero no para páginas de nuestra Intranet así que no lo instalaremos.

Una vez instalado o comprobado el servidor IIS, éstos se instalan en el servidor como "servicios". Un servicio es un programa especial que está continuamente en ejecución y que simplemente "espera conexiones" por ejemplo espera que le soliciten páginas web. Otros servicios pueden proporciona vídeo bajo demanda, transferencias de ficheros (FTP) o servicios de chat. En este caso nos centraremos en el servidor Web de Microsoft: Internet Information Server.

Vamos a comprobar que se están ejecutando correctamente los servicios necesarios para nuestro servidor. Para esto seleccionamos la opción "servicios" dentro de la carpeta "herramientas administrativas" del panel de control:

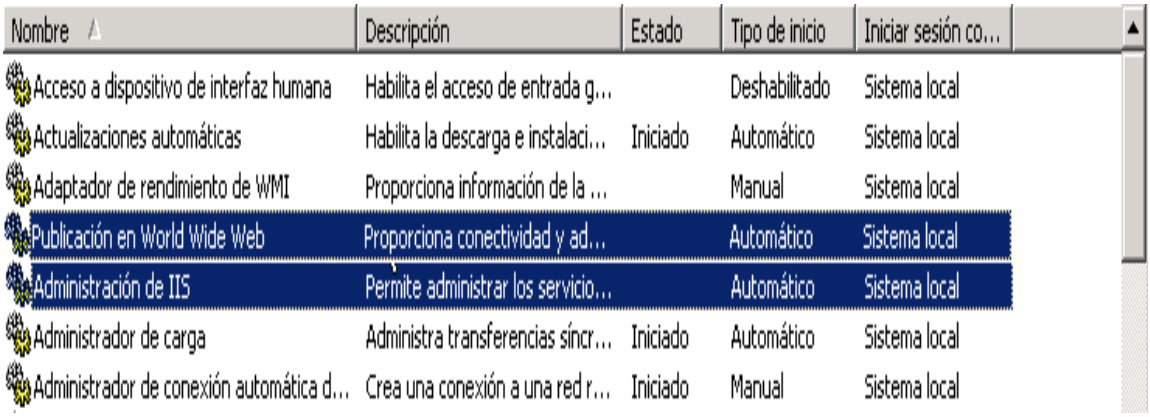

Figura 4.3.-Verificación de los servicios necesarios para el servidor.

Los dos servicios que deben estar funcionando son: la administración de IIS que nos va a permitir conectar la consola MMC de administración con el servidor web y el propio IIS como "Publicación en Word Wide Web". El inicio debe estar como en la imagen en "automático" de esta forma nos aseguramos que se inicia el servidor web al reiniciar el equipo o el servidor.

4.2.1.- Comentarios.

Técnicamente las páginas web utilizan el protocolo HTTP de TCP/IP que corresponde al puerto 80. Por lo tanto el navegador intenta conectarse a la dirección del servidor mediante el puerto 80.

El servidor IIS no tiene ninguna desventaja del famoso Apache de Linux. De hecho si quitamos la gratuidad al servidor Apache no le queda absolutamente nada que no pueda hacer IIS, incluso al contrario: la orientación a componentes de IIS es mucho más completa y mejor implementada que la del Apache. IIS soporta la misma carga de clientes, es fácil de instalar y configurar y su mantenimiento es trivial cosa que no se puede decir de su competidor. Uno de los temas en los que Microsoft todavía tiene que avanzar es en la seguridad, el abarcar tantos conceptos, tecnologías y componentes hace que IIS sean más susceptibles de tener agujeros de seguridad que su competidor, más simple y limitado. En cualquier caso en las Intranets IIS de Microsoft gana por goleada. A lo largo de este curso iremos viendo porqué y que elementos podremos integrar en nuestra Intranet.

Como complemento a nuestra Intranet debemos utilizar bases de datos para almacenar información. Quizás el uso de las bases de datos en las Intranets sea la parte más importante porque la función de una Intranet que es proporcionar información debe estar de alguna forma almacenada y ordenada en bases de datos.

Internet Information Server 5.0 es un servidor Web para plataformas Windows 2000 completamente integrado con el sistema operativo. IIS 5.0 forma parte de la instalación de Windows 2000 y permite disponer de un servidor Web tanto en el entorno de Internet como en el entorno de Intranet. IIS 5.0 se encuentra en todas las versiones de Windows 2000: BProfessional, Server, y Advanced Server, pero para implementar un servidor Web es más adecuado elegir la versión Server o Advanced Server, aunque para pruebas o desarrollo puede ser completamente válida la versión Professional.

IIS 5.0 ofrece una administración muy sencilla que se realizará mediante el Administrador de servicios de Internet. La versión 5.0 de IIS permite que el desarrollo de aplicaciones Web sea mucho más robusto y la creación de sitios Web sea más configurable y completa. Ofrece un entorno escalable basado en los componentes cliente/servidor que se pueden integrar dentro de las aplicaciones Web.

Internet Information Server 5.0 es el servidor Web más rápido y recomendable para la plataforma Windows 2000, ya que se encuentra integrado completamente con el Servicio de Directorios de Windows 2000, esta combinación del servicio Web con los servicios del sistema operativo permite desarrollar aplicaciones basadas en la Web fiables y escalables.

4.3.- Primeros pasos con IIS.

Si la instalación ha sido correcta podremos entrar ya en el sitio web. Para comprobarlo basta con iniciar un explorador web y escribir en la barra de dirección el nombre de nuestro servidor web, en nuestro caso se nombra como "servidor". Se pueden dar dos casos, si se ejecuta desde el servidor o desde un equipo de nuestra red. No es recomendable trabajar en el propio servidor pero si fuera así se muestra una pantalla como esta:

Figura 4.4.-Pantalla de la bienvenida al servidor IIS.

Pantalla que da la bienvenida al servidor IIS y facilita alguna herramienta de administración a través de páginas web. Sin embargo lo habitual y recomendable es que se trabaje desde otro equipo. Si es este el caso en lugar de recibir una pantalla con administración e información sobre el servidor web se muestra otra por seguridad similar a la siguiente:

Nota Si se esta trabajando con las versiones "personales" del IIS, es decir, con W2000 Professional o Windows XP, lógicamente se esta trabajando en local por lo que recibiremos la pantalla mencionada arriba.

En construcción

El sitio al que intentó conectarse no tiene en este momento una página predeterminada. Es posible que esté en proceso de actualización.

Inténtelo de nuevo más tarde. Si el problema continúa, póngase en contacto con el administrador del sitio Web.

Figura 4.5.-Pantalla de página en construcción.

Si nos fijamos en la primera pantalla, cuando se ejecuta en el equipo que tiene el servidor ya avisa de que los clientes recibirán este mensaje:

Actualmente no tiene ningún documento configurado para sus usuarios. A todos los usuarios que intenten conectar con su sitio, se les mostrará una página "En construcción".

Si nos fijamos en el mensaje lo que al principio podíamos tomar como un error es simplemente un mensaje que le falta una página de inicio al servidor web. La versión 4.0 de NT Server si que activaba por defecto un sitio web de ejemplo pero ese sitio era un agujero de seguridad puesto que permitía realizar algunas operaciones "peligrosas" por este motivo en el Server 2000 Microsoft no activa ningún web sino que devuelve una página diciendo que si está funcionando pero que ahora hay que alimentarlo.

Por lo tanto, para empezar a configurar los sitios Web debe indicar los directorios que contienen los documentos que desea publicar. El servidor Web no puede publicar documentos que no están en los directorios especificados. Por lo tanto, el primer paso para desarrollar un sitio Web debe ser determinar cómo desea organizar los archivos. Después se utiliza el complemento IIS para identificar los directorios que forman parte del sitio.
La estructura de directorios que IIS crea es la siguiente:
Para empezar, al configurar los sitios Web debe indicar los directorios que contienen los documentos que desea publicar. El servidor Web no puede publicar documentos que no están en los directorios especificados. Por lo tanto, el primer paso para desarrollar un sitio Web debe ser determinar cómo desea organizar los archivos. Después se utiliza el complemento IIS para identificar los directorios que forman parte del sitio.
En la siguiente sección veremos como administrar básicamente nuestro Internet Information Server y las opciones básicas más importantes.

4.4.- La consola Administrativa.

Para administrar y controlar nuestro servidor web vamos a utilizar la consola administrativa de IIS. Para utilizarla necesitamos tener instalado el componente de IIS en nuestro equipo. Si estamos trabajando directamente con el servidor o si tenemos un IIS instalado en nuestro equipo tenemos lo necesario para poder iniciar la consola.

Para ponerla en marcha pulsaremos el icono  "Servicios de Internet Information Server" de las Herramientas Administrativas del Panel de Control. O si estamos en el servidor seleccionamos la opción de la siguiente figura:

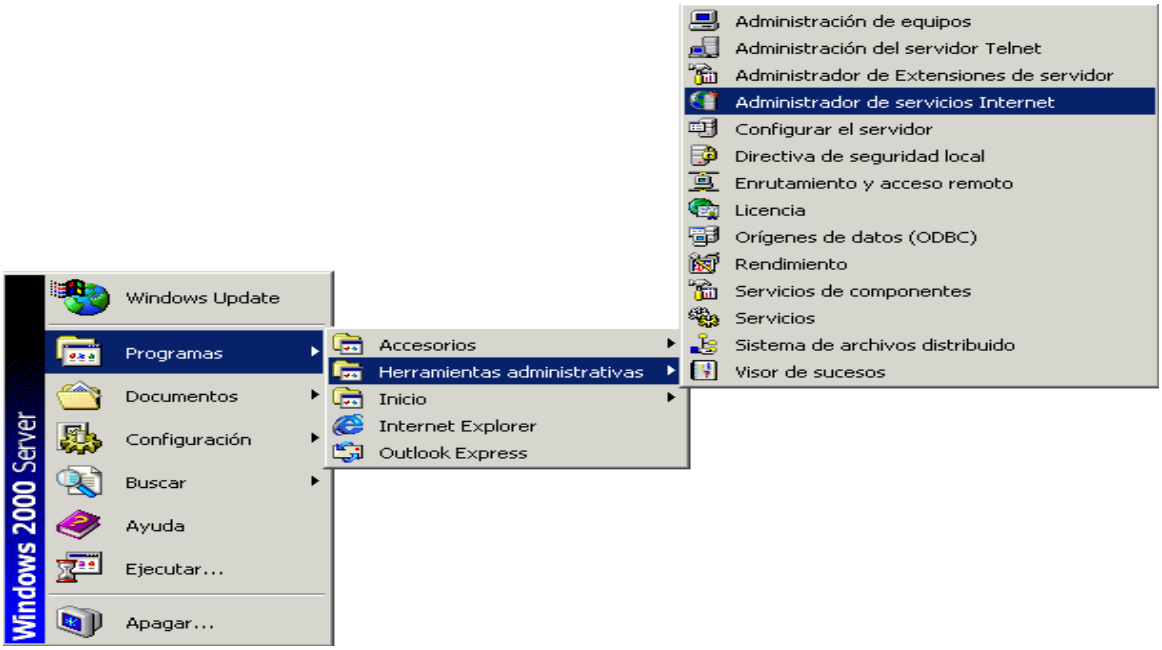

Figura 4.6.-Ruta para activar Internet Information Server (IIS).

Al iniciarse, la consola tendrá este aspecto:

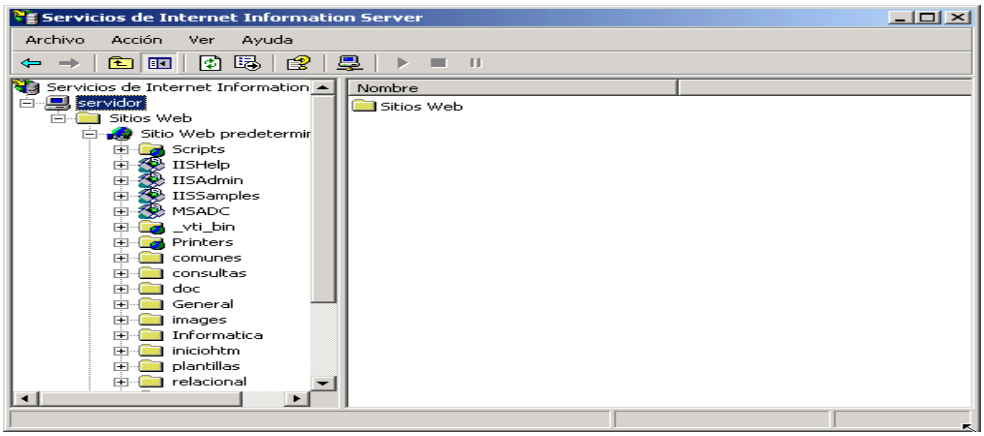

Figura 4.7.-Consola de Internet Information Server (IIS).

Por una parte se tiene un icono con el nombre del equipo que se esta administrando. Si disponemos de más servidores web en la organización se pueden administrar todos desde aquí. Para conectarse a otro bastaría con pulsar con el botón derecho en el título de la parte de la izquierda "Servicios de IIS" y seleccionar la opción "Conectar":

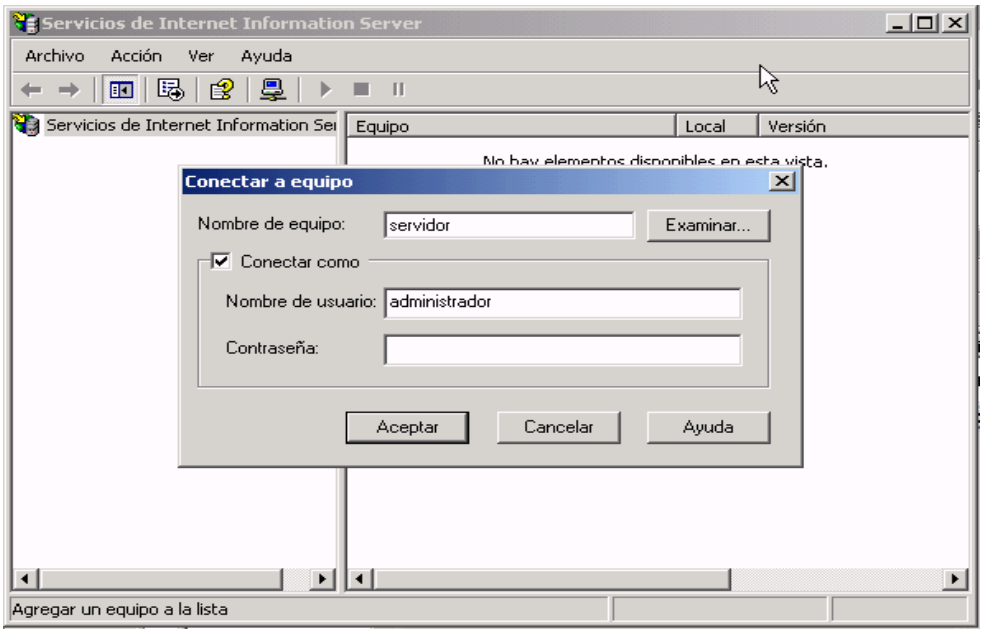

Figura 4.8.-Configuración de Internet Information Server (IIS).

Se introduce en el formulario el nombre del servidor y las credenciales de inicio de sesión si se necesitan. El equipo se conectará y podremos administrar el equipo remoto. Como avance de lo que veremos en este capítulo y en el siguiente se pulsa con el botón derecho en el "Sitio Web Predeterminado" para ver los detalles de este web:

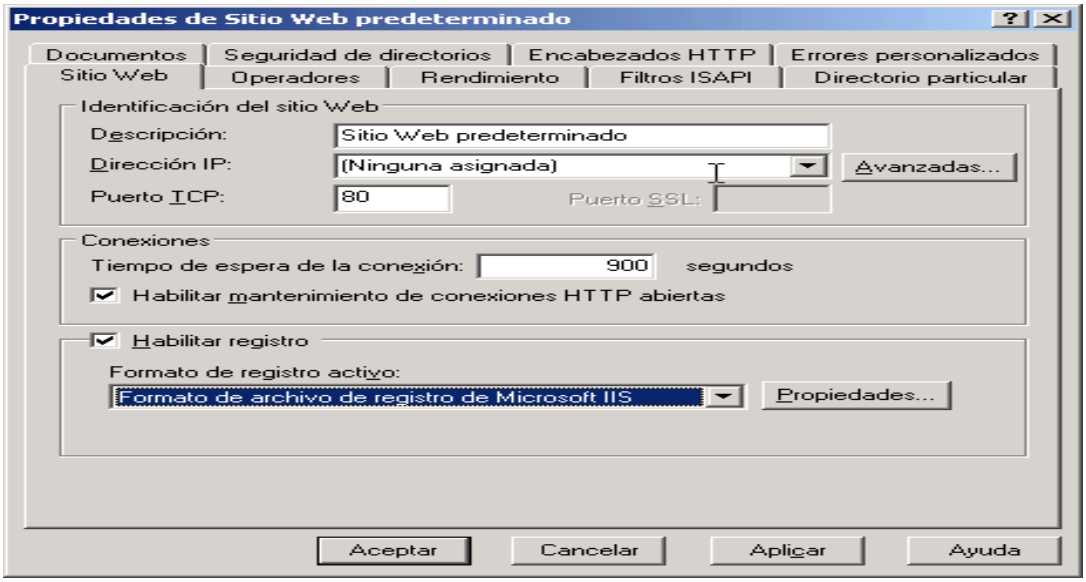

Figura 4.9.-Propiedades de sitio Web predeterminado.

Estas son todas las opciones que tenemos disponibles en el servidor IIS. La mayoría de ellas son conceptos sencillos y con una breve descripción podremos hacer uso de éstas. Antes de empezar a explicar sus detalles vamos a ver los elementos que pueden aparecer en la consola administrativa:

Dentro del Administrador de servicios de Internet se pueden distinguir varios nodos, dependiendo también de la instalación que se haya realizado de IIS 5.0. En la instalación más completa se muestra lo siguiente:

• Sitio FTP predeterminado: Es el sitio FTP del servidor, desde aquí se configura el servicio FTP que ofrece IIS 5.0.

• Sitio Web predeterminado: Es el elemento que más nos va a interesar, desde aquí se configura el servicio Web que ofrece IIS 5.0, incluyendo la configuración de las aplicaciones ASP.

• Sitio Web de administración: Ofrece la posibilidad de administrar IIS 5.0 desde un sitio Web, es decir sin tener instalada la consola administrativa podemos acceder a su administración mediante páginas web.

• Servidor virtual SMTP predeterminado: Representa el servicio de correo de IIS 5.0, se trata del servicio de correo saliente SMTP (Simple Mail Transfer Protocol).

• Servidor virtual NNTP predeterminado: Representa el servicio de noticias de IIS 5.0, se trata del servicio NNTP (Network News Transport Protocol). Es el servicio de Internet conocido como "grupos de noticias" o "newsgroups"

En este capítulo nos vamos a centrar en el sitio Web predeterminado, que representa el sitio Web por defecto del servidor IIS 5.0 y que se corresponde con http://nombreMaquina. Veamos ahora algunos detalles. ¿Cómo es posible que se tengan dos sitios web en un mismo equipo? .Pues sí podemos, se puede ver en la consola que se tienen dos sitios web:

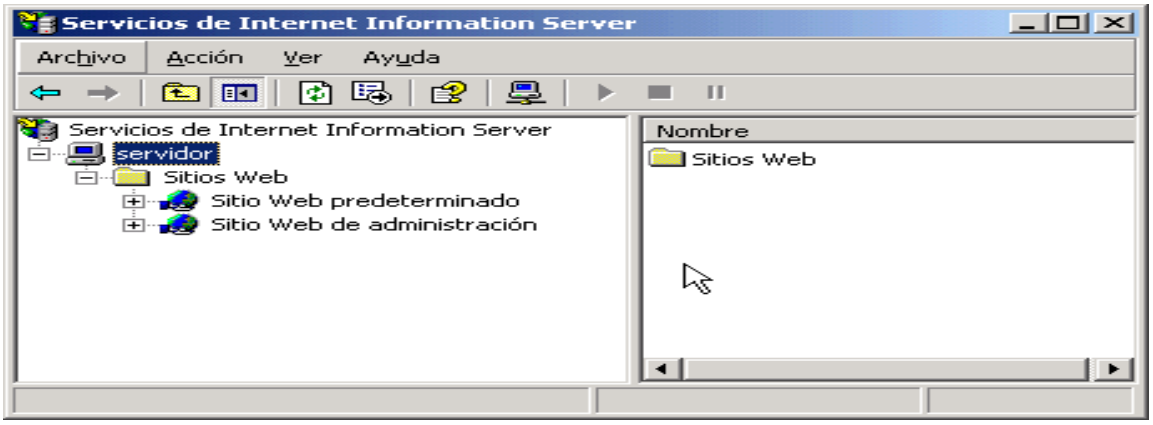

Figura 4.10.-Administración de sitio Web.

Uno es el sitio Web principal, con el que se va a trabajar normalmente y el otro es el sitio web administrativo. ¿Bien, pero cómo se debe acceder a cada uno de ellos? De acuerdo, se sabe que las páginas web (protocolo HTTP) utilizan el puerto 80 de TCP/IP. Esto es el canal de comunicaciones que va a utilizar el navegador con el servidor IIS. Cuando se solicita una página web, el navegador abre una conexión con el servidor indicado por el puerto 80. Si vemos otra vez la página de propiedades del "Sitio Web predeterminado":

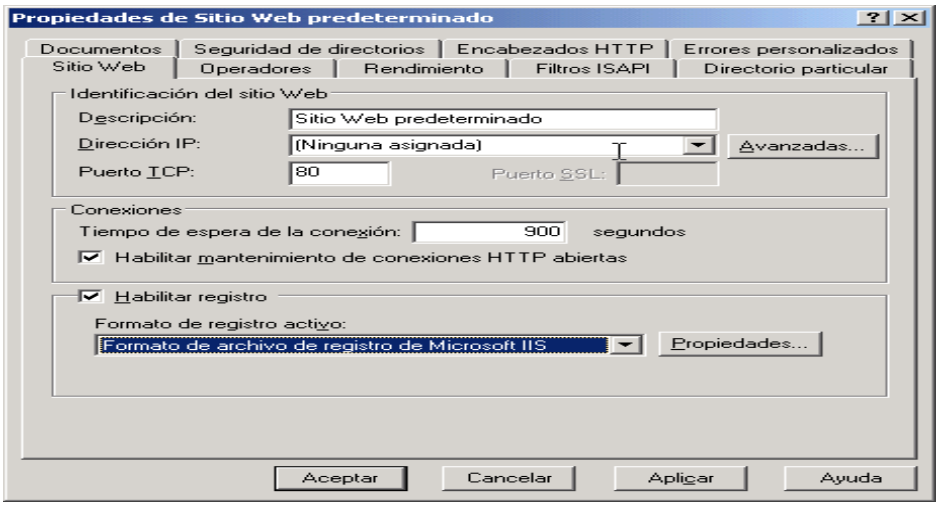

Figura 4.11.-Propiedades de sitio Web predeterminado.

Vemos la página de las propiedades principales del servidor Web. Se observa un título en el campo "Descripción", una dirección IP, que aparece como "Ninguna asignada" y un puerto TCP. Este es el puerto 80, que es estándar para las páginas web. Si se cambia este puerto, al 81 por ejemplo, y escribimos el nombre del servidor en el navegador veremos que no aparece ninguna página porque no puede establecer una conexión a un sitio web que exista en el puerto 81 porque el navegador por defecto busca uno en el 80:

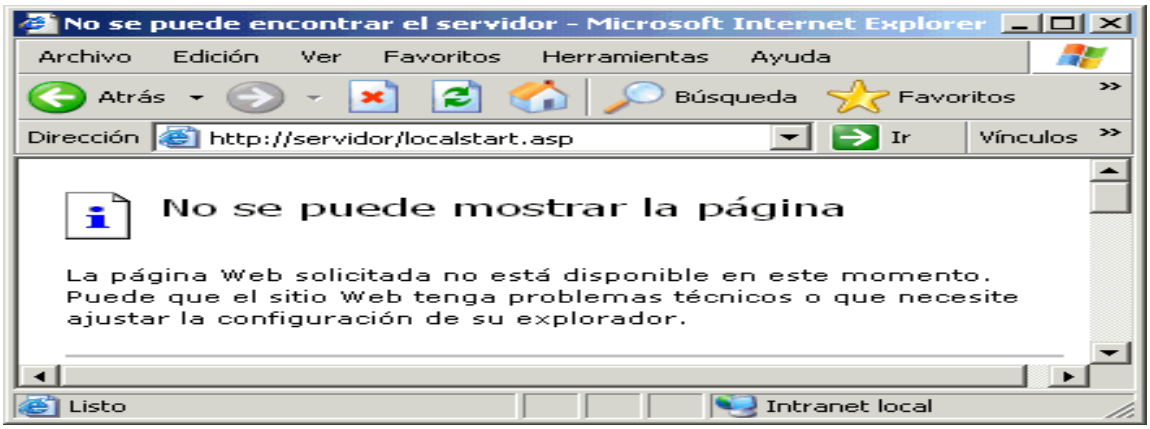

Figura 4.12.-Página de error al cambiar el puerto 80 estándar de las páginas Web.

Cuando se instala un sitio web en un puerto que no es el estándar se debe escribir en la URL a continuación del nombre del servidor el puerto TCP donde se encuentra el sitio web:

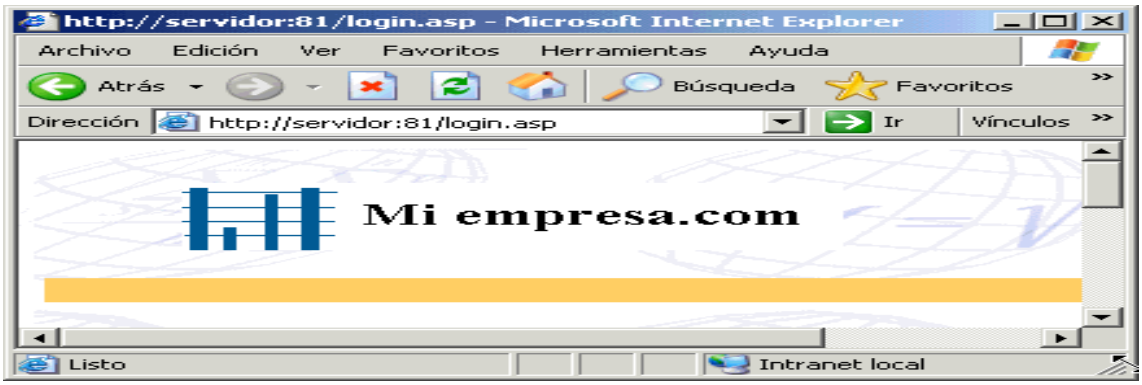

Figura 4.13.-Acceso a una Página que esta instalada en un puerto diferente al puerto estándar de las páginas Web.

Como vemos en este caso en la URL se ha escrito "http://servidor:81" y nos muestra la página de inicio. Pero volvamos a dejarlo como estaba con el 80. Vemos entonces que si se pueden tener varios sitios web, de hecho en la instalación se ha comprobado que se tiene un sitio web predeterminado y uno de administración.

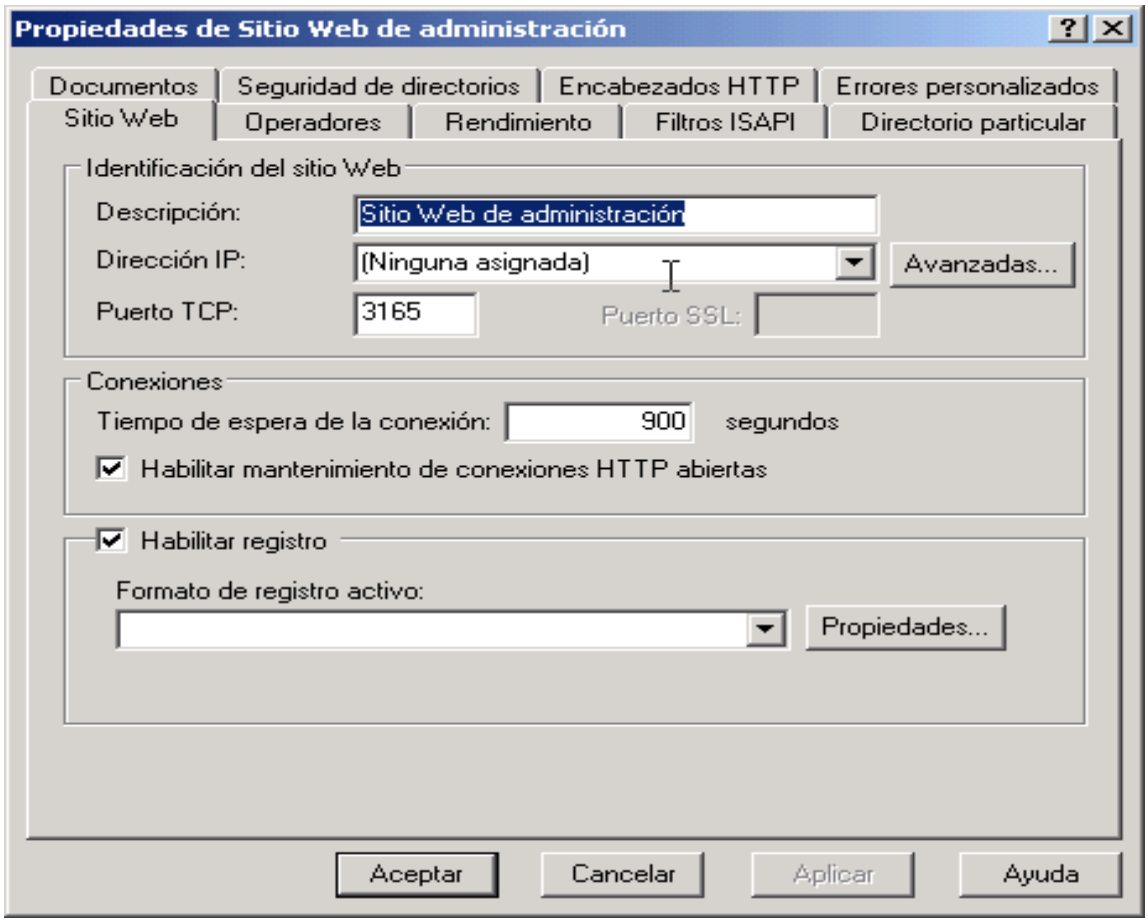

Figura 4.14.-Propiedades de sitio Web administrativo.

Por lo tanto el sitio Web de administración no puede estar en el mismo puerto 80. Como se puede observar en su página de propiedades, en este ejemplo está en el Puerto 3165. Que es el puerto que se debe poner en el navegador para poder acceder a este sitio web:

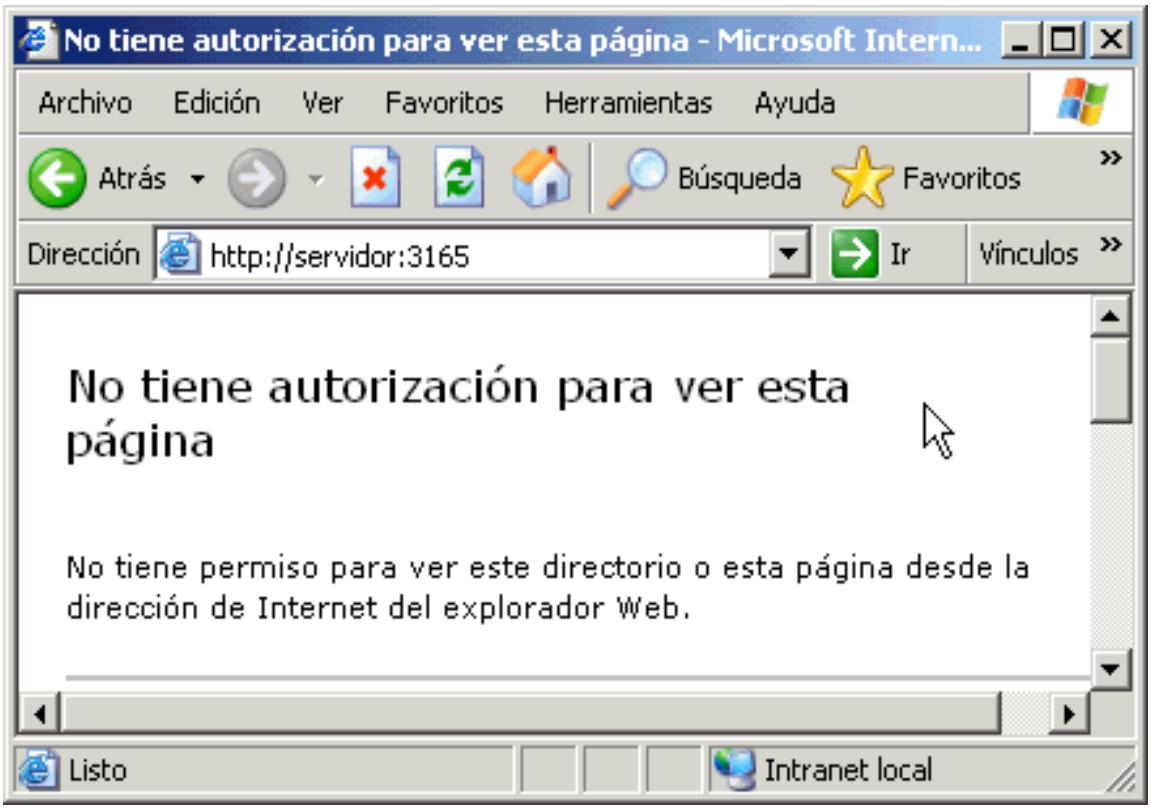

Figura 4.15.-Pàgina del sitio Web administrativo desde un sitio remoto.

Aun así todavía falta algún tipo de permiso. Esto esta bien, hay que darse cuenta que el que pueda llegar a esta página puede administrar completamente el sitio web. Podría borrarlo, desconfigurarlo o introducir una puerta trasera para posibles ataques. Entonces es normal que no sea fácil llegar hasta él. De momento ya hasta que se entre a temas de seguridad sólo va a funcionar desde el propio servidor, así que para probarlo se tienen dos posibilidades:

- Se mueve físicamente hasta el servidor para escribir la dirección URL: Puerto
- Si se esta trabajando con el servidor en local si que nos funcionará.

La página que se muestra tiene las mismas opciones que la consola administrativa:

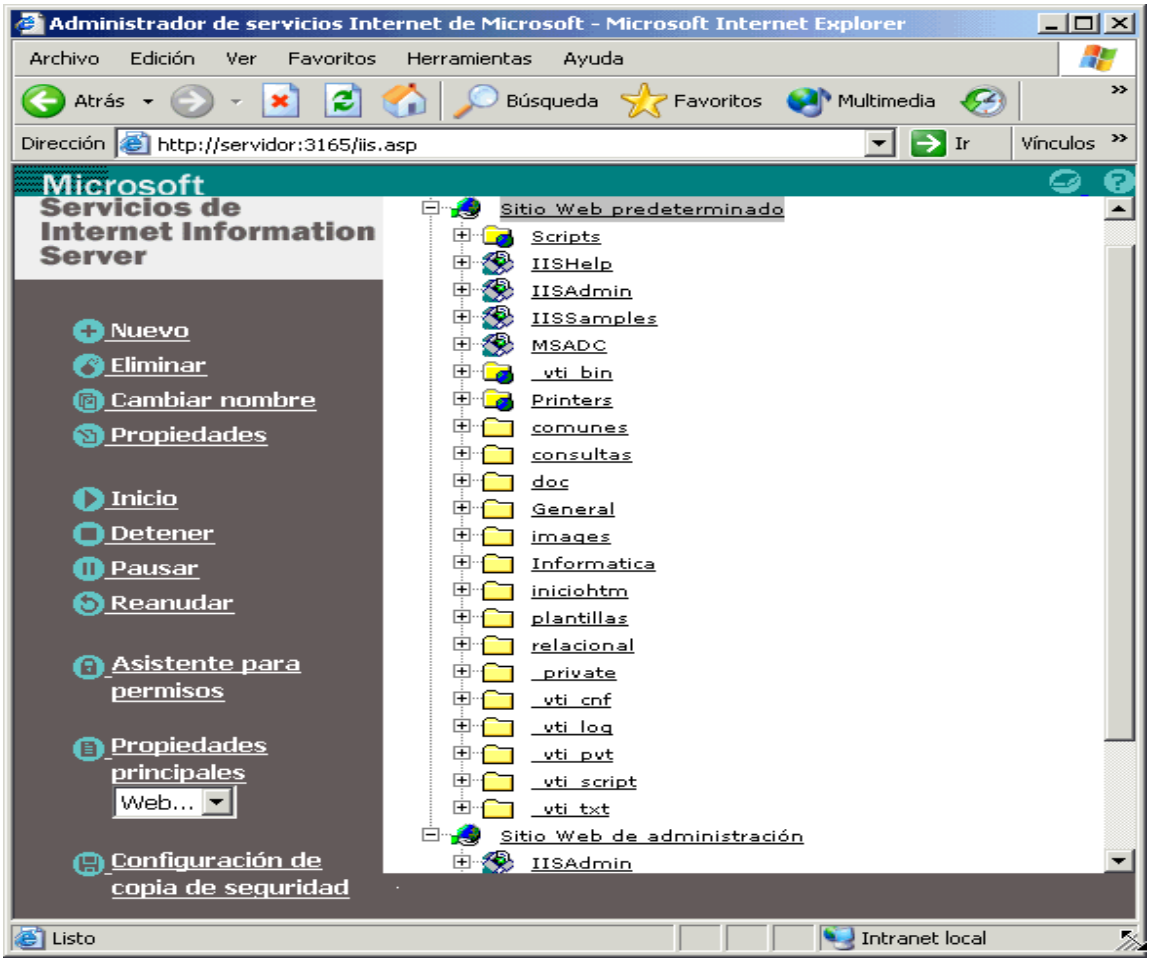

Figura 4.16.-Pàgina del sitio Web administrativo desde el servidor.

Pero por comodidad y por rapidez se hará con la consola. Antes de pasar a conocer qué son los directorios virtuales conozcamos mejor qué son las opciones que aparecen en las propiedades del sitio web.

4.5.- Propiedades del sitio web.

La primera página de propiedades de IIS que aparece al seleccionarlo es esta página:

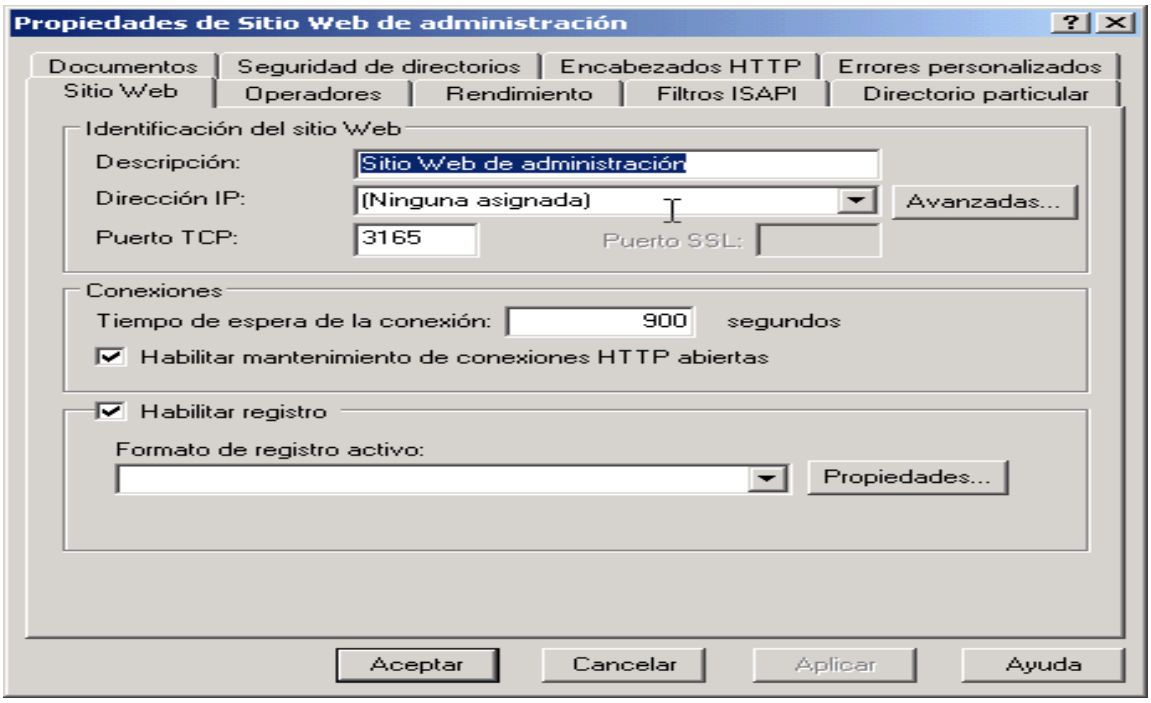

Figura 4.17.-Propiedades de sitio Web administrativo.

En esta ficha, se pueden configurar una serie de parámetros relacionados con la identificación del sitio Web, las conexiones al sitio Web y la forma de registrar los accesos al sitio Web.

En cuanto a la identificación del sitio Web se tienen cuatro parámetros: Descripción, Dirección IP, Puerto TCP y Puerto SSL.

- En descripción se deberá indicar el nombre con el que se identificará el sitio dentro de la consola, no se debe confundir con el nombre de dominio o URL que utilizamos para acceder al sitio Web a través de Internet. De esta forma se podrá cambiar la denominación de sitio Web Predeterminado por la que deseemos
- El siguiente parámetro es la dirección IP que tiene asociada el sitio Web, se puede elegir una de las que tenga asignadas el servidor o bien elegir la opción Todos no asignados, si se elige esta última opción se estará asignando al sitio Web todas las direcciones IP del servidor que se encuentren libres. De esta forma pasa a ser el sitio Web predeterminado.
- El número de puerto normalmente no será necesario modificarlo, por defecto el servicio Web se encuentra en el puerto 80.

- El puerto SSL (Secure Sockets Layer) sólo se debe utilizar para conexiones seguras, basados en certificados de cliente y servidor.
- Se puede indicar el tiempo de espera máximo (time-out) utilizado para establecer una conexión, esto asegurará que se cerrarán todas las conexiones si el protocolo HTTP no puede establecer una conexión desde el cliente en el tiempo especificado, por defecto son 900 segundos.
- Se pude activar el registro del sitio Web seleccionando la opción correspondiente. Se tienen diferentes formatos para guardar la información relativa los accesos al sitio Web. Cada uno de estos formatos definen que datos se van a almacenar y que estructura va a tener el fichero o tabla en la que van a ser almacenados.

4.6.- Los directorios virtuales.

Para empezar, al configurar los sitios Web debe indicar los directorios que contienen los documentos que desea publicar. El servidor Web no puede publicar documentos que no están en los directorios especificados. Por lo tanto, el primer paso para desarrollar un sitio Web debe ser determinar cómo desea organizar los archivos.

Si desea empezar ahora mismo sin tener que crear una estructura especial de directorios y todos los directorios se encuentran en el mismo disco duro del equipo que ejecuta los Servicios de Internet Information Server, puede publicar los documentos inmediatamente si copia los archivos Web en el directorio principal predeterminado, C:\InetPub\Wwwroot.

Cada sitio Web o FTP debe tener un directorio particular. El directorio particular es la ubicación central de las páginas publicadas. Contiene una página principal o archivo de índice que da la bienvenida a los clientes y contiene los vínculos a otras páginas del sitio. El directorio particular se asigna al nombre de dominio del sitio o al nombre del servidor. Por ejemplo, si el nombre del dominio de Internet del sitio es www.microsoft.com y el directorio particular es C:\Website\Microsoft, los exploradores utilizan la dirección URL http://www.microsoft.com para tener acceso a los archivos del directorio particular. En una intranet, si el nombre del servidor es AcctServer, los exploradores utilizan la dirección URL http://acctserver para tener acceso a los archivos del directorio particular.

El directorio particular predeterminado se crea al instalar los Servicios de Internet Information Server y crear un sitio Web nuevo. Veamos la página de propiedades "Directorio particular"

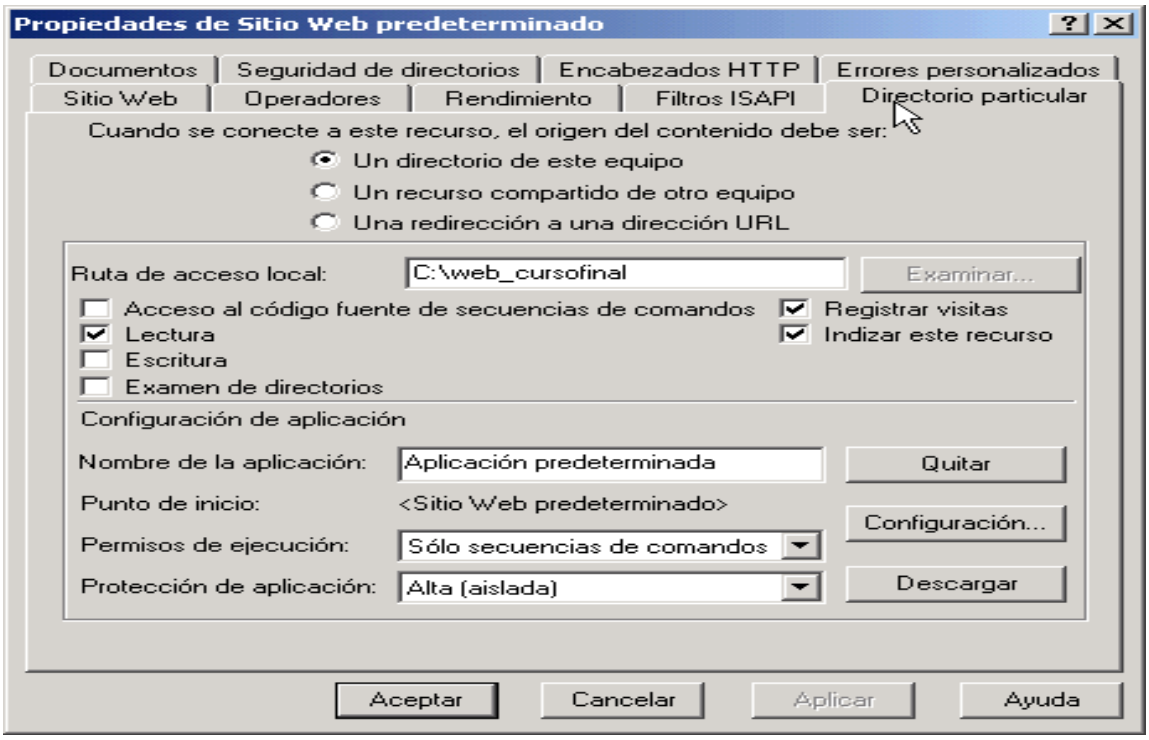

Figura 4.18.-Directorio particular.

En este caso las páginas web las está recogiendo del directorio "c:\web_cursofinal". Podemos hacer ahora una prueba: crea una página web sencilla desde FrontPage y guárdala en un directorio del disco duro. Si elegimos este directorio en esta página propiedades veremos que por fin nos funciona nuestro sitio web. Podremos ver esta página de ejemplo... Una vez probado volvemos a seleccionar nuestro directorio c:\inetpub\wwwroot. Ya veremos el resto de las opciones en el capítulo siguiente. Terminemos con nuestros directorios virtuales...

4.6.1.- ¿Qué es un directorio virtual?

Para publicar desde cualquier directorio que no esté contenido en el directorio particular, debe crear un directorio virtual. Un directorio virtual es un directorio que no está en el directorio particular pero que aparece en los exploradores de los clientes como si estuviera.

Es decir: sabemos que podemos poner páginas web en el directorio "c:\inetpub\wwwroot" y que estas se van a ver inmediatamente escribiendo en el navegador "http://servidor". Un directorio virtual es crear un directorio en nuestra página web pero que apunta físicamente a otra ruta física del disco duro diferente. Por ejemplo podemos crear un directorio virtual que llamaremos "docs" y que apunta a la ruta física "d:\intranet\documentos" para ver esto en el servidor bastaría con escribir: "http:/servidor/docs"

Un directorio virtual tiene un alias, un nombre que los exploradores Web utilizan para tener acceso al directorio. Puesto que el alias suele ser más corto que el nombre de la ruta del directorio, a los usuarios les resulta más cómodo escribirlo. Un alias es más seguro; los usuarios no conocen el lugar del servidor donde están ubicados físicamente los archivos y no pueden utilizar esa información para modificar los archivos. Con los alias es más fácil mover los directorios en el sitio. En lugar de cambiar la dirección URL del directorio, puede cambiar la asignación entre el alias y la ubicación física del directorio.

Otro ejemplo, supongamos que configuramos un sitio Web para el grupo de mercadotecnia en la intranet de la compañía. La tabla siguiente muestra las asignaciones entre las ubicaciones físicas de los archivos y las direcciones URL a través de las cuales se obtiene acceso a los archivos.

Tabla 4.4.- Asignaciones entre las ubicaciones físicas de los archivos y las direcciones URL para obtener acceso a los archivos.

Ubicación Física	**Alias**	**Ruta de la dirección URL**
C:\Inetpub\wwwroot	directorio particular (ninguno)	http://Ventas
\\Servidor2\DatosVentas\ClientesProd	Clientes	http://Ventas/Clientes

C:\Inetpub\wwwroot\Presupuestos	Ninguno	http://Ventas/Presupuestos
C:\Inetpub\wwwroot\EstadoPedidos	Ninguno	http://Ventas/EstadoPedidos
D:\Mrcdtcn\PR	PR	http://Ventas/PR

Los directorios virtuales y los físicos (directorios sin alias) aparecen en el complemento Servicios de Internet Information Server. Un directorio virtual viene indicado por un icono de carpeta con un globo en la esquina. La ilustración siguiente muestra el sitio Web de ejemplo descrito anteriormente; /Clientes y /PR son directorios virtuales:

Figura 4.19.-Sitio Web de ejemplo descrito anteriormente; /Clientes y /PR son directorios virtuales

En un sitio Web simple, puede que no necesite agregar directorios virtuales. Basta con colocar todos los archivos en el directorio particular del sitio. Si tiene un sitio complejo o desea especificar diferentes direcciones URL para distintas partes del sitio, puede agregar tantos directorios virtuales como sea necesario. En cualquier caso es un tema interesante.
A menudo nos encontraremos con que instalamos una utilidad para nuestra Intranet y la documentación la instala directamente en un directorio virtual, de esta forma está mas fácil y accesible que un fichero .htm tradicional.

4.6.2.- Crear directorios virtuales.

Si su sitio Web contiene archivos que se encuentran en un directorio diferente del directorio particular o en otros equipos, debe crear directorios virtuales para incluir esos archivos en el sitio Web. Para utilizar un directorio de otro equipo, debe especificar su nombre según la Convención de nomenclatura universal (UNC) e indicar un nombre de usuario y una contraseña para los permisos de acceso.

Para crear un directorio virtual

1. En la consola administrativa, seleccione el sitio Web o FTP al que desee agregar un directorio.
2. Haga clic en el menú Acción, seleccione Nuevo y haga clic en Directorio virtual.
3. Utilice el Asistente para crear un directorio virtual para completar esta tarea.

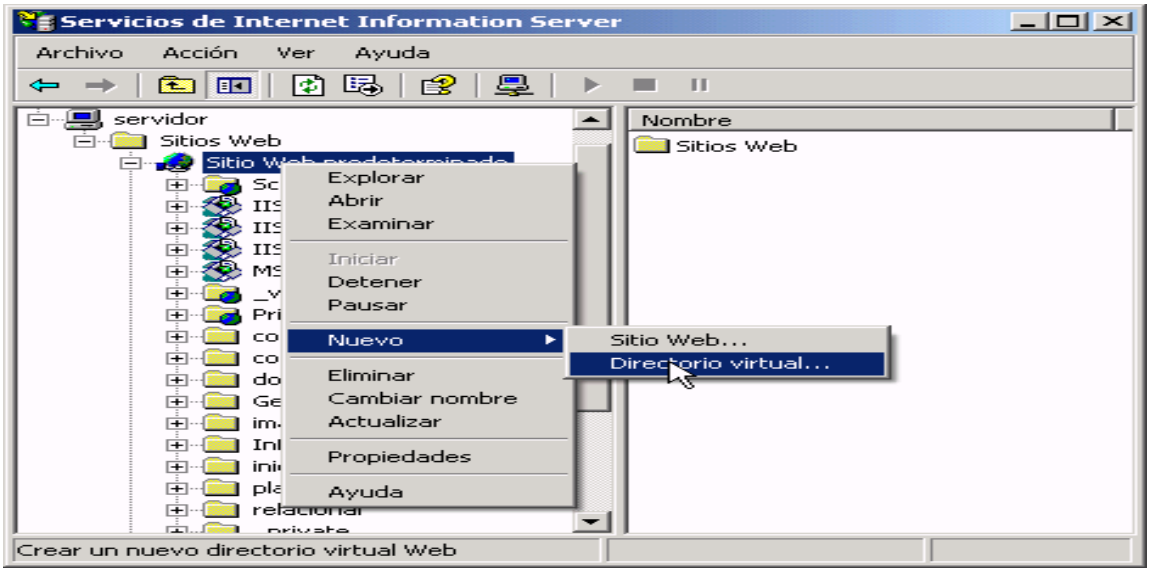

Figura 4.20.-Creaciòn de un Directorios Virtual.

A continuación de la pantalla de bienvenida aparecerá una ventana preguntando por el alias que tendrá el sitio Web, es decir el nombre que escribiremos en el navegador: http://servidor/alias

Luego tendremos que asociarlo con una ruta física del disco duro, seleccionamos un directorio o ruta y finalmente pulsamos en "siguiente". Por último indicaremos los permisos de ejecución para este directorio. Estos permisos los veremos con detalle en el siguiente capítulo.

4.6.3.- Eliminar un directorio virtual.

1. En la consola administrativa, seleccione el directorio virtual que desee eliminar.
2. Haga clic en el menú Acción y, a continuación, en Eliminar. Al eliminar un directorio virtual no se elimina el directorio o los archivos físicos correspondientes sólo esta conexión lógica.

4.7.-IIS avanzado – FrontPage.

A continuación veremos con detalle en las opciones avanzadas de nuestro servidor web: Internet Information Server. Una vez configurado correctamente veremos su integración con FrontPage. En ese punto prácticamente realizaremos todo el trabajo con este programa y no será necesaria la utilización de la administración de IIS para ninguna opción, exceptuando los cambios de funcionamiento de IIS.
Para ver todas sus opciones haremos como el capítulo anterior, veremos las fichas de la página de propiedades e iremos profundizando en cada una de las opciones. Finalmente dedicaremos una sección a la integración de FrontPage con Internet Information Server.

4.8.- Sitio Web.

Esta hoja de propiedades se utiliza para configurar básicamente el sitio web:

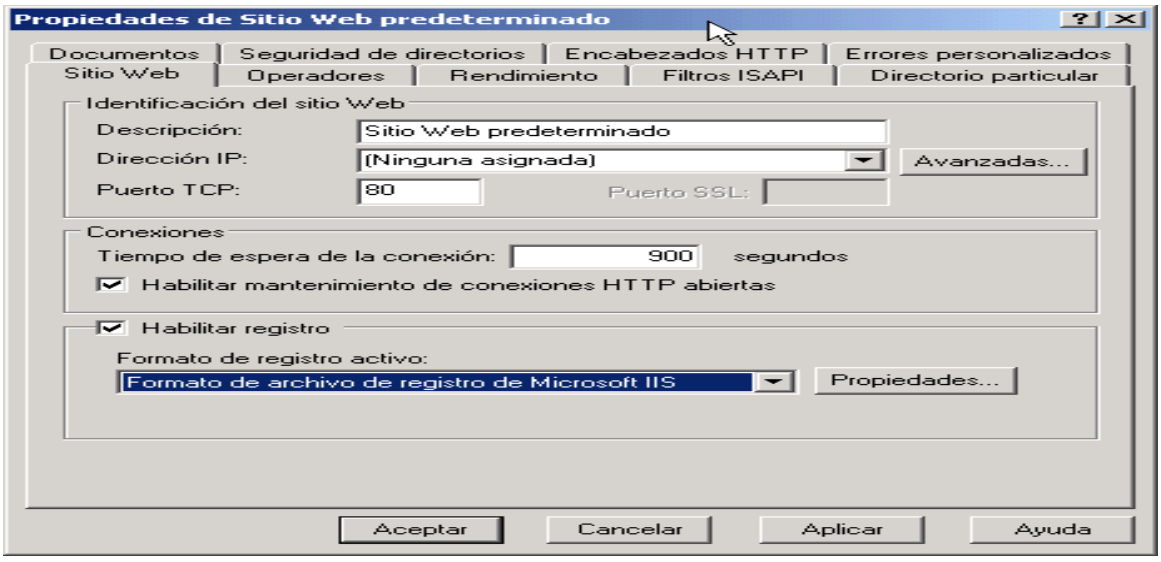

Figura 4.21.-Propiedades del sitio Web.

Ya vimos la mayoría de los apartados en el tema anterior pero nos falta uno realmente importante: el registro, opción que se activa en la parte inferior de la ficha.

Es posible recopilar información acerca de la actividad de los usuarios si habilita registros para los sitios Web. La información se almacena en archivos ASCII. Este registro tiene muchas posibilidades y supera el ámbito de las características de registro de sucesos o de supervisión del rendimiento de Windows. Los registros pueden incluir información referente a quién ha visitado el sitio, qué ha visto el visitante y cuándo se vio la información por última vez. Puede utilizar los registros para evaluar la popularidad del contenido o identificar los cuellos de botella de la información.

Puede configurar sus sitios Web o FTP para que graben entradas de registro generadas por la actividad de los usuarios y del servidor. Los datos de registro de IIS pueden ayudar a regular el acceso al contenido, evaluar la popularidad del contenido, planear los requisitos de seguridad y resolver problemas potenciales en los sitios Web o FTP. El registro de actividad del sitio IIS no se debe confundir con el registro de sucesos efectuado por Windows XP ó 2000, que se muestra con el Visor de sucesos. El registro en IIS es más extenso y lo veremos a continuación.

4.8.1.- El proceso de registro.

El registro de un sitio Web o FTP se realiza mediante unos módulos que funcionan independientemente de las demás actividades del servidor. Puede elegir el formato de los

registros para cada sitio Web o FTP individual. Si está habilitado el registro en un sitio, puede habilitarlo o deshabilitarlo individualmente para cada uno de sus directorios.

Cada formato de registro utiliza una zona horaria diferente como base para las horas mostradas en los registros. El formato extendido W3C utiliza el Horario universal coordinado (UTC), anteriormente llamado hora del meridiano de Greenwich. Los otros formatos utilizan la hora local. Las horas mostradas en los archivos de registro reflejan la hora que el servidor utiliza para procesar las peticiones y las respuestas. Estas horas no reflejan el tiempo transcurrido en la red hasta llegar al cliente ni el tiempo de proceso del cliente.

4.8.2.- Formatos de archivo de registro.

Puede elegir el formato que el servidor Web utiliza para registrar la actividad de los usuarios. Se dispone de los siguientes formatos:

1. Formato de archivo de registro extendido W3C
2. Formato de registro de Microsoft IIS
3. Formato del archivo de registro común NCSA

El formato de archivo de registro extendido W3C, el formato de archivo de registro Microsoft IIS y el formato de archivo de registro NCSA son todos formatos de texto ASCII. El formato extendido W3C y el formato NCSA registran datos con formato de año de cuatro dígitos. El formato de Microsoft IIS utiliza un formato de dos dígitos para el año 1999 y anteriores y un formato de cuatro dígitos para los años posteriores. El formato de registro que se proporciona con Microsoft IIS asegura la compatibilidad con versiones anteriores de IIS. Únicamente se puede utilizar el formato de archivo de registro extendido W3C para crear formatos de registro personalizados con los campos precisos que se necesiten.

A título informativo comentaremos los tres tipos de registro que existen en IIS:

1. Formato de archivo de registro extendido W3C

El formato extendido W3C es un formato ASCII que puede personalizarse con diversos campos diferentes. Puede incluir campos que considere importantes y limitar al mismo tiempo el tamaño del registro si omite los campos que no desea. Los campos están separados por espacios. La hora se registra como UTC (Horario universal coordinado).

En el ejemplo siguiente se muestran líneas de un archivo que incluye los campos siguientes: Hora, Dirección IP del cliente, Método, Recurso (URL) visitado, Estado del protocolo y Versión del protocolo.

#Software: Servicios de Internet Information Server 5.1 de Microsoft

#Version: 1.0

#Fecha: 1998-05-02 17:42:15

#Campos: time c-ip cs-method cs-uri-stem sc-status cs-version

17:42:15 172.16.255.255 GET /default.htm 200 HTTP/1.0

La entrada anterior indica que el 2 de mayo de 1998, a las 5:42 p.m., UTC, un usuario con HTTP versión 1.0 y dirección IP 172.16.255.255 emitió un comando GET de HTTP para el archivo \Default.htm. La petición se resolvió sin errores. El campo #Fecha: indica cuándo se hizo la primera entrada de registro, que es cuando se creó el registro. #Versión: indica que se utilizó el formato de registro W3C.

Se puede seleccionar cualquiera de los campos, pero puede que algunos no tengan información disponible para algunas peticiones. Para aquellos campos seleccionados que no tengan información aparecerá un guión (—) en el campo como marcador de posición.

Al seleccionar este formato hemos dicho que podemos personalizar sus campos. Si pulsamos en el botón "Propiedades" nos aparecerá una pantalla cuya segunda ficha será como esta:

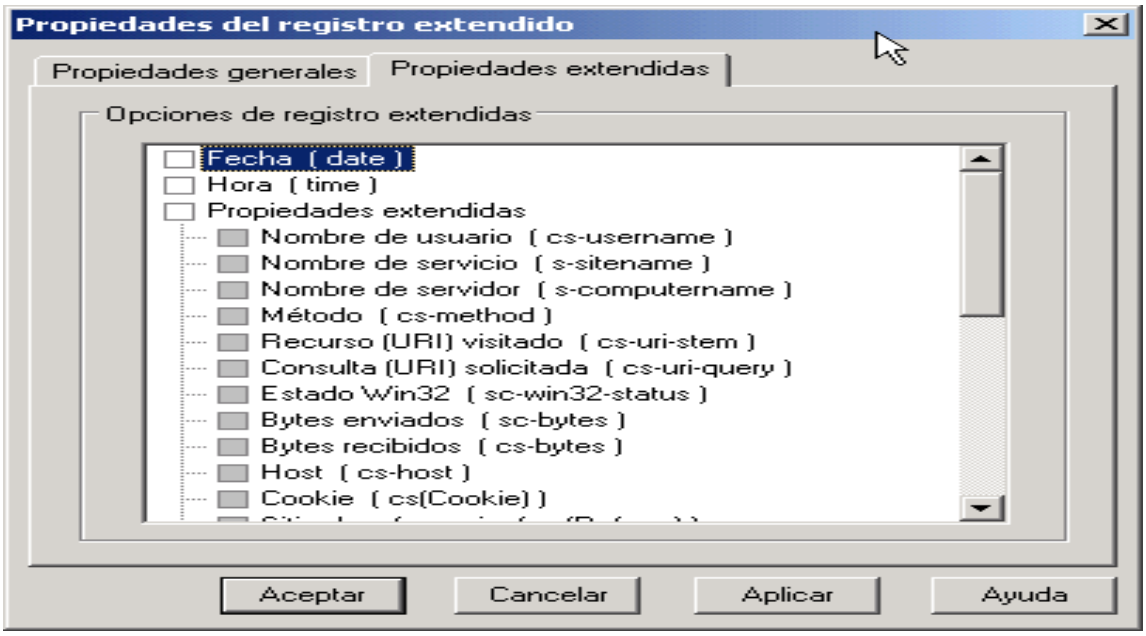

Figura 4.22.-Opciones de registro extendido.

Esta pantalla permite indicar que campos queremos que figuren en el registro.

2. Formato de registro de Microsoft IIS

El formato de Microsoft IIS es un formato ASCII fijo (no puede personalizarse) pero registra más datos que el formato común NCSA. El formato de Microsoft IIS incluye elementos básicos como la dirección IP del usuario, el nombre de usuario, la fecha y la hora de petición, el código de estado de servicio y el número de bytes recibidos. Además, incluye elementos detallados como el tiempo transcurrido, el número de bytes enviados, la acción (por ejemplo, una descarga realizada con un comando GET) y el archivo de destino. Los elementos se separan con comas, por lo que leer el formato resulta más sencillo que con los demás formatos ASCII, que utilizan espacios como separadores. La hora de registro es la local.

Al abrir un archivo con formato Microsoft IIS en un editor de textos, las entradas serán similares a las de los ejemplos siguientes:

192.168.114.201, —, 03/20/98, 7:55:20, W3SVC2, VENTAS1, 192.168.114.201, 4502, 163, 3223, 200, 0, GET, /DeptLogo.gif, —,

172.16.255.255, anónimo, 03/20/98, 23:58:11, MSFTPSVC, VENTAS1, 192.168.114.201, 60, 275, 0, 0, 0, PASS, /intro.htm, —,

En las tablas siguientes se interpretan las entradas anteriores. La fila superior de cada tabla proviene de la segunda instancia del sitio Web (que aparece en "Servicio" como W3SVC2) y la fila inferior de la primera instancia del sitio FTP (que se indica en "Servicio" como MSFTPSVC1). El ejemplo se presenta en tres tablas por la limitación de ancho de página.

Tabla 4.5.-Registros extendidos 1.

Bt	**Nombre del usuario**	**Fecha**	**Hora**	**Servicio instancia**	**Uso y resultado**
192.168.114.201	—	03/20/98	7:55:20	W3SVC2	VENTAS1
172.16.255.255	anónimo	03/20/98	23:58:11	MSFTPSVC1	VENTAS1

Tabla 4.6.-Registros extendidos 2.

Dirección IP del servidor	**Tiempo empleado**	**Bytes enviados**	**Bytes recibidos**	**Código de estado de servicio**	**Código de estado de Windows**
192.168.114.201	4502	163	3223	200	0
172.16.255.255	60	275	0	0	0

Tabla 4.7.-Registros extendidos 3.

Tipo de solicitud	**Destino de la operación**	**Parámetros**
GET	/DeptLogo.gif	—
[376] PASS	/intro.htm	—

En el ejemplo, la primera entrada indica que un usuario anónimo, con la dirección IP 192.168.114.201, envió un comando GET de HTTP para el archivo de imagen /DeptLogo.gif a las 7:55 a.m. del 20 de marzo de 1998, desde un servidor llamado

VENTAS1 que tiene la dirección IP 172.21.13.45. La petición HTTP de 163 bytes ha tenido un tiempo de proceso de 4502 milisegundos (4,5 segundos) y devolvió, sin errores, 3223 bytes de datos al usuario anónimo.

En el archivo de registro, todos los campos terminan en coma (,). Un guión (—) actúa como marcador de posición si no hay un valor válido para un campo determinado.

3. Formato del archivo de registro común NCSA

El formato común NCSA es un formato ASCII fijo (no puede personalizarse), disponible para sitios Web, pero no para sitios FTP. Registra información básica acerca de las peticiones de los usuarios, como nombre de host remoto, nombre de usuario, fecha, hora, tipo de petición, código de estado HTTP y número de bytes enviados por el servidor. Los elementos están separados con espacios en blanco y la hora de registro es la local.

Al abrir un archivo con formato común NCSA en un editor de textos, las entradas serán similares a las del ejemplo siguiente:

172.21.13.45 — REDMOND\fred [08/Apr/1997:17:39:04 -0800] "GET /scripts/iisadmin/ism.dll?http/serv HTTP/1.0" 200 3401

En las tablas siguientes se interpreta la entrada de ejemplo anterior. Se utilizan dos tablas por la limitación de ancho de página.

Tabla 4.8.-Registros extendidos con limitación de ancho de página 1.

Nombre de host remoto	**Nombre de inicio de sesión remota**	**Nombre de usuario**	**Fecha**	**Hora y diferencia con GMT**
172.21.13.45	—	REDMON/fred	08 de abril de 1997	17:39:10 -0800

Tabla 4.9.- Registros extendidos con limitación de ancho de página 2.

Petición/Versión	**Código de estado de servicio**	**Bytes enviados**
GET /scripts/iisadmin/ism.dll?http/serv HTTP/1.0	200	3401

La entrada indica que un usuario llamado fred del dominio REDMON, con la dirección IP 172.21.13.45, envió un comando GET de HTTP (es decir, descargó un archivo) a las 5:39 p.m. del 8 de abril de 1997. La petición devolvió, sin errores, 3401 bytes de datos al usuario fred.

4.8.3.- Tamaño de archivo de registro y creación de nuevos archivos de registro

Cuando está habilitado el registro de IIS, como lo está de manera predeterminada, se generan nuevas entradas de registro siempre que un usuario tiene acceso al servidor. Esto produce un incremento progresivo del tamaño del archivo de registro o del número de archivos de registro. Puede necesitar equilibrar la recopilación de datos detallados con la necesidad de limitar los archivos a un número y tamaño fáciles de administrar. IIS ofrece dos opciones para administrar la generación de datos de registro y la creación de nuevos archivos de registro.

Una forma de administrar los datos de registro es personalizar el registro extendido W3C de modo que sólo se recopilen los datos que se necesitan. Otra opción para administrar archivos de registro es limitar el tamaño del registro mediante el cambio de la frecuencia de creación del archivo de registro. Esta opción aparece pulsando el botón Propiedades:

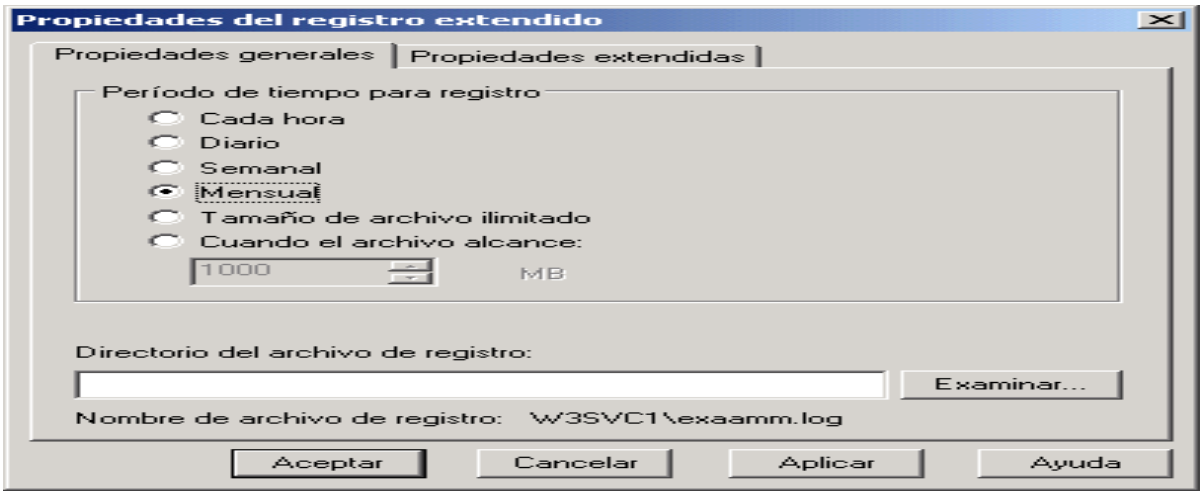

Figura 4.23.-Periodo de tiempo para registro.

Los archivos de registro son simplemente archivos ASCII (de texto). Si ha creado muchos archivos pequeños y prefiere uno grande, puede combinarlos como haría con cualquier archivo ASCII.

Si el servidor se queda sin espacio en disco cuando IIS intenta agregar una entrada de registro a un archivo, el registro de IIS se cierra. Al mismo tiempo, en el registro de aplicación del Visor de sucesos de Windows, se registra un suceso. Cuando vuelve a haber espacio disponible en disco, se reanuda el registro de IIS. Esto hace que se registre un suceso adicional en el registro de aplicación del Visor de sucesos de Windows.

4.8.4.- Nombres de archivo de registro.

En los nombres de los archivos de registro se utilizan las primeras letras para representar el formato y los números restantes para indicar el marco horario o la secuencia del registro. Consulta la tabla siguiente para obtener más información. Las letras en cursiva representan dígitos: nn para dígitos secuenciales, aa para el año, mm para el mes, ss para la semana del mes, dd para el día y hh para la hora en formato de 24 horas (es decir, 17 es 5:00 p.m.).

Tabla 4.10.-Formato de registros.

Formato	**Criterio para nuevo registro**	**Patrón de nombre de archivo**
Formato de registro de Microsoft IIS	Por el tamaño del archivo	inetsvnn.log
	Cada hora	inaammddhh.log
	Diario	inaammdd.log
	Semanal	inaammss.log
	Mensual	inaamm.log
Formato del archivo de registro común NCSA	Por el tamaño del archivo	ncsann.log
	Cada hora	ncaammddhh.log

	Diario	ncaammdd.log
	Semanal	ncaammss.log
	Mensual	ncaamm.log
Formato de archivo de registro extendido W3C	Por el tamaño del archivo	extendnn.log
	Cada hora	exaammddhh.log
	Diario	exaammdd.log
	Semanal	exaammss.log
	Mensual	exaamm.log

4.9.- Directorio particular.

Esta hoja de propiedades es utilizada para configurar el directorio de publicación del sitio Web:

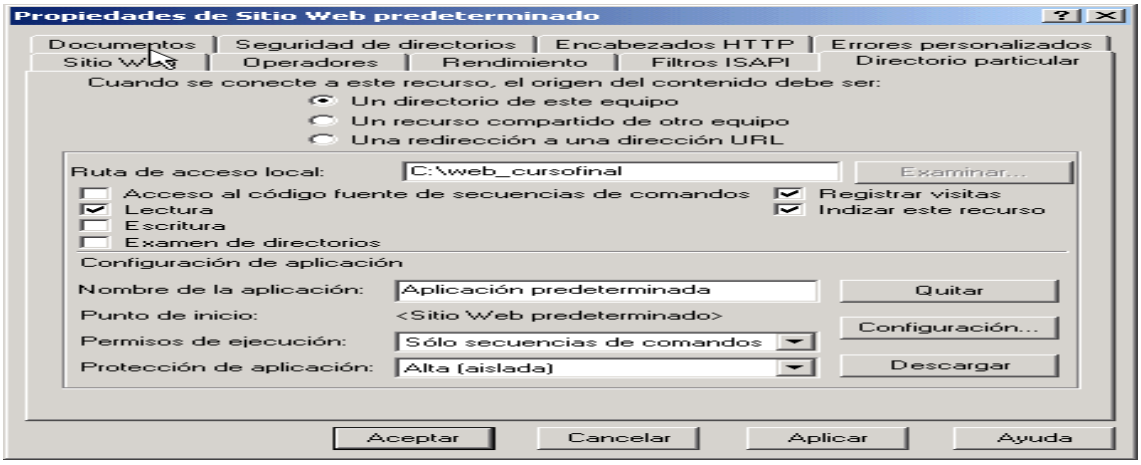

Figura 4.24.- Configuración del directorio de publicación del sitio Web.

4.9.1.- Origen del web.

La primera parte hace referencia a la ubicación de las páginas web. Ya vimos en el capítulo anterior cómo asociábamos nuestro web con un directorio físico del disco duro, e incluso de directorios virtuales con directorios. Las tres opciones posibles son:

- Un directorio de este equipo: "c:\inetpub\wwwroot"
- Un recurso compartido de otro equipo. Si seleccionamos esta opción debemos indicar la ruta UNC \\servidor\recurso. Si además debemos identificarnos en ese directorio pulsaremos en el botón "conectar como" que se mostrará al elegir esta opción:

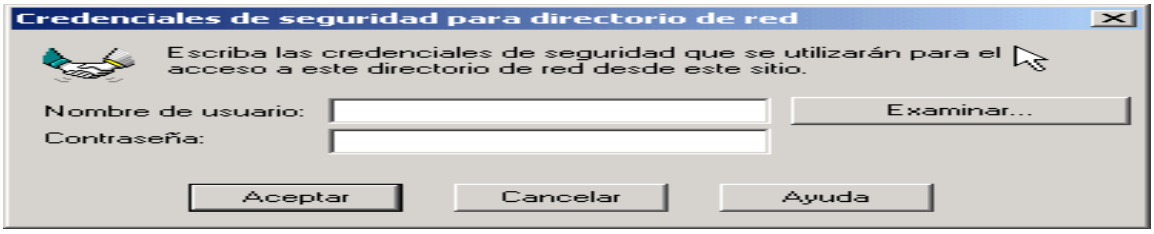

Figura 4.25.-Credenciales de seguridad para directorio de red.

- Poco utilizada: redirección a una URL. Redirige un directorio virtual a la dirección URL de destino sin agregar ninguna parte de la dirección URL original. Puede utilizar esta opción para redirigir un directorio virtual completo a un archivo. Por ejemplo, para redirigir al archivo Predeter.htm en el directorio particular todas las peticiones realizadas al directorio virtual /scripts, escriba /Predeter.htm en el cuadro de texto Redirigir a y seleccione esta opción

4.9.2.- Permisos de ejecución.

Existen varias formas de dar permiso de acceso al sitio web:

- Acceso al código fuente de secuencias de comandos. Selecciona esta opción para permitir que los usuarios tengan acceso al código fuente si disponen de los permisos

de escritura o de lectura. El código fuente incluye las secuencias de comandos en aplicaciones ASP.

- Lectura. Esta opción permite que los usuarios lean o descarguen archivos o directorios y sus propiedades asociadas.
- Escritura. Permitir que los usuarios carguen archivos y sus propiedades asociadas en un directorio con este permiso del servidor o para cambiar el contenido de un archivo con este permiso. La escritura sólo se puede realizar con un explorador que admita la característica PUT del estándar de protocolo HTTP 1.1.
- Examinar directorios. Esta opción permite que el usuario vea una lista con formato de hipertexto de los archivos y subdirectorios de este directorio virtual. Los directorios virtuales no aparecen en las listas de directorios. Los usuarios deben conocer su alias. Importante El servidor Web presentará el mensaje de error "Acceso prohibido" en el explorador Web del usuario si éste intenta tener acceso a un archivo o directorio y las dos condiciones siguientes se cumplen:
    - La opción Examinar directorios está deshabilitada.
    - El usuario no especifica un nombre de archivo, como NombreArchivo.htm.
- Registrar visitas. Es opción registra las visitas de este directorio en un archivo de registro. Las visitas sólo se registran si está habilitado el registro para este sitio Web.
- Indizar este recurso. Selecciona esta opción para que Servicios de Microsoft Index Server incluya este directorio en un índice de texto del sitio Web.

4.9.3.- Configuración de la aplicación.

Esta es la parte que enlaza el mundo ASP con el IIS. Una aplicación es la capacidad del IIS para ejecutar secuencias de comandos como ASP. Es decir si esta sección está desactivada no funcionarán nuestra páginas ASP

Una aplicación es un archivo que se ejecuta dentro de un conjunto definido de directorios de un sitio Web. Al crear una aplicación, el complemento IIS se usa para designar el directorio de punto de inicio de la aplicación, también denominado raíz de la aplicación, en el sitio Web. Cada archivo y subdirectorio incluido en este directorio del sitio Web se considera parte de la aplicación hasta llegar al directorio de punto de inicio de otra

aplicación. Por tanto, los límites de los directorios permiten definir el alcance de las aplicaciones.

En el complemento IIS, el punto de inicio de una aplicación aparece indicado con un icono en forma de paquete. En el ejemplo siguiente se muestra una aplicación con un directorio de punto de inicio llamado /SiteAdmin:

Figura 4.26.- Aplicación con un directorio de punto de inicio llamado /SiteAdmin.

Los archivos de los directorios \Login, \Order y \SetupDB se consideran parte de la aplicación /SiteAdmin.

Por lo tanto puede haber más de una aplicación por cada sitio Web. El sitio Web predeterminado creado al instalar Servicios de Internet Information Server es un punto de inicio de aplicaciones. Esto es importante porque cuando comencemos a construir páginas ASP necesitaremos saber el ámbito de la aplicación para manejar nuestras variables. El concepto de aplicación es muy sencillo, simplemente es dividir nuestro web en "sitios independientes" donde cada uno puede tener sus variables y programas ejecutándose. Muchas veces nos encontraremos con que sólo necesitamos una "aplicación web" que coincide con el "Sitio Web predeterminado"

Resumiendo, sólo necesitamos indicar un nombre para la aplicación y con esto IIS creará internamente la estructura necesaria para que pueda ejecutar páginas ASP entre otras.

4.9.3.1.-Protección de aplicaciones.

IIS 5.1 ofrece tres grados de protección de aplicaciones. La protección de aplicaciones se refiere al proceso en el que se ejecutan las aplicaciones. En IIS 4.0, se podían configurar las aplicaciones para ejecutarse en el mismo proceso como servicios Web (Inetinfo.exe) o en un proceso separado de los servicios Web (DLLHost.exe). En IIS 5.0 y 5.1, hay una tercera

opción: las aplicaciones se pueden ejecutar en un proceso agrupado (otra instancia de DLLHost.exe).

Estas opciones proporcionan varios grados de protección para situaciones en las que una aplicación que funciona de forma incorrecta puede tener un error de modo que el proceso en el que se ejecuta deje de responder. De forma predeterminada, los servicios Web (Inetinfo.exe) se ejecutarán en su propio proceso y otras aplicaciones lo harán en un único proceso agrupado (DLLHost.exe). A continuación, puede establecer que las aplicaciones con prioridad alta se ejecuten como procesos aislados (otra instancia de DLLHost.exe). Por motivos de rendimiento, no se deben ejecutar más de 10 aplicaciones separadas.

El gráfico siguiente ilustra la hoja de propiedades usadas para establecer las propiedades de protección de la aplicación.

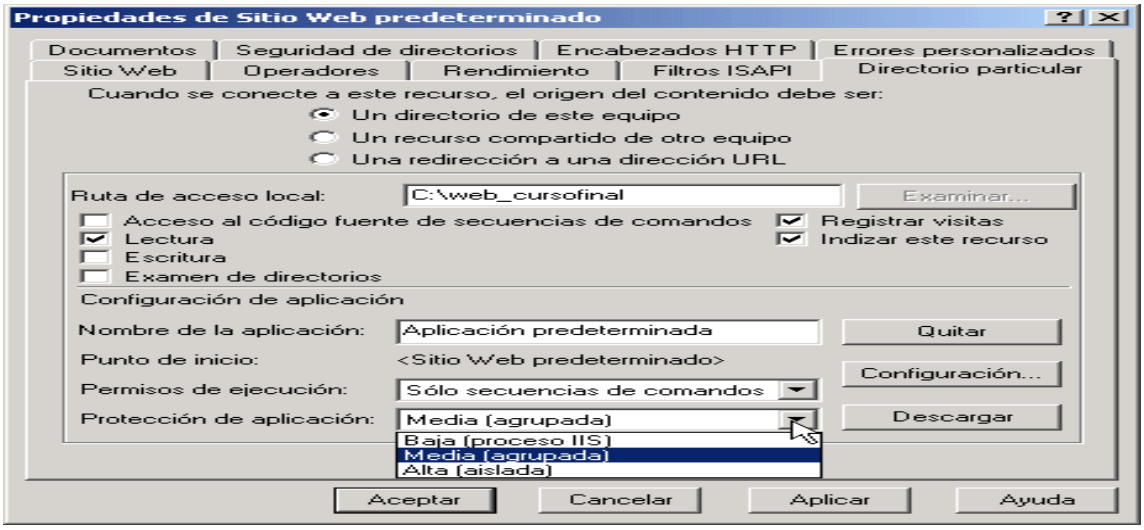

Figura 4.27.-Propiedades del directorio particular.

La protección de aplicaciones sólo puede establecerse en un directorio de inicio de la aplicación.

4.9.3.2.-Rendimiento de la aplicación.

Hay un equilibrio entre el rendimiento y el grado de protección de la aplicación. Las aplicaciones que se ejecutan en procesos de servicios Web (Inetinfo.exe) obtienen un rendimiento superior, pero también existe un mayor riesgo de que una aplicación que no

funciona correctamente pueda hacer que los servicios Web dejen de estar disponibles. La configuración recomendada es ejecutar inetinfo.exe en su propio proceso, ejecutar aplicaciones decisivas en sus propios procesos y ejecutar el resto de las aplicaciones en un proceso agrupado y compartido.

Observaciones:

- Para detener una aplicación y descargarla de la memoria, haga clic en el botón Descargar. Si el botón Descargar aparece atenuado, significa que no se encuentra en el directorio que sirve como punto de inicio de la aplicación.
- Si desea anular la asociación de este directorio principal con una aplicación, haga clic en el botón Quitar.
- Active la casilla de verificación Ejecutar en otro espacio de memoria (proceso aislado) para ejecutar la aplicación en un proceso diferente del proceso del servidor Web. La ejecución de una aplicación aislada protege otras aplicaciones, incluido al propio servidor Web, de que se vean afectadas si esta aplicación tiene un error o deja de responder.

4.9.3.3.-Establecer permisos para una aplicación.

Los niveles de permisos para la aplicación son:

- Ninguno para impedir la ejecución de ningún programa o secuencia de comandos.
- Sólo secuencias de comandos para permitir la ejecución de las aplicaciones asignadas a un motor de secuencias de comandos en este directorio sin tener establecido el permiso Ejecución. Este es el que tenemos que tener activado para nuestra página ASP. El permiso Secuencia de comandos es más seguro que el permiso Ejecución, ya que permite limitar las aplicaciones que se pueden ejecutar en el directorio.
- Establezca el permiso Secuencias de comandos y ejecutables para permitir la ejecución de cualquier aplicación en este directorio, incluso de las aplicaciones asignadas a motores de secuencias de comandos y archivos binarios de Windows (archivo .dll y .exe). (ojo con esto)

4.9.3.4.-Establecer asignaciones para la aplicación.

Aunque esta sección entra en el nivel de avanzado la vamos a comentar para que tengamos una referencia completa de IIS. Se pueden desarrollar aplicaciones Web en diversos lenguajes de programación y de secuencias de comandos. Los Servicios de Internet Information Server (IIS) utilizan la extensión de archivo de un recurso solicitado en el sitio Web para determinar el programa ISAPI o CGI que se va a ejecutar para procesar la petición. Por ejemplo, la petición de un archivo con la extensión .asp hace que el servidor Web inicie el programa ASP (Asp.dll) para procesar la petición. La asociación de una extensión de archivo a un programa ISAPI o CGI recibe el nombre de asignación de aplicación. IIS está configurado para permitir las asignaciones de aplicaciones comunes. Puede agregar o quitar asignaciones para todas las aplicaciones de un sitio Web o de aplicaciones individuales.

Para asignar una extensión a una aplicación:

1. En la consola administrativa seleccionamos el sitio Web o el directorio que sirve como punto de inicio de una aplicación.
2. Abrimos las hojas de propiedades del directorio y haga clic en la ficha Directorio particular, Directorio virtual o Directorio.
3. Hacemos clic en el botón Configuración.
4. En la ficha Asignaciones seleccionamos Agregar.
5. En el cuadro Ejecutable, escribimos la ruta de acceso del programa ISAPI o CGI que procesará el archivo. Debemos especificar un programa en un directorio local del servidor Web.
6. En el cuadro Extensión, escribimos la extensión de archivo que desea asociar al programa ISAPI o CGI. Cuando el servidor Web reciba una dirección URL que identifique un archivo con esta extensión, iniciará el programa asociado para procesar la petición.
7. Para permitir el procesamiento de archivos de este tipo en un directorio con el permiso Secuencia de comandos, activamos la casilla de verificación Motor de secuencias de comandos. Si un directorio tiene establecido el permiso Secuencia de

comandos (en lugar del permiso Ejecución), sólo se podrán procesar en el directorio los archivos asociados a aplicaciones que sean motores de secuencias de comandos designados.

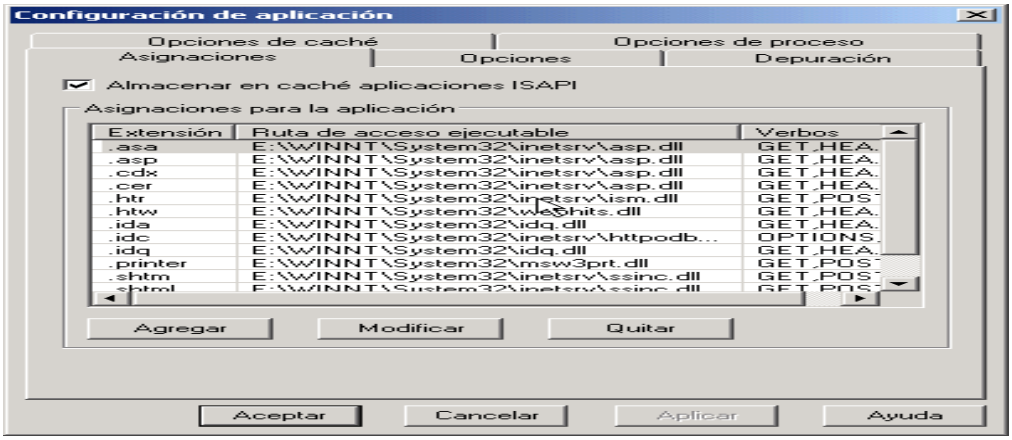

Figura 4.28.-Asignaciòn de una extensión a una aplicación.

4.9.3.5.- Ficha de Opciones en propiedades de aplicación.

Aquí vamos a comentar las opciones que nos aparecen en la pestaña Opciones, algunas de ellas muy importantes:

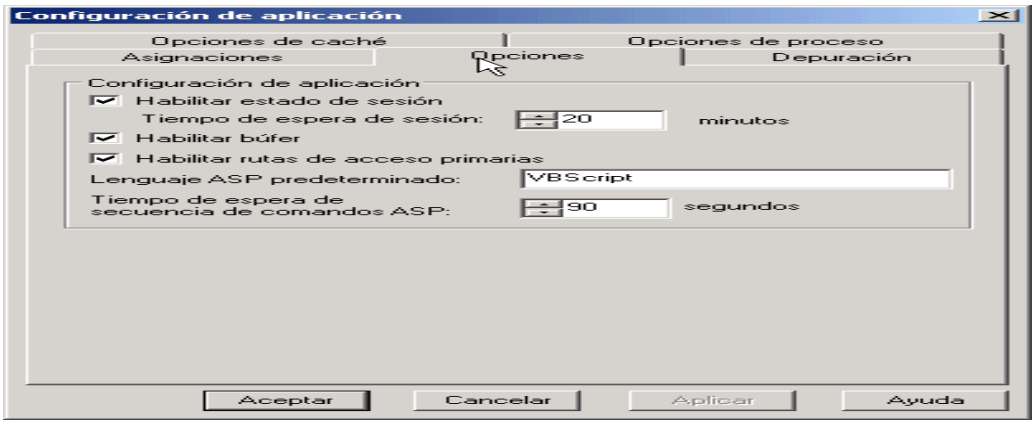

Figura 4.29.- Ficha de Opciones en propiedades de aplicación.

- Habilitar estado de sesión. Esta opción es muy importante a la hora de trabajar con "variables globales" dentro de las ASP. En los capítulos 10, 11 y 12 haremos mención a esta opción y podremos entenderla con un ejemplo.

- Habilitar búfer. Esta opción está deshabilitada por defecto en IIS 4.0. También afecta al funcionamiento de las ASP que veremos mas adelante.
- Habilitar rutas de acceso primarias. Permite que las páginas ASP utilicen rutas de acceso relativas para el directorio primario del directorio actual (rutas de acceso con la sintaxis ...)
- Lenguaje ASP predeterminado. Tenemos dos motores instalados: Vbscript y Javascript y podemos utilizar cualquiera de ellos. De forma predeterminada y el recomendado es VBScript
- Tiempo de espera: Especifica el intervalo de tiempo que ASP permitirá ejecutarse a una secuencia de comandos. Superado ese tiempo devolverá un error.

4.9.3.6.- Ficha de Opciones en depuración de aplicación.

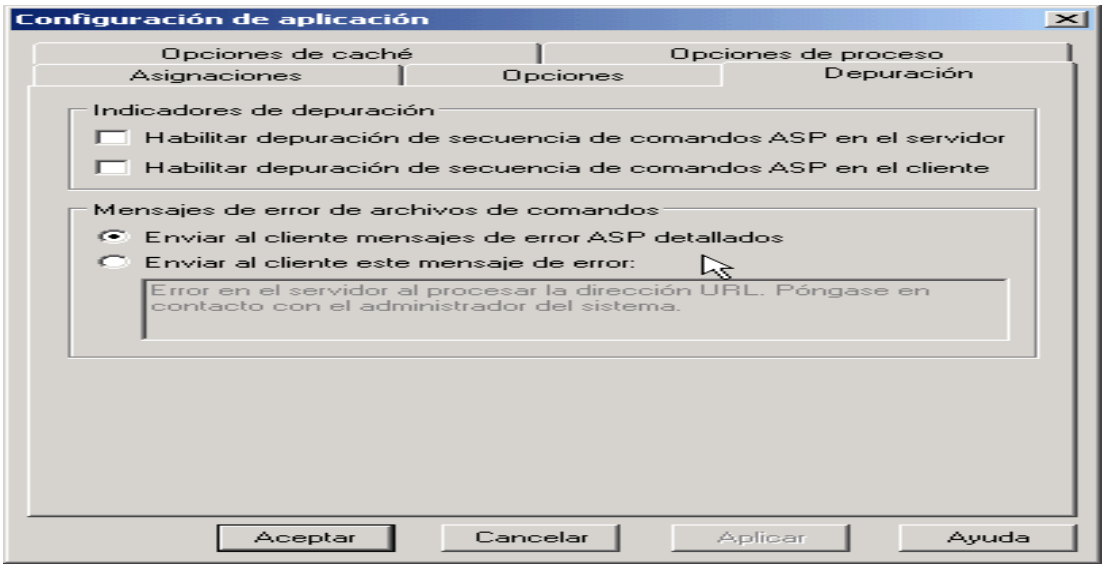

Figura 4.30.- Ficha de Opciones en depuración de aplicación.

Permite operaciones como la depuración de las secuencias ASP. Tenemos dos niveles o tipos de depuración: en el cliente o en el servidor.

4.9.3.7.- Almacenar en memoria caché archivos de comandos ASP.

ASP procesa los archivos que contienen secuencias de comandos ASP, almacena estos archivos procesados en una caché y proporciona los archivos en caché a los clientes. El almacenamiento de archivos ASP en caché mejora el rendimiento ya que las secuencias de comandos ASP en caché no se procesan cada vez que se hace una llamada a las mismas. Puede mejorar aún más el rendimiento cambiando el número de archivos que se almacenan en caché para todas las aplicaciones con protección baja (en proceso) o media (agrupadas), o bien de forma individual para aplicaciones con protección alta (aisladas).

Si no hemos seleccionado la opción de ejecución "Aislada" (Isolated) no se mostrará esta ficha.

4.10.- Instalar filtros ISAPI.

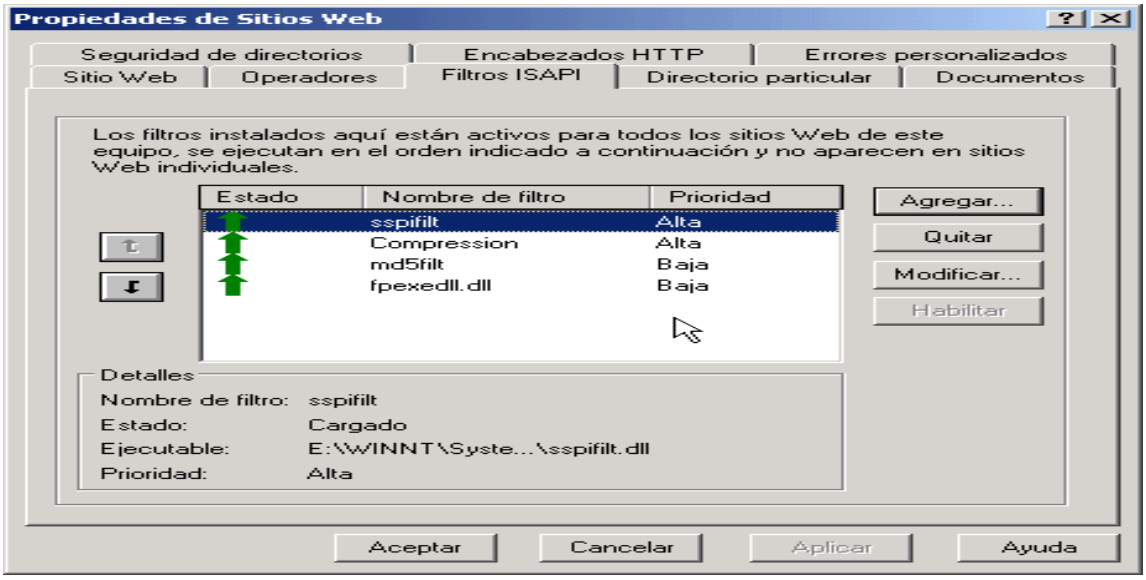

Figura 4.31.-Configuración de filtros ISAPI.

Es una opción que no utilizaremos seguramente nunca pero esa bueno comentarla porque aprendemos más de las "tripas" de IIS. Al igual que las extensiones ISAPI (programación con IIS), los filtros ISAPI son programas que responden cuando el servidor Web recibe una

petición HTTP. Sin embargo, a diferencia de las extensiones ISAPI, los filtros ISAPI se ejecutan siempre en los procesos del servidor. Los filtros ISAPI son diferentes de las aplicaciones porque se controlan por sucesos del servidor Web y no por peticiones de cliente. Puede asociar un filtro ISAPI a un suceso específico del servidor Web; el filtro recibirá una notificación cada vez que se produzca el suceso asociado. Por ejemplo, un filtro puede recibir una notificación cuando se produzca un suceso de lectura o escritura, y cifrará, a continuación, los datos que se van a devolver al cliente.

Puede instalar filtros para todos los sitios de un servidor (filtros globales) y también puede instalar filtros para sitios Web individuales. Si instala filtros globales y filtros de sitio, se combinarán las dos listas de filtros para el sitio.

Cuando se han registrado varios filtros para el mismo suceso, se les llama secuencialmente. Los filtros con mayor prioridad se ejecutan antes que los de menor prioridad. Si varios filtros tienen la misma prioridad, los filtros globales establecidos en las propiedades principales se ejecutan antes que los establecidos para el sitio. Los filtros que tienen la misma prioridad con el mismo grado de herencia se ejecutan según el orden en que se cargaron. Puede cambiar el orden de carga de los filtros en las hojas de propiedades del servidor Web o del sitio Web.

4.11.- Mensajes de error personalizados.

Cuando se produce un error en nuestra Intranet: no encuentra una página, error del servidor, excedido tiempo de espera... IIS muestra una página con el error. Estas páginas las encontramos en un directorio de nuestro disco duro y podemos cambiarlas. Siempre es mejor mostrar un mensaje personalizado con el logo y aspecto de nuestra Intranet que uno genérico. Veamos un ejemplo del mismo mensaje de error visto por IIS de forma predeterminada y después de haber hecho alguna pequeña modificación en su aspecto:

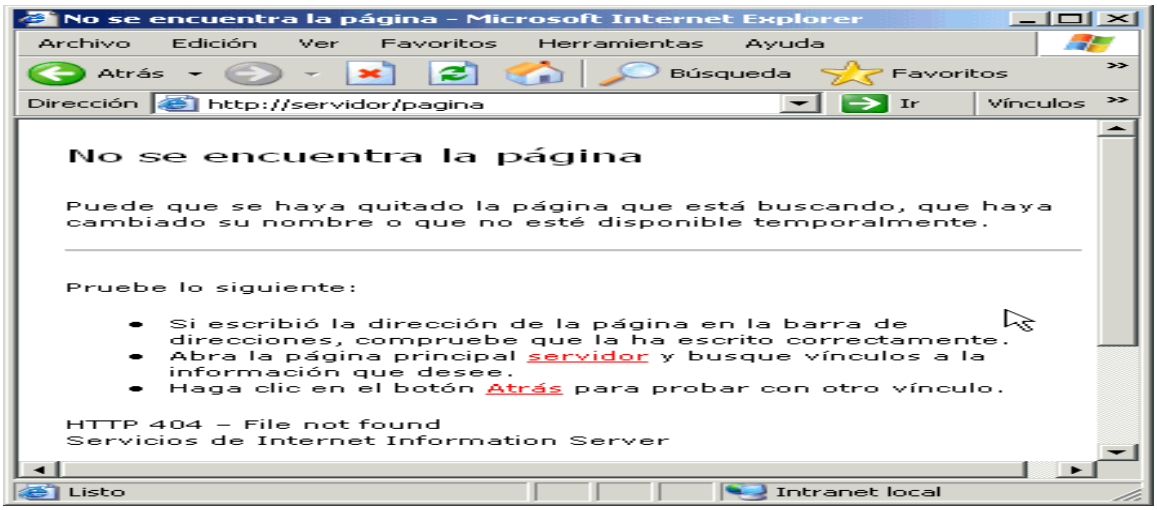

Figura 4.32.- Mensaje de error visto por IIS de forma predeterminada.

Estos son algunos de los errores que se pueden personalizar y que son los más comunes:

Tabla 4.11.-Codigo de error y mensajes.

Código de error	**Mensaje**
400	Solicitud incorrecta
403.1	Acceso de ejecución prohibido
403.2	Acceso de lectura prohibido
403.3	Acceso de escritura prohibido
403.8	Acceso al sitio denegado
403.14	Lista de directorios denegada
404	No se encuentra
404.1	Sitio no encontrado
500	Error interno del servidor
500-100.asp	Error ASP

Los mensajes de error se muestran en una lista del complemento IIS que IIS trata como una sola propiedad. Por ejemplo, cuando se configura un conjunto de mensajes de error personalizados para el sitio Web, todos los directorios de este servidor heredan la lista completa de mensajes personalizados. Es decir, no se combinan las dos listas de mensajes de error personalizados (para el servidor y para el directorio).

El error 404.1 sólo se produce en equipos con direcciones IP múltiples. Si se recibe una solicitud de cliente en una combinación de dirección y puerto IP determinada y la dirección IP no está configurada para la recepción en ese puerto específico, IIS devolverá el mensaje de error HTTP 404.1. Por ejemplo, si un equipo dispone de dos direcciones IP y solamente una de ellas está configurada para escuchar en el puerto 80, cualquier solicitud con puerto 80 que se reciba en la otra dirección IP hará que IIS devuelva el mensaje de error 404.1.

Podemos asignar mensajes de error personalizados a un archivo o a una dirección URL para esto utilizaremos la hoja de propiedades Errores personalizados del complemento IIS:

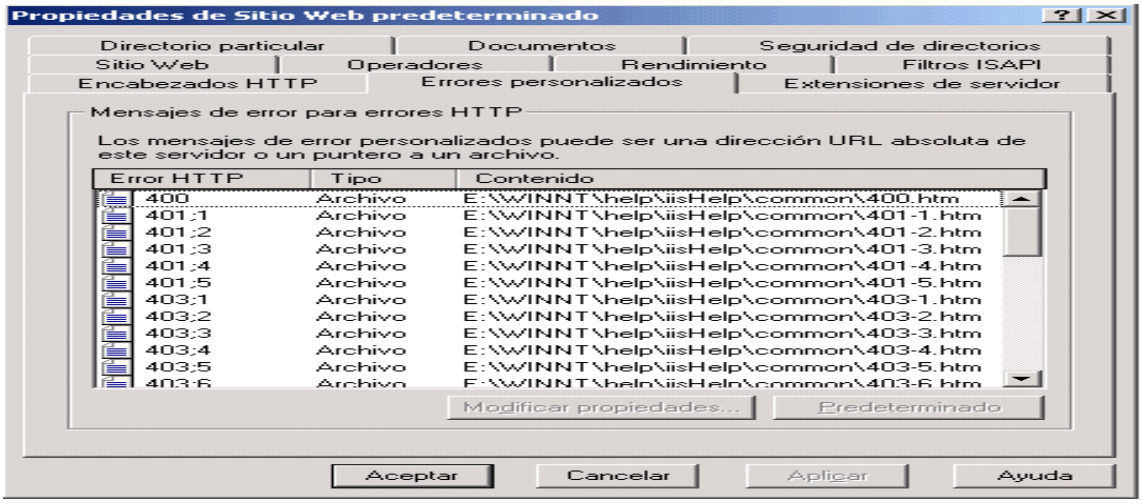

Figura 4.33.-Configuración de mensajes de error.

Para personalizar un mensaje de error mediante su asignación a un archivo:

1. Creamos un archivo que contenga su mensaje de error personalizado y colocamos el archivo en un directorio.
2. Seleccionamos el error HTTP que desea cambiar.
3. Hacemos clic en el botón Modificar propiedades.

4. Seleccionamos Archivo en el cuadro Tipo de mensaje.
5. Escribimos la ruta de acceso y el nombre del archivo que apunta al mensaje de error personalizado o utilizamos el botón Examinar para localizar el archivo en el disco duro del equipo.
6. Hacemos clic en Aceptar.

Podemos modificar los ficheros con FrontPage pero ojo, si incluimos un gráfico debe ser con la forma http://servidor/images/logo.gif. De lo contrario incluirá un enlace a una ruta local c:\imagenes\logo.gif que no funcionará bien. Por ejemplo, modificando el fichero "404b.htm" que es el que se muestra cuando no encuentra la página quedaría así:

Figura 4.34.-Ejemplo de error personalizado.

4.12.- Documentos.

En esta hoja podremos indicar la página por defecto del sitio Web. Cuando un usuario no especifique en el navegador ningún fichero en concreto de nuestro sitio Web se le mostrará esta página por defecto. Podemos indicar diferentes documentos predeterminados dentro de la lista que vemos a continuación:

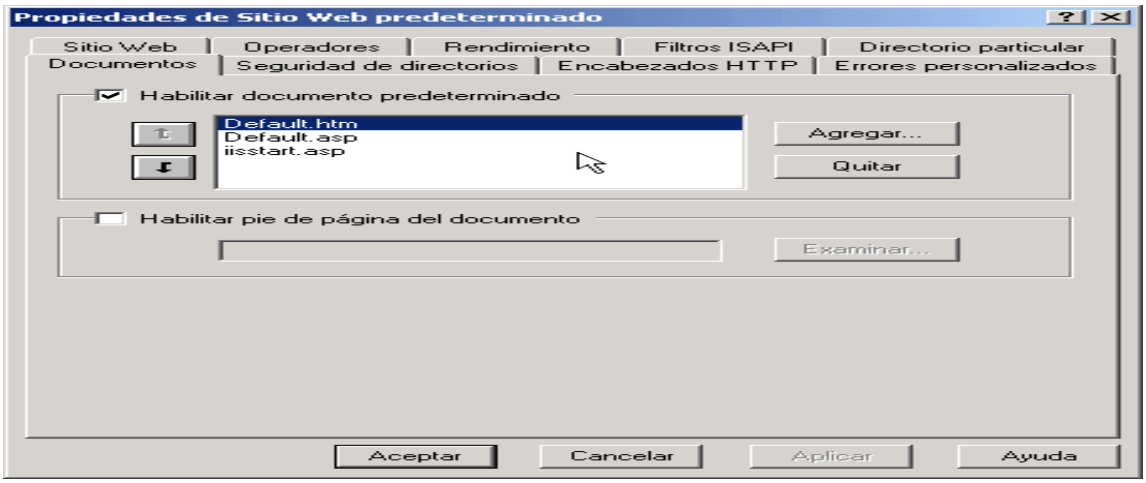

Figura 4.35.-Configuración de error de indicado por página por defecto.

El orden en el que se indican los documentos es significativo, el servidor Web devolverá el primero que encuentre. El orden de prioridad de los documentos lo podemos modificar utilizando las flechas. El documento predeterminado podrá ser tanto una página HTML como una página ASP.

Con la opción inferior "Habilitar pie de página del documento" podremos configurar el servidor Web para que inserte de manera automática un fichero en formato HTML en la parte inferior de todos los documentos del sitio Web.

4.13.- Encabezados HTTP.

En esta hoja de propiedades vamos a poder establecer los valores de las cabeceras HTTP que se envíen a nuestros clientes (navegadores Web). Puesto que no nos van a afectar mucho para nuestra intranet las enumeraremos para identificarlas.

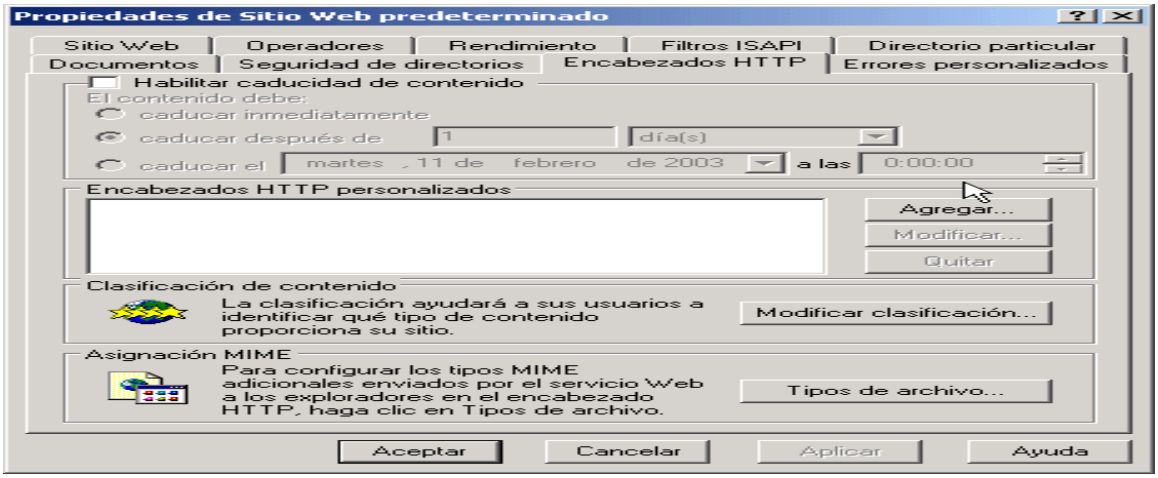

Figura 4.36.- Propiedades de Encabezados HTTP personalizados.

Si activamos la casilla de verificación *Habilitar caducidad de contenido* nos permitirá establecer el momento en el que la información de la página se considera no válida u obsoleta (ha caducado), el navegador Web comparará la fecha del sistema con la de la página que le llega y determinará si se visualiza la página almacenada en la caché o bien pedirá una actualización de la misma.

En la propiedad Encabezados HTTP personalizados podremos enviar un encabezado HTTP personalizado del servidor Web al navegador del equipo cliente.

Las páginas Web pueden incorporar cabeceras con información que identifique sus contenidos desde un punto de vista moral, la configuración de estas cabeceras la realizaremos a través del apartado "Restricción de contenido". De esta manera los usuarios pueden filtrar las páginas en función de ese contenido. IIS utiliza un método desarrollado por el organismo RSAC (Recreational Software Advisory Council) que clasifica los contenidos atendiendo a diversos grados de violencia, pornografía y lenguaje ofensivo. Para establecer estas restricciones de contenido se debe pulsar el botón "Modificar clasificación".

En la opción Tipos MIME (Multipurpose Internet Mail Extensions) podemos determinar los tipos de archivos que se enviarán al cliente Web.

4.14.- Operadores.

En esta hoja podemos definir qué cuentas de usuarios del dominio pertenecen a la figura especial del operador Web. Un operador es una cuenta de usuario de Windows 2000 que

tiene permisos para alterar la dinámica del servicio Web, es decir iniciar, detener o pausar el sitio Web.

Para añadir una cuenta para que actúe de operador del sitio Web pulsaremos únicamente el botón Agregar y seleccionaremos la cuenta de usuario de Windows correspondiente, podremos indicar tanto cuentas como grupos de cuentas de usuarios. Para eliminar una cuenta de los operadores se selecciona de la lista y se pulsa el botón Quitar. La hoja de propiedades Operadores es:

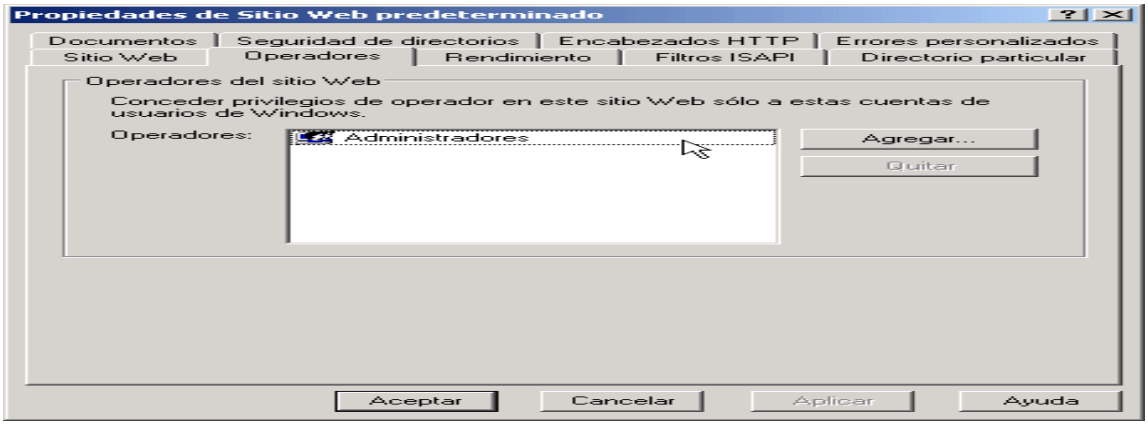

Figura 4.37.-Configuración de cuentas de usuario.

Por defecto el grupo Administradores de dominio de Windows se encuentra dentro de los operadores del sitio Web.

4.15.- Seguridad de directorios.

Esta es una de las partes más complejas de la administración del sitio web con IIS. No es de gran dificultad sino que son parámetros que van a determinar cómo va a funcionar nuestra Intranet. Además concederá y negará el acceso a usuarios y otros aspectos relativos a la seguridad.

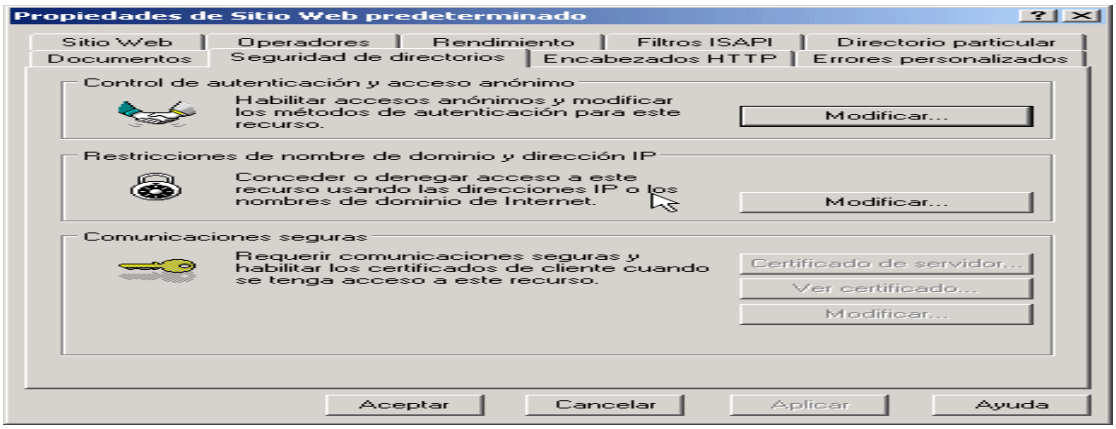

Figura 4.38.-Configuracion de Seguridad de directorios

Estas son las tres secciones referentes a la seguridad y los permisos. La tercera parte la dejaremos porque escapa al objeto de nuestra intranet al entrar en el campo de los certificados y la seguridad SSL, nos centraremos en las dos primeras. De ellas la primera parte es la fundamental para establecer el comportamiento del servidor.

4.15.1.- ¿Qué es autenticación?

En este capítulo explicaremos con profundidad el tema de la autenticación y en el siguiente lo resumiremos y nos quedaremos ya con la configuración apropiada para nuestra intranet. Podemos configurar IIS para autenticar o determinar la identidad de la cuenta de un usuario de Windows, antes de permitir que éste establezca una conexión de red con su servidor. Sin embargo, la autenticación de los usuarios sólo tendrá lugar cuando esté desactivado el acceso anónimo o cuando los permisos NTFS requieran que los usuarios se identifiquen con el nombre y la contraseña de una cuenta de usuario válida de Windows.

Con las opciones de autenticación que ofrece IIS, podemos elegir un método de autenticación que se ajuste a los requisitos de seguridad y a las capacidades del explorador Web del usuario.

Puede especificar que los usuarios proporcionen el nombre de usuario y la contraseña de una cuenta de usuario válida de Microsoft Windows para poder tener acceso a cualquier información del servidor. Este proceso de identificación recibe el nombre de autenticación. La autenticación, como muchas de las características de IIS, se puede establecer para sitios

Web, directorios o archivos. IIS proporciona los siguientes métodos de autenticación para controlar el acceso al contenido del servidor. Veamos los métodos más importantes.

4.15.1.1.- Autenticación anónima.

La autenticación anónima proporciona a los usuarios acceso a las áreas públicas del sitio Web o FTP sin preguntar el nombre de usuario o la contraseña. Cuando un usuario intenta conectarse al sitio Web o FTP público, el servidor Web le asigna la cuenta de usuario de Windows llamada IUSR_nombre_equipo, donde nombre_equipo es el nombre del servidor en el que se ejecuta IIS. De manera predeterminada, la cuenta IUSR_nombre_equipo está incluida en el grupo de usuarios Invitados de Windows. Este grupo tiene restricciones de seguridad impuestas por los permisos NTFS, que designan el nivel de acceso y el tipo de contenido que hay a disposición de los usuarios públicos.

Si tiene varios sitios en el servidor o si tiene áreas de su sitio que requieren diferentes privilegios de acceso, puede crear varias cuentas anónimas, una para cada sitio Web o FTP, directorio o archivo. Al dar a estas cuentas diferentes permisos de acceso o al asignar estas cuentas a grupos de usuarios de Windows diferentes, puede otorgar a los usuarios acceso anónimo a distintas áreas de contenido público Web y FTP.

1. La cuenta IUSR_nombre_equipo se agrega al grupo Invitados del equipo IIS durante la instalación.
2. Cuando se recibe una solicitud, IIS suplanta la cuenta IUSR_nombre_equipo antes de ejecutar cualquier código o de tener acceso a cualquier archivo. IIS puede suplantar la cuenta IUSR_nombre_equipo porque conoce el nombre de usuario y la contraseña de esta cuenta.
3. Antes de devolver una página al cliente, IIS comprueba los permisos de archivos y directorios NTFS para determinar si la cuenta IUSR_nombre_equipo tiene acceso al archivo.
4. Si está permitido el acceso, se completará la autenticación y los recursos estarán disponibles para el usuario.
5. Si no está permitido el acceso, IIS intentará utilizar otro método de autenticación. Si no hay ninguno seleccionado, IIS devolverá al explorador un mensaje de error "HTTP 403 Acceso denegado".

La cuenta anónima debe tener el derecho de usuario para el inicio de sesión local. Si la cuenta no tiene el permiso Inicio de sesión local, IIS no podrá atender ninguna solicitud anónima. La instalación de IIS concede específicamente el permiso Inicio de sesión local a la cuenta IUSR_nombre_equipo. De forma predeterminada, las cuentas IUSR_nombre_equipo de los controladores de dominio no se asignan a las cuentas de invitados. Para permitir inicios de sesión anónimos, debe cambiar las cuentas IUSR__nombre_equipo a Inicio de sesión local

4.15.1.2.- Autenticación básica.

La autenticación básica es un método estándar muy extendido para recopilar información de nombre de usuario y contraseña. El proceso para autenticar se realiza de la siguiente forma:

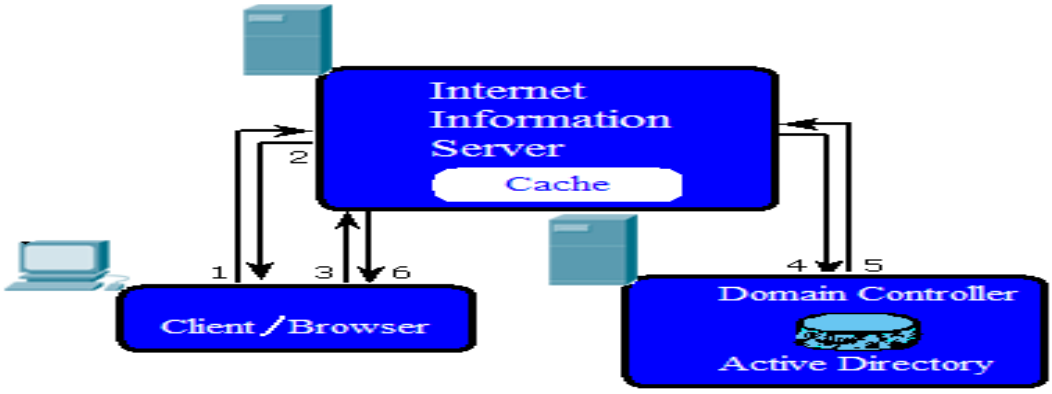

Figura 4.39.-Proceso para autenticar.

1. El explorador Web Internet Explorer muestra un cuadro de diálogo en el que el usuario debe escribir su nombre de usuario y contraseña de Windows previamente asignados, que también se conocen como credenciales.
2. El explorador Web intentará establecer la conexión con un servidor, mediante las credenciales del usuario. La contraseña de texto simple se codifica en Base64 antes de enviarla a través de la red.
    - Importante La codificación en Base64 no es un cifrado. Si una contraseña codificada en Base64 es interceptada en la red por un husmeador de redes, la contraseña puede ser descodificada y utilizada por personas no autorizadas.
3. Si las credenciales de un usuario son rechazadas, Internet Explorer muestra una ventana de diálogo de autenticación para que el usuario vuelva a escribir sus

credenciales. En Internet Explorer se permite al usuario tres intentos de conexión antes de informarle de que no se puede establecer la conexión.

4. Cuando el servidor Web compruebe que el nombre de usuario y la contraseña corresponden a una cuenta de usuario válida de Microsoft Windows, se establecerá una conexión.

La autenticación básica tiene la ventaja de que forma parte de la especificación HTTP y es compatible con la mayoría de los exploradores. La desventaja de los exploradores Web que utilizan la autenticación básica es que transmiten las contraseñas sin cifrar. Mediante la supervisión de las comunicaciones en la red, alguien podría fácilmente interceptar y descodificar estas contraseñas mediante herramientas de dominio público. Por tanto, la Autenticación básica no es recomendable a menos que tenga la seguridad de que la conexión entre el usuario y el servidor Web sea segura, como una línea dedicada o una conexión Capa de sockets seguros (SSL).

4.15.1.3.- Autenticación de texto implícita.

La autenticación de texto implícita ofrece la misma funcionalidad que la autenticación básica. Sin embargo, la autenticación de texto implícita supone una mejora en la seguridad debido a la forma en que se envían las credenciales del usuario a través de la red. La autenticación de texto implícita transmite las credenciales a través de la red como un hash MD5, también conocido como mensaje implícito, en el que el nombre de usuario y la contraseña originales no pueden descifrarse del hash. La autenticación de texto implícita está disponible para los directorios del Sistema distribuido de creación y control de versiones Web (Web DAV).

Antes de habilitar la autenticación de texto implícita en el servidor IIS, asegúrese de que se cumplen los requisitos mínimos siguientes. Sólo los administradores de dominio pueden comprobar que se cumplen los requisitos del controlador de dominio (DC). Si tiene dudas, consulte al administrador del dominio si el controlador del dominio cumple con los requisitos siguientes:

Todos los clientes que tienen acceso a un recurso protegido con autenticación de texto implícita van a utilizar Internet Explorer 5.0 o posterior.

- El usuario y el servidor IIS deben ser miembros o tener la confianza del mismo dominio.
- Los usuarios deben tener una cuenta válida de usuario de Windows almacenada en Active Directory en el controlador de dominio.
- El controlador del dominio debe ser un equipo con Windows 2000 o posterior.
- El servidor IIS debe ser un equipo con Windows 2000 o posterior.

4.15.1.4.- Autenticación de Windows integrada.

La autenticación de Windows integrada (anteriormente llamada NTLM, también denominada autenticación de desafío y respuesta de Windows NT) es un método seguro de autenticación, ya que el nombre de usuario y la contraseña se procesan con el método de hash antes de enviarlos a través de la red. Al habilitar la autenticación de Windows integrada, el explorador del usuario demuestra que conoce la contraseña mediante un intercambio criptográfico con el servidor Web, en el que interviene el método de Hash.

La autenticación de Windows integrada utiliza los métodos de autenticación Kerberos v5 y NTLM. Si los servicios Active Directory están instalados en un controlador de dominio con Windows 2000 o posterior y el explorador del usuario es compatible con el protocolo de autenticación Kerberos v5, se utilizará la autenticación Kerberos v5; de lo contrario, se utilizará la autenticación NTLM.

Traduciendo este definición digamos que el navegador no se validad cada vez sino que envía los credenciales del dominio/usuario y establece una comunicación donde no vuelve a enviar la contraseña. Es el mejor sistema para una Intranet pero debemos tener un sistema de dominios instalado en nuestra red.

4.15.2.- ¿Qué autenticación escoger?

Revisamos ya con la consola administrativa los niveles de seguridad que son

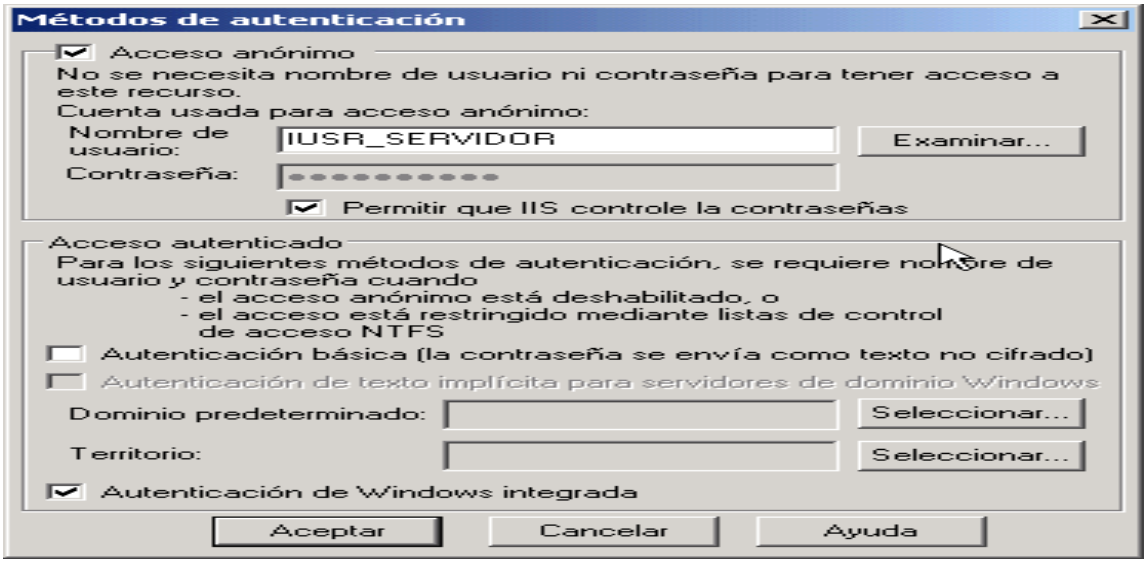

Figura 4.40.-Configuración de los métodos de autenticación.

Y corresponden a:

- Autenticación anónima: permite que cualquier usuario tenga acceso sin que se le pida su nombre de usuario y contraseña.
- Autenticación básica: solicita al usuario su nombre de usuario y contraseña, que se envían sin cifrar a través de la red.
- Autenticación de texto implícita: Funciona de manera similar a la autenticación básica, pero difiere de ella en que las contraseñas se envían como un valor de hash. La autenticación de texto implícita sólo está disponible para los dominios con un controlador de dominio de Windows 2000.
- Autenticación de texto implícita avanzada. La autenticación de texto implícita avanzada es idéntica a la autenticación de texto implícita, excepto en que la avanzada almacena las credenciales de cliente como un hash MD5 de Active Directory en el controlador de dominio de Windows XP para mejorar la seguridad.

- La autenticación de Windows integrada utiliza la tecnología de hash para identificar al usuario sin enviar realmente la contraseña a través de la red.

Si utilizamos la primera opción el acceso será anónimo y no tendremos ningún tipo de identificación a lo largo de la sesión del usuario. Es una seguridad propia para un web de Internet, ya que nadie debe, en principio, identificarse. La segunda opción la rechazamos inmediatamente por no tener ningún tipo de seguridad a la hora de transmitir la contraseña.
Y de las demás nos quedamos con la "Seguridad Integrada" Esta envía los credenciales del usuario en cada petición. Esto funcionalmente hace que desde ASP podamos saber siempre que usuario ha solicitado la página. Como veremos más adelante es un aspecto fundamental a la hora de manejar una Intranet.

4.15.3.- Restricciones de nombres de dominio y direcciones IP.

Otro de los métodos para controlar el acceso es a través de las direcciones IP. Si observamos la siguiente pantalla:

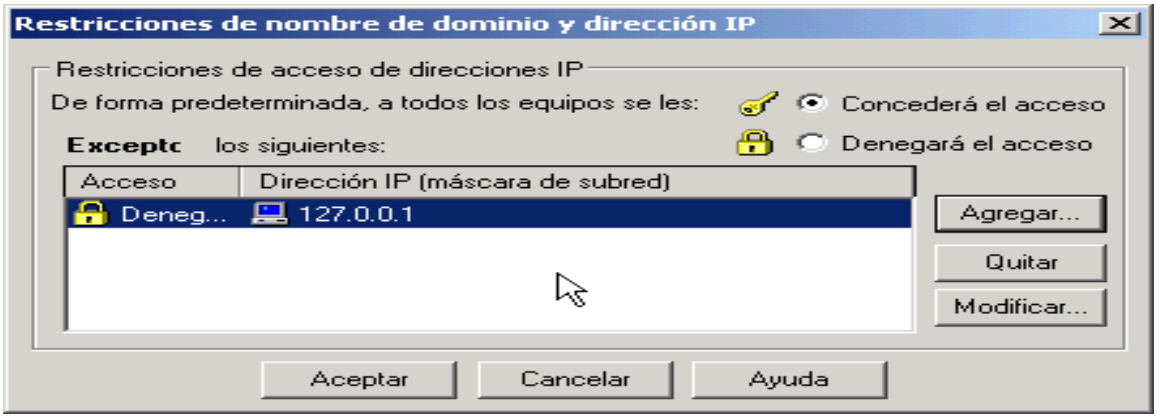

Figura 4.41.-Restricciones de nombres de dominio y direcciones IP.

Observamos que podemos indicar una dirección IP que será la o las excepciones de lo que indiquemos. Es decir, en el ejemplo por defecto se les concede a todos el acceso excepto para la dirección 127.0.0.1, que es una dirección especial que indica al propio equipo.

Esta restricción la tiene el web de administración de nuestro IIS. Si recuerda el alumno no nos funcionaban las páginas web del sitio de administración más que en el propio servidor.

Esta es la razón. Si queremos conceder acceso a alguna dirección IP en particular, la podemos realizar desde aquí.

4.16.- Extensiones de servidor.

Uno de los elementos mas importantes en nuestro servidor IIS son las "Extensiones de servidor". Esta es una aplicación incluida con IIS (hasta la versión 4.0 era externa) que permite conectar el programa FrontPage con el IIS. Por ejemplo desde FrontPage podremos crear y administrar distintos sitios web trabajando con un IIS. Es decir le podemos decir "Crear un sitio Web" en el servidor "intranet". Frontpage buscará un servidor de páginas web (IIS) en esa ubicación y luego que esté el módulo de "extensiones de servidor". Si está correctamente podré recuperar los datos de este servidor: sitios web, permisos, ... y otros detalles que harán que no necesitemos manejar mas veces la consola administrativa de IIS. Veamos la siguiente pantalla:

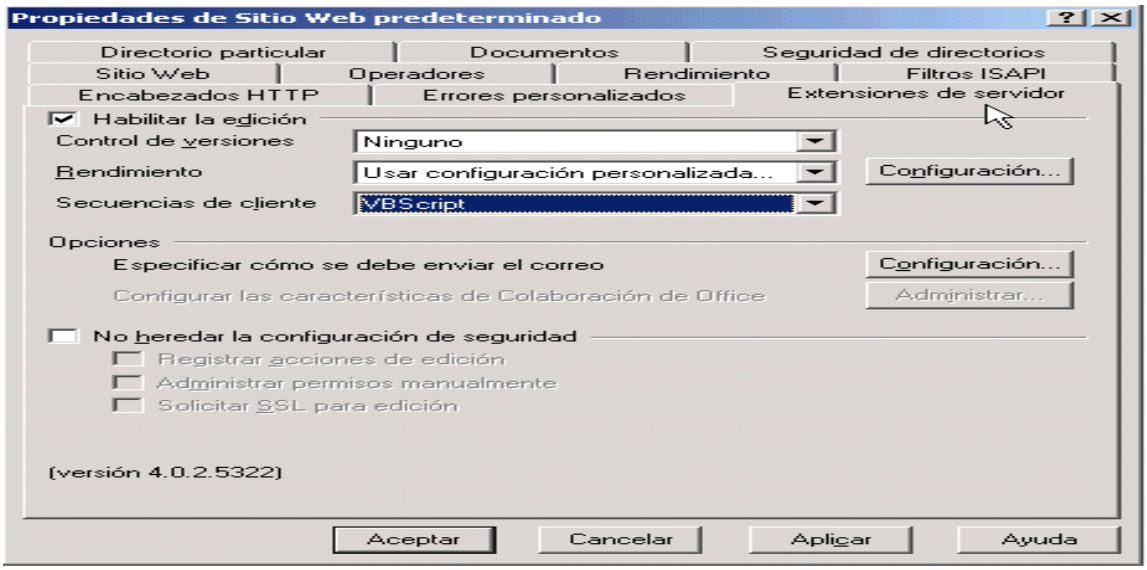

Figura 4.42.-Configuración de extensiones.

Podemos ver que apenas hay opciones, la verdad es que no hay que activar prácticamente nada. Las opciones son:

- Habilitar edición (sólo para la web raíz). Permite que los autores utilicen FrontPage para acceder y modificar el web. Debe estar activada para que podamos editar el web con Frontpage.
- Control de versiones. Si activamos esta opción podemos obtener información sobre quién está modificando el contenido del web, identificar los cambios o evitar que los cambios realizados por un autor borren los de otro. Podemos elegir el incorporado u otro externo más potente como Visual Sourcesafe.
- Rendimiento. Estimando el volumen de movimiento de nuestra web Frontpage reservará memoria para su caché.
- Secuencias de cliente. Cuando las extensiones de frontpage nos genere algún código podemos seleccionar el lenguaje.
- Especificar cómo se debe enviar el correo. Podemos especificar los parámetros de su configuración de la cuenta y correo electrónico para los casos que se necesite.

El siguiente grupo de opciones utilizan las opciones del servidor raíz. Si queremos que no las hereden activaremos la casilla para conseguir:

- Registrar acciones de edición. El sistema graba quien ha realizado modificaciones: usuario, web, equipo remoto, ... estos datos se almacenan en un archivo: "_vti_log/Autor.log".
- Administrar permisos manualmente. Si está activada podemos utilizar las extensiones del servidor para administrar permisos, en caso contrario hay que realizar los cambios manualmente.
- Solicitar SSL para edición. Permite autenticar a los autores de la web.

Por defecto los sitios Web incluyen las extensiones de servidor. Durante la vida de nuestra web es posible que éstas se deterioren: un corte de luz, corrupción interna, ... entonces debemos comprobar y/o reinstalar estas extensiones. Para realizar esta operación debemos seleccionar el web y en la opción "Todas las tareas" que aparece al pulsar con el botón derecho seleccionamos "Comprobar extensiones Web":

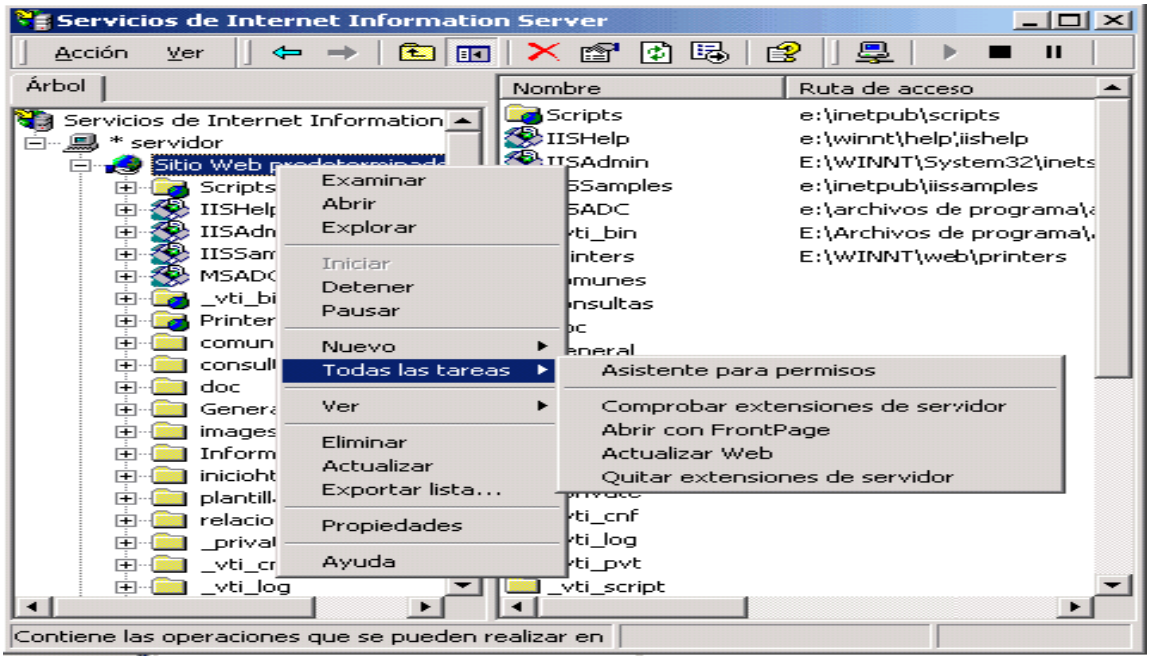

Figura 4.43.-Comprobación de extensiones de servidor.

Veremos como comprueba y repara si es el caso los errores que se hubiesen producido. En ocasiones esta reparación no es suficiente y hay "Quitar las extensiones" y volver a instalarlas con estas opciones para rehabilitarlo. Pero en general es un módulo que suele presentar dificultades... Pasemos a la práctica con FrontPage.

4.17.- IIS + FrontPage.

Ahora comienza la parte sencilla. Ya hemos terminado de ver todas las opciones de IIS y pasaremos a la acción con FrontPage. Como hemos comentado este programa es el idóneo para trabajar con nuestra web ya que IIS incluye un módulo especial que conecta IIS con FrontPage: “las extensiones de servidor" .

Estas extensiones van a permitir entre otras cosas crear webs directamente desde Frontpage en nuestro IIS o incluir componentes web avanzados dentro de las páginas. Veamos las opciones más importantes:

4.17.1.- Abrir sitios web.

Para abrir un web simplemente seleccionaremos la opción de abrir web. Si escribimos http://servidor abriremos el web raíz del servidor IIS. Para abrir otros webs haremos la misma operación pero escribiendo la ruta correcta: http://servidor/miweb

4.17.2.- Crear sitios web.

1. En Microsoft FrontPage, en el menú Archivo, seleccionamos Nuevo y, a continuación Web.
2. En el panel de tareas Nueva página o Web, en Nuevo a partir de una plantilla, haga clic en Plantillas de sitio Web.
3. Hacemos clic en Web de una página y a continuación en el cuadro especificar la ubicación del nuevo sitio Web, escriba la dirección URL del sitio Web. La dirección URL la escribiremos con el formato http://servidor/miweb

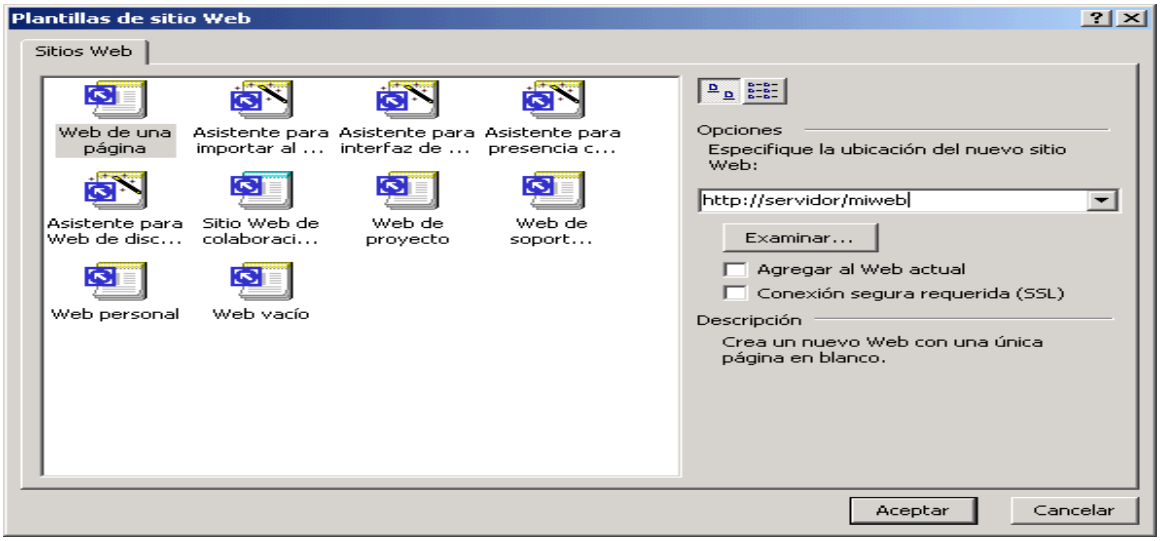

Figura 4.44.-Plantillas para crear un sitio Web.

Hacemos clic en Aceptar. FrontPage creará el sitio Web en el servidor:

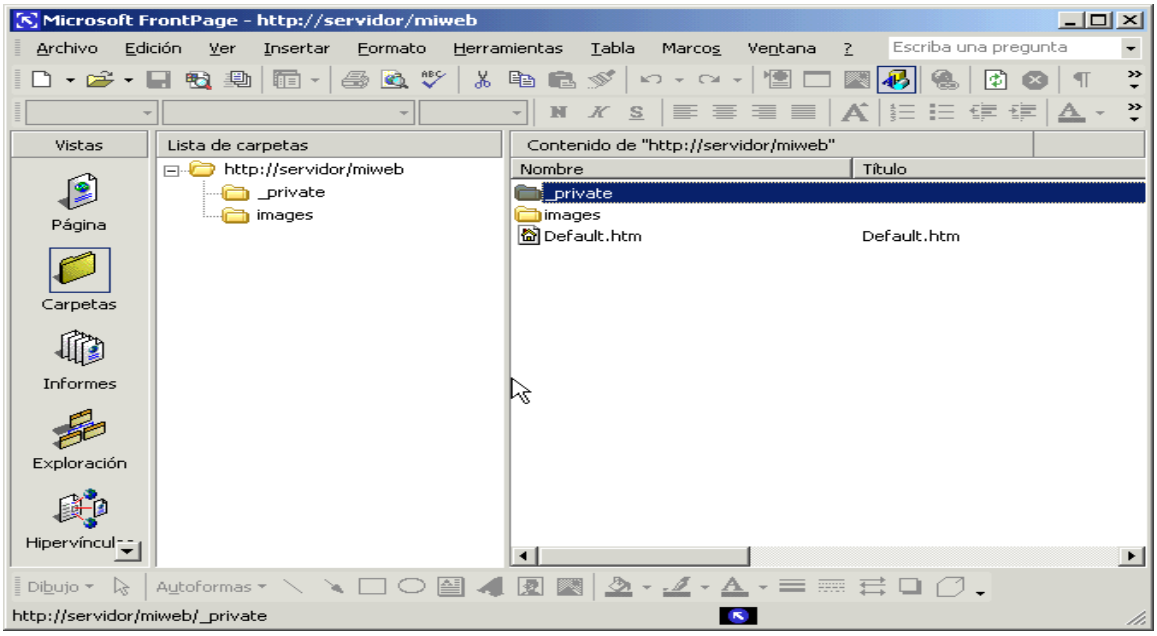

Figura 4.45.-Sitio Web creado en el servidor por FrontPage.

Para comprobar que los parámetros de "ejecución de comandos" están activos pulsamos con el botón derecho en la raíz del web:

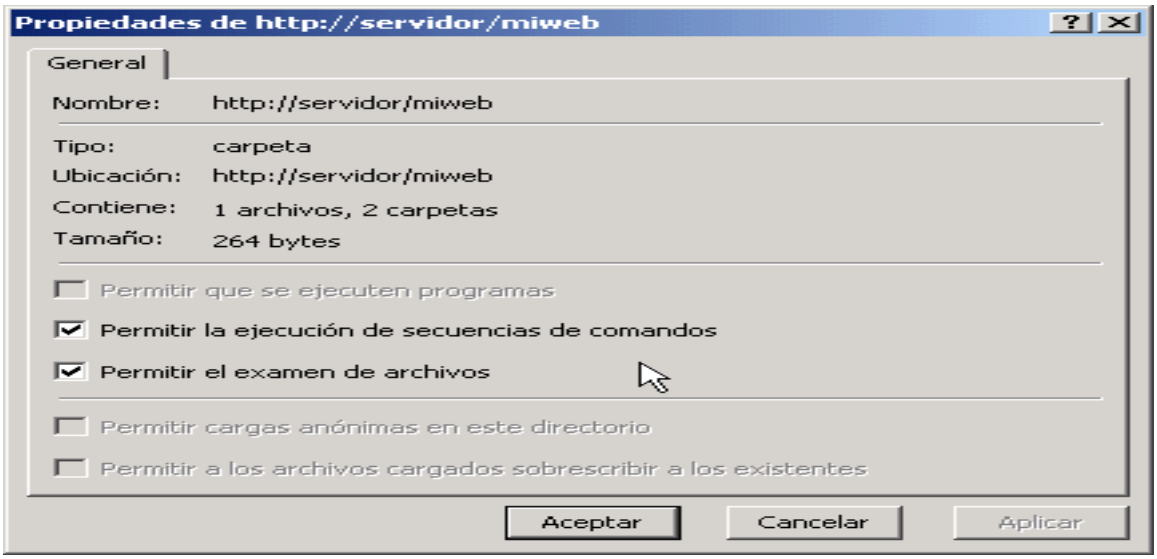

Figura 4.46.-Propiedades del sitio Web creado.

En este caso también está activa la opción de "Permitir el examen de directorios" opción no recomendable pero que en desarrollo es útil mientras se construyen las páginas con los hipervínculos.

4.17.3.- Mantenimiento de permisos en el servidor.

Los permisos para que los usuarios puedan administrar y modificar se encuentran en la opción "Permisos" de la sección "Servidor" del menú "Herramientas".

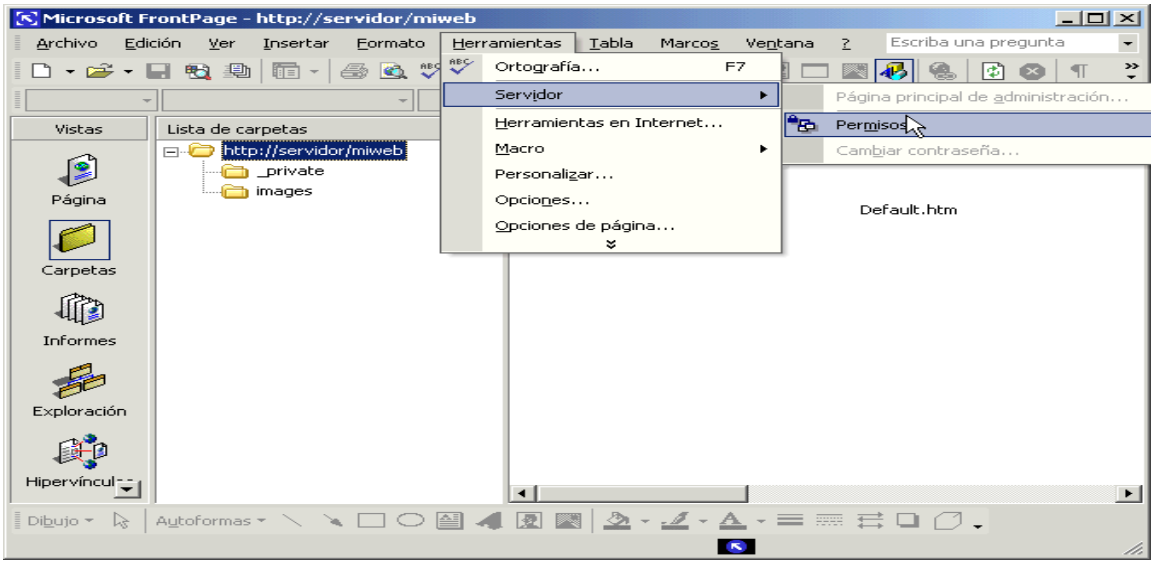

Figura 4.47.- Mantenimiento de permisos en el servidor.

Aquí podremos dar tres tipos de permiso a los usuarios. Si estamos trabajando con un sistema de dominios de Windows Nt 4.0 o Directorio Activo de Windows 2000 tendremos la ventaja de que podremos recuperar los nombres de los usuarios de la red para poder asignarles permisos.

Capítulo 5.- Utilización de la intranet.

5.1.- Internet Explorer.

La función de un navegador es la de enviar peticiones de archivos a un Web y visualizar la información recibida en la estación de trabajo.

En un navegador se puede mostrar todo tipo de información, como textos, imágenes, sonido, video, etc. Así mismo, puede utilizarse también para introducir formularios y transmitirlos al servidor.

La aparición del navegador Internet Explorer 3.0 supuso una pequeña revolución en el escenario de las herramientas Web, hasta ese momento dominado por Netscape con Navigator.

Internet Explorer es el navegador que da nombre a la suite completa y es muy similar a versiones anteriores. Esto sin duda beneficia a los usuarios que podrán utilizar el navegador de la misma manera en que lo venían haciendo. Sin embargo se han incluido grandes cambios que hacen de esta aplicación una potente herramienta de navegación disponible para todos los sistemas operativos Windows. A continuación, se mostrará una breve descripción en la versión que incorpora Windows Server 2003.

Las principales características que muestra este navegador son:

- Posibilidad de navegación offline.
- Gestión de perfiles de usuario.
- Las opciones de Búsqueda, Favoritos e Historial se pueden incluir como paneles dentro de la ventana del explorador.
- Personalización de todo el entorno.

5.2.- Los servicios de correo electrónico.

Los servicios de correo electrónico cuentan con los tres componentes siguientes:

- Cliente de correo electrónico POP3. Este cliente se utiliza para leer, redactar y administrar los mensajes de correo electrónico.
- Servicio SMTP. Este servicio dirige los mensajes salientes desde el remitente al destinatario.
- Servicio POP3. Este servicio se encarga de descargar el correo electrónico desde el servidor de correo al equipo local del usuario.

Los administradores organizan el servicio POP3 en tres niveles administrativos:

- Servidores de correo. Son los equipos donde se encuentra instalado el servicio POP3. Los usuarios se conectan al servidor para recuperar sus correo electrónico
- Dominios de correo electrónico. Debe ser un nombre de dominio registrado y deberá coincidir con el registro de recurso del Agente de Intercambio de Correo (MX) creado en el servidor DNS que da soporte ~ servidor de correo.
- Buzones. Cada buzón corresponde a un usuario que es miembro del dominio de correo electrónico. A cada buzón se le asigna un directorio donde el correo se almacenará hasta que el usuario lo recupere.

5.2.1.- Introducción a la recuperación y transferencia de correo electrónico.

El proceso que sigue un mensaje de correo electrónico desde que sale del equipo remitente al equipo destinatario es el siguiente:

1. El equipo cliente del remitente se conecta a Internet a través de proveedor de servicios Internet (ISP). Mediante un cliente de correo electrónico, el remitente envía un mensaje de correo electrónico. El mensaje utiliza el protocolo SMTP y se transfiere al ISP del remitente que a su vez lo encamina a Internet.
2. El mensaje de correo electrónico utiliza Internet y transmite a través de un número variable de servidores intermedios durante su trayecto destinatario. Cuando el correo electrónico llega al ISP del destinatario se deposita en su buzón.
3. Cuando el equipo del destinatario se conecta al ISP del destinatario el correo

electrónico se transfiere a su equipo local, de acuerdo con el protocolo POP3.

5.2.2.- Protocolo POP3.

El Protocolo de oficina de correo 3 (POP3, Post Office Protocol 3) es un protocolo estándar para recuperar correo electrónico. El protocolo POP3 controla la conexión entre un cliente de correo electrónico POP3 y un servidor donde se almacena el correo electrónico. El servicio POP3 emplea el protocolo POP3 para recuperar el correo electrónico desde un servidor de correo a un cliente de correo electrónico POP3.

El protocolo POP3 tiene tres estados de proceso para controlar la conexión entre el servidor de correo y el cliente de correo electrónico POP3:

- El estado de autenticación. Durante este estado, el cliente de correo electrónico POP3 conectado al servidor debe autenticarse para que los usuarios puedan recuperar su correo electrónico. Si el nombre de usuario y la contraseña suministrados por el cliente de correo electrónico coinciden con los del servidor, el usuario se autenticará y se pasará al estado de transacción (en caso contrario se mostrará al usuario un mensaje de error y no se permitirá la conexión para recuperar correo electrónico).

  Para impedir daños en el almacén de correo una vez que se ha autenticado al cliente, el servicio POP3 bloquea el buzón del usuario. El nuevo correo electrónico entregado en el buzón después de la autenticación del usuario (y del bloqueo del buzón) no estará disponible para su descarga hasta que la conexión haya finalizado. Asimismo, sólo se puede conectar un cliente a un buzón cada vez y se rechazan las solicitudes adicionales de conexión al buzón.
- El estado de transacción. Durante este estado, el cliente envía comandos POP3 que el servidor recibe y responde de acuerdo con este mismo protocolo (se omitirán todas las solicitudes de cliente recibidas por el servidor que no sean compatibles con el protocolo POP3 y se devolverá un mensaje de error).
- El estado de actualización cierra la conexión entre el cliente y el servidor. Éste es el último comando que transmite el cliente.

Tras el cierre de la conexión, el almacén de correo se actualiza para reflejar los cambios realizados mientras el usuario estaba conectado al servidor de correo.

5.2.3.- El almacén de correo.

El almacén de correo es un directorio donde el servicio POP3 almacena todo el correo electrónico hasta que los usuarios lo recuperan desde su equipo cliente.
Al crear un dominio, el servicio POP3 crea un directorio correspondiente en el directorio que se ha designado como almacén de correo (por defecto, C:\linetpub\mailroot\mailbox). Para cada usuario con un buzón en dicho dominio POP3 crea un directorio en el directorio del dominio. El correo electrónico que recibe el usuario se almacena como un archivo individual en el directorio del usuario hasta que éste lo recupera mediante un cliente de correo electrónico POP3.
Los permisos de directorio y archivo de cada directorio del almacén de correo son idénticos. Cuando se configura el almacén de correo, los permisos se establecen de forma que sólo se asignan permisos de acceso a los directorios de los administradores locales o de dominio y al servicio de red local, en el que está configurado para ejecutarse el servicio POP3. A ningún otro usuario se le asignan permisos de lectura o escritura.
La funcionalidad del almacén de correo depende de que haya suficiente espacio en disco duro disponible. Para garantizar dicha funcionalidad, se debe realizar una estimación de los requisitos de espacio en disco basada en el número de usuario del servidor, el volumen de correo electrónico que recibirán y el tamaño medio de correo que recibirán. Además, se pueden implementar cuotas de disco para proteger el servidor en situaciones en las que el uso del disco del almacén de correo pueda incrementarse de forma inesperada.

5.2.4.- Como añadir una tarjeta de presentación a la libreta de direcciones.

Cuando reciba un mensaje vera que contiene una tarjeta de presentación si hay incluido un archivo con extensión VCF o, si en la parte derecha de la cabecera incluye el icono de dichas tarjetas (es como una hoja de agenda horizontal).
Cuando vea las primeras líneas del mensaje en el panel de vista previa, pulse el botón izquierdo del ratón sobre el icono que representa a la tarjeta y seleccione abrirlo para ver los datos que incorpora o guardarlo en el disco (deberá hacerla en un archivo con extensión

VCF).

Si lo guarda en un archivo con extensión VCF, podrá incorporarlo a la Libreta de direcciones.

La seguridad en el envío y recepción de mensajes

Outlook Express incorpora distintas características de seguridad en el envío y recepción de mensajes.

Destaca S/MIME (Secure MIME), que es el sistema de seguridad mas utilizado por los programas de correo.

Define una doble protección a los mensajes:

- Autentificación a través de una firma digital.
- Privacidad mediante la encriptación de los mensajes.

Además, puede indicarle si el mensaje ha sido alterado durante la transmisión por Internet.

Un sistema criptográfico es un método por el que los mensajes se alteran siguiendo unas determinadas normas para que no pueda ser leído por personas no autorizadas.

En todos los sistemas criptográficos se han de utilizar dos claves: una para cifrar el mensaje y otra para descifrado.

Existen dos tipos de sistemas criptográficos:

- Sistemas de clave simétrica. Es el que utiliza la misma clave para cifrar y descifrar el mensaje. Por tanto, cuando se descubre una clave, se descubre también la otra.
- Sistemas de clave asimétrica. Es el que utiliza una clave distinta para cifrar y descifrar el mensaje. Por tanto, cuando se descubre una clave, no se descubre necesariamente la otra.

S/MIME utiliza un sistema híbrido. Es decir, encripta el mensaje con una clave simétrica y dicha clave simétrica se codifica con una clave asimétrica.

Estas dos claves se conocen como clave pública y clave privada. Son asimétricas y por tanto de una no se puede deducir la otra.

La clave pública se puede distribuir a todos los destinatarios del mensaje, la clave privada es personal y sólo la conoce su propietario.

Para que un usuario consiga su propio par de claves, ha de solicitar un identificador digital recurriendo a una Agencia de Credenciales (CA) que es una compañía especializada en proporcionar certificados a los usuarios.

Cuando recibe su identificador digital, se crea un archivo en su ordenador para cada clave. El archivo de la clave privada está protegido y nunca viaja por Internet, el archivo de la clave pública se puede copiar todas las veces que se desee y se envía por Internet a los destinatarios de los mensajes.

Este par de claves sirve para realizar dos operaciones distintas:

- Firma digital. La firma digital se utiliza para que el destinatario del mensaje esté seguro de que el emisor es realmente quien dice ser. Cuando se envía un mensaje con firma digital, se genera un número utilizando un algoritmo sobre el texto del mensaje y lo encripta utilizando la clave privada del emisor. Cuando llega a su destino, el receptor desencripta el número utilizando la clave pública del emisor, vuelve a generar el número y lo compara con el que previamente había desencriptado.
- Cifrar el mensaje. Se utiliza para que únicamente el destinatario pueda leerlo. El emisor cifra el mensaje con la clave pública del destinatario y cuando llega a su destino el receptor lo descifra utilizando su clave privada.

Utilizando ambas operaciones se puede estar seguro de la identidad del destinatario del mensaje.

5.2.5.- Cómo obtener un identificador digital.

Un usuario particular puede conseguir su identificador digital recurriendo a una Agencia de Credenciales (CA) que es una compañía especializada en proporcionar de forma gratuita este servicio (para empresas y profesionales se proporciona el servicio con costo).

Estas agencias además de expedir identificadores digitales para usuarios particulares también los expiden para servidores Web. Un servidor Web seguro manda toda la información encriptada de forma que no pueda ser interceptada por personas no autorizadas (un servidor Web seguro se distingue porque el nombre de su página comienza por https:// en lugar de por http://).

Cada identificador digital está asociado con una determinada dirección del correo electrónico, por tanto si posee varias direcciones de correo, deberá solicitar varios

identificadores digitales. De la misma manera, es posible tener identificadores para una misma dirección de correo pero cada uno ha de ir expedido por una agencia diferente o por la misma pero con diferente nombre.

Para solicitar un identificador digital abra el menú Herramientas, seleccionar Opciones, abra la ficha Seguridad y marque Obtener Id. Digital.
Se procederá a realizar la conexión con Internet para solicitar el identificador digital (siga los pasos que se le indican).
Cuando finalice su solicitud, deberá esperar a recibir un mensaje electrónico (no tarda más de cinco minutos) para proceder a su instalación.

5.3.- NetMeeting.

NetMeeting es la herramienta de trabajo en grupo incorporada a la suite de Explorer.
Es una aplicación muy potente que permite, entre otras opciones establecer conferencias de audio y video entre varias personas.
Los requisitos básicos para poder utilizada son: un ordenador con procesador a 90Mhz, 24 MB de RAM y al menos 15 MB de memoria en disco duro.
Además de estos requerimientos para poder utilizar audio y vídeo se necesitará una tarjeta de sonido, altavoces y micrófon. En el caso de vídeo, una tarjeta de vídeo con controlador compatible Video for Windows.
La principal función de NetMeeting es realizar trabajo en grupo a través de conferencias. Una conferencia podría definirse como una sesión establecida entre dos o mas personas en las que pueden comunicarse (ya sea utilizando el teclado o por vídeo), enviarse datos entre sí (documentos o cualquier tipo de archivo) y compartir aplicaciones.
Para ello, las posibilidades que ofrece son:

- Transferencia de archivos. Se pueden enviar archivos a todos o algunos usuarios conectados a la conferencia. Además el destinatario puede aceptar o no dicha transmisión.
- Comunicación entre usuarios. Para establecer una conferencia es imprescindible que exista una comunicación entre los distintos miembros. Esta comunicación puede ser

escrita utilizando la voz (de audio) o videoconferencia.

- Pizarra. La pizarra permite que todos los miembros de la misma conferencia utilicen de manera conjunta una aplicación de dibujo básica (parecida al programa Paint de Windows).

- Compartición de aplicaciones. Esta opción permite que todos los miembros de la conferencia vean una aplicación Windows que esté ejecutando uno de ellos. Es posible además, si el propietario lo permite, que todos los miembros la utilicen.

Es necesario resaltar que para poder hacer uso de las opciones de conferencia y audio por más de dos usuarios dentro de una conferencia, es necesario conectarse a un servidor que soporte videoconferencia y audio multipunto (el resto de las opciones se pueden llevar a cabo por más de dos personas necesidad de hacer uso de un servidor).

NetMeeting es una herramienta muy importante dentro del trabajo en grupo para una intranet (especialmente en los casos en los que esté distribuida dentro de un edificio).

Previamente a su utilización, se ha de proceder con la instalación del programa (como las opciones posibles son varias, no se explica el proceso).

Para poder utilizarlo y una vez instalado, se ha de seleccionar el icono del escritorio o de la barra de inicio rápido (según lo que se indica en el proceso de instalación).

5.4.- Conferencias.

Para establecer una conferencia con otros usuarios se puede utilizar el servidor de directorios.

En un servidor de directorios se localiza la lista de usuarios (el directorio usuarios) que están conectados a ese servidor y con los que se pueden establecer conferencias (también es posible conectarse si no se dispone de un servidor de directorio, pero hay que especificar la dirección IP de la máquina con la que se pretende conectar).

Para conectarse con otro usuario se utiliza el icono *Llamar* (en la parte superior derecha) de la barra de herramientas (el usuario remoto ha de aceptar llamada).

Una vez conectado con otro usuario, se puede realizar conversaciones utilizando el teclado. Para ello, hay que pulsar en el icono *Conversación* de la parte inferior de la pantalla.

Además de esta opción, en la conferencia se pueden compartir aplicaciones. Para ello es

necesario pulsar el icono *Compartir programa* y seleccionar una aplicación deseada (para poder compartir la aplicación ha de estar abierta en el ordenador desde donde será compartida). A partir de ese instante, cualquier miembro de la conferencia podrá ver la aplicación funcionando en su ordenador.

Además para que los demás usuarios puedan controlar la utilización de la aplicación, se debe pulsar el botón *Permitir control de la pantalla* que muestra al pulse el icono *Compartir programa* (de este modo, cualquier persona que este colaborando en una conferencia podrá usar la aplicación como si realmente fuese suya).

Otra opción que permite Netmeeting es enviar archivos, utilizando el icono *Transferir archivos* de la parte inferior de la pantalla (cuando el archivo llegue al destinatario, le mostrará un aviso que indica la llegada del fichero).

5.5.- Necesidades para abrir la Intranet a Internet.

En la tecnología intranet se usan diversos medios para salvaguardar la integridad de los datos y sistemas. Estos medios pueden ser de tipo estructural o bien pueden ser mediante el uso de protocolos de seguridad empleados en las transacciones de información que fluyen por la red.

Las necesidades que se requieren para abrir una Intranet a Internet, van a depender de la forma de acceso a Internet que se va a utilizar.

Existen tres tipos de acceso aunque, para una Intranet, se pueden considerar principalmente dos de ellos:

- A través de un proveedor de acceso. Para ello, se necesitara disponer de un equipo que realice la transmisión de datos con el exterior, software de comunicaciones y una cuenta en un proveedor de acceso a Internet.
- A través de otras redes. Para ello, se necesitara disponer de una conexión a otra red que disponga de acceso a Internet. En este caso, deberá disponer, además del equipo de transmisión de datos con el exterior, de una cuenta en la otra red que le permita realizar la conexión.

En ambos casos, se deberá contratar con una compañía de teléfonos el sistema de comunicaciones que cubra las necesidades de la empresa y permita establecer la comunicación con Internet.

Si desea que todos los ordenadores de la intranet tengan acceso a Internet, tiene dos opciones:

- Mediante hardware. Utilizando un encaminador (router) que se encargará de administrar los requerimientos de los ordenadores que este configurado para que sirva de puerta de enlace.
- Mediante software. Utilizando un ordenador como servidor proxy que se encargará de redirigir los requerimientos de los ordenadores (habrá que ser configurado para que reciba todos los requerimientos).

5.6.- Seguridad de TCP/IP.

La seguridad es una preocupación importante siempre que se conecta una red al exterior.
El software básico de TCP/IP no cifra los datos por sí mismo y por ello deberá realizarlo la aplicación. Si no se cifran los datos, la contraseña se enviará en texto plano y podrá ser leída fácilmente durante el trayecto por personas que dispongan de medios y conocimientos. Es importante que los datos (sobre todo la contraseña) vayan cifrados para evitar que sean examinados por personas ajenas.

5.6.1.- Cortafuegos.

Otra opción es mantener alejadas del sistema a todas aquellas personas ajenas. Para ello lo mejor es instalar un cortafuegos (firewall).
Su función es filtrar los intentos de establecimiento de conexión de forma que se pueda detectar e impedir el acceso al sistema a posibles intrusos sin que ni siquiera se haya llegado a establecer un enlace directo entre ellos.
El cortafuegos puede ser configurado para permitir que solo determinadas direcciones, origen y destino, puedan acceder a la red (o desde ella).
Las funciones de cortafuegos se pueden realizar por:

- Ordenadores dedicados exclusivamente al filtrado de paquetes.
- Encaminadores de red (routers) configurados para esta tarea.
- Programas de software para distintos sistemas operativos.
- Cualquier otro dispositivo intercalado entre la red y el exterior que soporte el filtrado de paquetes según unos parámetros previamente definidos.

Entre los posibles beneficios de utilizar cortafuego s se encuentran:

- Acceso controlado a la red.
- Protección para servicios de Internet que sean vulnerables.
- Administración de seguridad centralizada.
- Estadísticas de las conexiones a la red.
- Filtrado sofisticado de paquetes.
- Configuración desde un sistema de hardware independiente que no dependa de ningún otro sistema de hardware y software.

Entre las posibles razones para no utilizar un cortafuegos se encuentran:

- El acceso a los servicios deseados puede llegar a ser más complejo de lo normal.
- El peligro de acceso por una puerta trasera a la red se incrementa si no se tiene prevista su inutilización.
- Es necesario una administración suplementaria de la red.
- El costo económico es mayor.
- La configuración se hace demasiado compleja para realizarla de forma adecuada por un usuario sin experiencia.

La implementación de un cortafuegos requiere las siguientes tareas:

1. Determinación de los requerimientos. Es decir, decidir los servicios de niveles de acceso que se incluirán en la configuración de conectividad. Por ejemplo, puede no ser necesario dar servicio FTP pero sí HTTP. Para ello puede ser útil establecer una matriz con protocolos como columnas y aplicaciones como filas.
2. Establecer una política de seguridad. Es preciso definir en primer lugar qué necesita ser protegido y qué tipo de acceso se va a permitir tanto a los usuarios internos hacia el exterior como a los agentes externos hacia el interior. Hay que tener en consideración los puntos remotos de acceso, el nivel de acceso a internet, correo electrónico, cómo se va a implementar la autenticación y el cifrado, reglas de construcción y validez de passwords, etc...

3. Diseño de la arquitectura. Es el momento de tener en cuenta las consideraciones de diseño del cortafuegos y su conexión con el mundo interior/exterior. La arquitectura más común incluye la creación de una zona neutral (DMZ), especialmente en casos de extranets, servidor web, o cuando hay un conjunto de modems que permiten el acceso a través de conexiones telefónicas conmutadas.
4. Instalar y configurar el sistema. Una vez elegido el cortafuegos, debe configurarse según las instrucciones del fabricante para implementar en él las reglas que se ajusten a lo establecido en los puntos 1 y 2. Es importante probar el cortafuegos a fondo una vez configurado. Cualquier descuido u omisión puede producir un agujero de seguridad. Hay herramientas en el mercado para probar este tipo de sistemas y producir informes con los agujeros detectados.
5. Monitorización. Los cortafuegos normalmente son capaces de construir un registro con los eventos que tienen lugar durante su funcionamiento (ficheros log). Es importante revisar con regularidad estos registros buscando elementos "sospechosos": direcciones IP, uso excesivo de ciertos puertos, etc...

5.6.2.- Servidores Proxy.

Un servidor proxy es un dispositivo estrechamente ligado a un cortafuegos hasta el punto que en ocasiones ambos son la misma máquina. Para algunos autores los proxy son un tipo especial de cortafuegos. La diferencia fundamental reside en que el cortafuegos trabaja a nivel de la capa de red (esquema OSI), mientras que el proxy trabaja a nivel de la aplicación.

El proxy se puede implementar también por software. Incluso hay aplicaciones baratas de fabricantes como Microsoft que permiten instalar un proxy en un simple PC con Windows 95.

En una organización que tenga acceso a internet, el proxy actúa como intermediario entre las estaciones de trabajo de los usuarios internos y los servicios externos proporcionados por la red. Cuando un cliente desea un servicio, por ejemplo una página web, se lo pide al proxy el cual realiza la conexión en su lugar. El funcionamiento en este típico ejemplo es el siguiente:

El proxy recibe una petición para un servicio desde la dirección de un usuario. Entonces filtra la petición de acuerdo a las reglas establecidas por el administrador. A continuación busca la página solicitada en su cache. En caso de no existir en la cache, el proxy usa una de sus direcciones legales para conectarse con la URL solicitada y le devuelve la información solicitada al cliente que realizó la petición. Para el usuario, el proxy es invisible. Todas las peticiones vienen aparentemente del servidor de Internet direccionado. El usuario tan solo tiene que tener configurada la dirección del proxy como una opción de su navegador.

En este ejemplo se han puesto de manifiesto dos de las principales características de
Un servidor proxy:

- Permite "aislar" a la red del mundo exterior y utilizar cualquier conjunto de direcciones IP en nuestra intranet. El único que aparece con dirección "legal" en Internet es el propio proxy. Para cada petición de servicio hace una traslación entre la dirección del cliente y una de las direcciones legales asignadas.
- Hace funciones de cache. Es muy común que dentro de la misma organización los usuarios trabajen sobre las mismas URL's. Por este motivo, la probabilidad de que una petición de una dirección web sea servida directamente desde la cache del proxy es relativamente alta. Esto supone un impacto considerable en el rendimiento y en el tiempo de respuesta de cara al usuario.

En ocasiones el proxy también es capaz de analizar tráfico de entrada. En estos casos, la frontera entre proxy y cortafuegos es muy delgada. Es común tener el proxy y el cortafuegos en la misma máquina, formando un único paquete.

Ahora bien, todos los sistemas de seguridad perimetral son ineficientes si nuestra intranet tiene "puertas traseras", es decir servidores que permiten la conexión de máquinas remotas a través de servicios de acceso tales como Microsoft Remote Access Service (RAS). En estos casos, todas las posibilidades de conexión deben ser cuidadosamente analizadas en busca de posibles agujeros. Para estas conexiones es imprescindible el uso de una buena disciplina en la configuración de contraseñas y el uso de medidas adicionales de seguridad como la autenticación y la retrollamada preestablecida (call-back).

5.7.-Protocolos de seguridad.

En los diseños de redes intranet/extranet es preciso contar también con sistemas para autenticación, identificación y encriptación de los datos transmitidos, especialmente en el caso de extranet donde hay acceso a nuestros sistemas desde el mundo exterior, máxime si se realizan transacciones de comercio electrónico. Existen diversos protocolos que permiten garantizar tal necesidad de seguridad en las conexiones.

Estos protocolos tienen por objeto garantizar la firma, autenticación y encriptación para las peticiones y respuestas ofrecidas por los clientes y servidores. No todos están implementados en todos los navegadores y servidores web, pero su utilización en la red está cada vez más extendida.

La siguiente tabla muestra la relación entre los protocolos de seguridad aquí expuestos y la aplicación o servicio al que va cada uno de ellos dirigido:

Tabla 5.1.-servicios y protocolos.

SERVICIO	PROTOCOLO
WEB	S-http
Correo electrónico	PGP, S-MIME
Protocolos de la capa superior	SSL
TCP/IP	TCP/IP IPSEC
Enlace de datos	Encriptación por hardware

5.7.1.- SSL (Secure Sockets Layer).

Es un protocolo ampliamente usado para aportar seguridad a la transmision por internet.

Se trata de un protocolo situado entre la capa de TCP/IP y la capa de aplicación. Por tanto, puede ser utilizado con cualquier protocolo de este nivel de aplicación, como por ejemplo

HTTP o FTP. Permite la seguridad de los datos en las comunicaciones: identificación de servidor, cifrado e integridad de datos, mediante un mecanismo de negociación entre el servidor y el cliente, previo al envío de información encriptada entre los mismos.
Desarrollado por Netscape, en la actualidad los servidores web más extendidos, tales como Microsoft Internet Information Server (IIS), así como los navegadores (browsers) en sus versiones actuales proporcionan soporte para SSL. Se está trabajando en una versión avanzada de SSL denominada TLS (Seguridad de la capa de transporte).
SSL usa mecanismos de cifrado de clave pública y privada, incluyendo un certificado digital. Como algoritmo de cifrado de clave pública utiliza RSA, mientras que los algoritmos de clave privada son algoritmos de cifrado de bloque (como por ejemplo DES), aunque la elección de este algoritmo depende de la implementación de SSL. Si un sitio web está alojado en un servidor que soporta SSL, entonces se puede activar el mecanismo para identificar a las páginas como "seguras" requiriendo acceso vía SSL.

Puede ser usado en cualquier servidor usando la librería SSLRef de Netscape, que puede ser descargada gratuitamente para uso no comercial, o adquirida bajo licencia para uso comercial.

La negociación entre servidor y cliente se realiza en dos fases:

1. Se negocia en primer lugar una clave simétrica válida exclusivamente para esa sesión.
2. Se realiza la transferencia de paquetes de datos cifrados con dicha clave.

El mecanismo es transparente para las aplicaciones finales, las cuales simplemente saben que el canal establecido entre el navegador y el servidor seguro se encarga de proporcionan confidencialidad entre extremos. El cliente (navegador) contiene claves públicas de ciertas Entidades de Certificación Autorizadas. Cuando entra en contacto con el servidor seguro, éste le envía su clave pública, rubricada por la entidad correspondiente y la identificación se lleva a cabo enviando al servidor un mensaje de tipo aleatorio que éste debe firmar, garantizando así al cliente su identidad.

Una vez verificada la identidad del servidor, el cliente genera una clave de sesión y la envía cifrada con la clave pública del servidor. Finalizada esta fase, ya puede comenzar el diálogo y la transmisión de datos entre ambos, bajo la seguridad proporcionada por el cifrado de la conversación mediante la clave privada que sólo ellos conocen.

SSL es una alternativa a otro protocolo de seguridad S-HTTP, ambos soportados por los navegadores actuales. SSL es un standard de hecho, aunque ha sido propuesto al IETF (Internet Engineering Task Force) como un standard oficial.

5.7.2.- S-HTTP (Secure HTTP).

S-HTTP es una extensión de HTTP que permite el intercambio seguro de ficheros y datos en la World Wide Web, al igual que SSL. Su mayor diferencia frente a SSL reside en el hecho de permitir al cliente enviar un certificado para autentificar al usuario, mientras que SSL sólo permite autenticación del servidor.

Fue desarrollado originalmente por CommerceNet para difundir el uso del comercio electrónico en internet.

Está basado en HTTP, aunque soporta distintos formatos de encriptación de mensajes mediante una negociación entre cliente y servidor, para lo cual existen dos modalidades: utilizar una clave privada de encriptación y la parte contraria una clave pública para desencriptar, o bien utilizar una clave de sesión establecida con anterioridad entre las partes.

También ha sido enviado al IETF para ser definido como estándar. Una descripción de S-HTTP en detalle se puede encontrar en el documento RFC Internet Draft 2660.

5.7.3. - S/MIME (Secure Multipurpose Internet Mail Extension).

Es un mecanismo para cifrado de correo electrónico, al igual que PGP. Utiliza certificaciones digitales para correo seguro y debe utilizarse junto con una autoridad o Entidad de Certificación.

S/MIME está basado en el algoritmo de RSA, y también está incluido en las versiones más recientes de los navegadores y otros productos de correo electrónico. La sintaxis de S/MIME está descrita en el documento PKCS-7 (Public- Key Cryptography Standard)

5.7.4.- PGP (Pretty Good Privacy).

Creado por Phil Zimmerman en 1991, se trata de una sólida herramienta para cifrar correo electrónico mediante clave pública, muy resistente a los intentos de violación. Se usa también para enviar una firma digital encriptada que permite al destinatario verificar la identidad del remitente y garantizar que el mensaje no ha sido alterado durante su transporte por la red.

Es en realidad una mezcla de RSA e IDEA (algoritmo internacional de cifrado de datos). Se puede utilizar para crear una firma digital mediante el cifrado de caracteres que se añaden al final del documento, lo que permite verificar que el documento y la firma digital coinciden. Si se altera un solo carácter del documento, la firma no podrá ser verificada.

También hay versiones de PGP basados en Diffie-Hellman y CAST. El principio de funcionamiento de PGP es muy simple. Usa un cifrado rápido mediante una clave corta para el mensaje a transmitir y después usa la clave pública para cifrar dicha clave corta. A continuación, envía al destinatario el mensaje cifrado y la clave corta, la cual es descifrada mediante la clave privada del destinatario para después descifrar con ella el mensaje.

Para usar PGP hay que descargar una versión (gratuita o bajo licencia) e instalarla en el ordenador. Suele contener un interface que se integra con el agente de correo electrónico.

Por último, hay que registrar la clave pública en algún servidor de PGP público, de modo que los destinatarios de los mensajes puedan encontrar nuestra clave pública. Network Associates contiene un servidor LDAP/HTTP con más de 300.000 claves públicas.

Aunque su uso principal y original es el cifrado de mensajes de correo electrónico, en la práctica se usa también en otro tipo de aplicaciones.

5.7.5.- SET (Secure Electronic Transaction).

Se trata de una extensión de SSL, desarrollada por compañías de medios electrónicos de pago (principalmente VISA, MasterCard y American Express) para fomentar el uso de las tarjetas de crédito como mecanismo de pago a través de internet.

SET garantiza la seguridad de todas las partes implicadas en una transacción electrónica y garantiza la privacidad de la transacción, contando con el apoyo de muchos de los

fabricantes de software y hardware, por lo que nace con vocación de convertirse en el estándar de facto para la realización de pagos electrónicos.

Mediante SET, el usuario recibe una "cartera electrónica", que no es más que un certificado digital. Las transacciones se llevan a cabo y son verificadas usando una combinación de certificados digitales y firmas digitales entre el comprador, el comercio, y el banco del comprador, garantizando en todo momento la privacidad y confidencialidad. SET hace uso de SSL, STT (Microsoft Secure Transaction Technology) y S-HTTP.

Funciona de la siguiente manera, suponiendo que el cliente tiene un navegador SET y que los servidores involucrados también soportan SET:

1. El cliente abre una cuenta en una entidad de crédito: VISA, MasterCard, etc...
2. El cliente recibe un certificado digital, que no es más que un fichero que funciona como una tarjeta de crédito con su fecha de caducidad, y una clave pública.
3. Los comercios también reciben certificados desde las entidades de crédito, que incluyen la clave pública del comercio y la clave pública de la entidad de crédito
4. El cliente realiza una compra a través de la web.
5. El navegador del cliente recibe el certificado del comercio y confirma que es válido.
6. El navegador emite la información del pedido: El mensaje se encripta con la clave pública del comercio, la información del pago es encriptada con la clave pública de la entidad (por lo que el comercio no puede verla) y otra información que garantiza que el pago sólo puede ser usado con este pedido.
7. El comercio verifica el cliente chequeando la firma digital de su certificado.
8. El comercio envía el mensaje del pedido a la entidad de crédito, incluyendo la clave pública de la entidad, la información de pago del cliente y el certificado del comercio.
9. La entidad verifica el comercio y el mensaje, usando la firma digital del certificado del mensaje, y verifica también la información de pago.
10. La entidad firma digitalmente y envía autorización al comercio para que acepte el pedido.

5.7.6.- Seguridad del protocolo de internet.

La Seguridad del protocolo de Internet (IPSec) permite:

- Una protección eficaz contra redes privadas y ataques de Internet.
- Un conjunto de servicios de protección basados en criptografía y protocolos de seguridad.
- Proteger el contenido de los paquetes IP.
- La capacidad de proteger la comunicación entre grupos de trabajo, equipos de redes privadas, dominios, sitios, sitios remotos, extranets y clientes de acceso telefónico.
- Seguridad de principio a fin. Los únicos equipos que deben conocer que el tráfico está protegido son los equipos remitente y receptor. Este modelo permite implementar IPSec correctamente en los casos siguientes:
- Red de área local (LAN): cliente-servidor y entre iguales.
- Red de área extensa (WAN): entre enrutadores y entre puertas enlace.
- Acceso remoto: cliente de acceso telefónico y acceso a Internet desde redes privadas.

5.8.- La seguridad de la red.

IPSec se implementa en la capa Internet de la pila de protocolos TCP/IP (que coincide con la capa de red del modelo de referencia OSI) y activa un nivel alto de protección por lo que no es necesario realizar ningún cambio en las aplicaciones existentes o en el sistema operativo. Otros mecanismos de seguridad que operan encima de estas capas sólo proporcionan seguridad en las aplicaciones que saben cómo utilizar dichos mecanismos, como Secure Sockets Layer (SSL) que opera en las capas de transporte y aplicación de la pila de protocolos TCP/IP.

La implementación de IPSec en la capa Internet proporciona protección para todos los protocolos IP y de capa superior dentro del conjunto de protocolos TCP/IP (por ejemplo, TCP, UDP, ICMP). La primera ventaja de asegurar información en esta capa es que todas las aplicaciones y servicios que utilizan IP para el transporte de datos se pueden proteger con IPSec, sin que se produzca ninguna modificación en estas aplicaciones o servicios (para asegurar otros protocolos distintos de IP, se han de encapsular los paquetes mediante

IP).

5.8.1.- Protección basada en criptografía.

IPSec protege los datos de modo que a un intruso le resulte bastante difícil ser interpretados. Para proteger la información se utiliza una combinación formada por un algoritmo y una clave. Mediante las claves y los algoritmos basados en criptografía que consigue un alto grado de seguridad. Una clave es el código, o el número secreto necesario para leer, modificar o comprobar los datos protegidos. Las claves se utilizan junto con algoritmos (un proceso matemático) para proteger los datos.

Se reduce significativamente la posibilidad de que se produzcan ataques a través de la red gracias a las siguientes características:

- Administración automática de claves.
- Generación de claves. Para hacer posible una comunicación segura los equipos deben poder establecer la misma clave compartida, ser transmitida a través de la red. Para ello, inician el cálculo utilizando el algoritmo Diffie-Hellman y después intercambian un resultado intermedio de forma pública y segura mediante la autenticación, ninguno de los equipos envía la clave real. A partir de la información compartida en el intercambio, cada equipo genera una clave secreta, que es la misma en los dos casos. Los usuarios expertos pueden cambiar la configuración predeterminada de la clave de cifrado de datos y del intercambio de claves.
- Longitud de las claves. Cada vez que se incrementa en un bit la longitud de una clave, el número de claves posibles se duplica, con lo que se dificulta exponencialmente el descubrimiento de la clave. La negociación de la seguridad IPSec entre dos equipos genera dos tipos de claves secretas compartidas: claves maestras y claves de sesión.
- Las claves maestras o principales se utilizan para generar las claves de sesión. Pueden se1eccionarse entre 768, 1.024 ó 2.048 bits denominadas grupo Diffie-Hellman Menor (1), Medio (2) y Alto (2048), respectivamente. Su duración corresponde a la duración de la asociación de seguridad de IKE y suele ser prolongada (por defecto es de ocho horas). Su generación consume muchos más recursos que la generación de las claves de sesión.
- Las claves de sesión se utilizan para proteger los datos durante el tráfico entre el

equipo emisor y el receptor, y tienen duraciones basadas en la cantidad de datos enviados y el tiempo transcurrido desde que se empezó a utilizar la clave.

- Generación dinámica de claves. Se puede generar automáticamente claves nuevas durante una comunicación. Así se evita que un intruso tenga acceso a toda la comunicación mediante una sola clave. Los usuarios expertos pueden cambiar los intervalos predeterminados para la generación de claves.

5.8.2.- Servicios de seguridad.

- Integridad. Se protege la información durante la comunicación de modificaciones no autorizadas, lo que garantiza que la información recibida coincide exactamente con la enviada. Se utilizan las funciones hash para marcar o señalar de forma única cada paquete. El equipo remitente utiliza una función hash y una clave compartida para calcular el código de integridad de mensajes (MIC) que es una suma de comprobación criptográfica y la incluye en el paquete. El equipo receptor antes de abrir el paquete comprueba el código de integridad de mensajes (MIC) utilizando la misma función hash sobre el mensaje recibido con la clave compartida y compara el resultado con el original. Si ha cambiado entonces también habrá cambiado el paquete, éste se descarta para evitar un posible ataque a través de la red.

- MD5 (Message Digest 5) que se basa en la RFC 1321. Realiza cuatro pases sobre los bloques de datos y utiliza una constante numérica distinta para cada palabra del mensaje en el número de constantes de 32 bits que se utilizan durante el cálculo de MD5. Produce una función hash de 128 bits que se emplea para comprobar la integridad de los datos.

- SHAl (Secure Hash AIgorithm 1) fue diseñado por el National Institute of Standard and Technology. Se basa en gran medida en el de MD5. El cálculo SHA1 produce una función hash de 160 bits que se utilizan para comprobar la integridad de los datos. Las mayores longitudes de hash suponen una mayor seguridad, por lo que es más efectivo que MD5.

- Autenticación. Comprueba que un mensaje sólo puede provenir de un equipo que conoce la clave secreta compartida. El remitente (con el mensaje) proporciona un código de autenticación de mensaje, cálculo que incluye la clave secreta compartida. El receptor realiza el mismo cálculo y si el resultado no coincide con el código de autenticación que se encuentra en el mensaje, éste se descarta. El código de autenticación del mensaje coincide con la suma de comprobación criptográfica utilizada para comprobar la integridad.
- Confidencialidad. Se garantiza que los datos sólo serán revelados a los destinatarios previstos. Los datos de los paquetes se cifran de la transmisión, con lo que se asegura que no se pueden leer durante la misma, aunque el paquete sea supervisado o interceptado por un intruso. Sólo los equipos que tengan la clave secreta compartida pueden interpretar o modificar los datos.

Se utilizan los siguientes algoritmos para el cifrado de los datos:

- DES. Aplica un cifrado por bloque (es decir, se aplica a bloques de datos de tamaño fijo) con una clave de 56 bits. Cifra datos en bloques de 64 bits con una clave de 64 bits (aunque la clave parece tener 64 bits, como un bit de cada 8 se utiliza la comprobación de errores, da un resultado de 56 bits útiles).
- 3DES. Proporciona un elevado nivel de seguridad, ya que procesa cada bloque tres veces utilizando una clave única de 56 bits cada vez (por eso, se denomina algoritmo triple DES). El proceso que sigue es el siguiente:

  1. Cifra el bloque con la clave 1.
  2. Descifra el bloque con la clave 2.
  3. Cifra el bloque con la clave 3.

Este proceso se invierte si el equipo descifra un paquete.

También, se utiliza el encadenamiento de bloques de cifrado (CBC) para ocultar los patrones de bloques de datos idénticos dentro de un paquete. Como primer bloque aleatorio se utiliza un vector de inicialización (un número aleatorio inicial) para cifrar y descifrar un

bloque de datos. Para cifrar cada bloque sucesivo se utilizan distintos bloques aleatorios junto con la clave secreta. Así se garantiza que los conjuntos idénticos de datos sin proteger (texto sin cifrar) se convierten en bloques de datos cifrados únicos.

- Aceptación o imposibilidad de repudio. Se garantiza que el remitente de un mensaje es la única persona que puede haber enviado el mensaje o el remitente no puede negar que ha enviado el mensaje.

Reproducción no permitida (también se conoce como impedimento de reproducción o prevención de repetición). Garantiza la unicidad de cada paquete. Asegura que los datos capturados por un intruso no se puedan volver a utilizar ni reproducir para establecer una sesión u obtener acceso a la información sin autorización.

5.8.3.- Modo de transporte.

El modo de transporte es el predeterminado para IPSec y se utiliza para comunicaciones extremo a extremo. Cuando se utiliza el modo de transporte, sólo se cifra la carga IP. El modo de transporte proporciona la protección de una carga IP. Una carga IP típica es un segmento TCP (con su encabezado TCP), un segmento UDP [con su encabezado UDP] y un mensaje ICMP (con su encabezado ICMP) mediante un encabezado AH o ESP:

- Encabezado de autenticación (AH). Proporciona autenticación, integridad y antirreprodución para todo el paquete. AH firma el paquete entero pero no cifra la información, por lo que no proporciona confidencialidad. La información es legible, pero está protegida contra modificaciones. Utiliza algoritmos hash con claves que se denominan HMAC (Códigos hash de autenticación de mensajes), para firmar el paquete.

- Carga de seguridad de encapsulación (ESP). Proporciona confidencialidad (además de autenticación, integridad y antirreprodución) para la carga IP. No firma normalmente el paquete entero (a no ser que se esté realizando un túnel), ya que sólo protege la información y no el encabezado. Puede utilizarse por sí solo o en combinación con AH.

5.8.4.- Agente de directivas IPSec.

El Agente de directivas IPSec es un servicio que reside en cada equipo Windows Server 2003 y que se muestra en la lista de servicios del equipo Servicios IPSec (se inicia automáticamente al iniciar el sistema). Permite recuperar información de la directiva de IPSec activa y transferirla a otros componentes IPSec que requieren que dicha información realice los servicios de seguridad.

5.8.5.- Negociación de seguridad IPSec.

Antes de que se pueda intercambiar información segura, debe establecerse un acuerdo de seguridad entre los dos equipos. Con el fin de establecer este acuerdo el Internet Engineering Task Force (IETF) ha establecido un método de asociacion de seguridad y resolución de intercambio de claves deno. Intercambio de claves de Internet (IKE, Internet Key Exchange) que:

- Centraliza la administración de asociacion de seguridad, reduciendo el tiempo de conexión.
- Genera y administra las claves secretas compartidas que se utilizan para proteger la información.

Se denomina a este acuerdo asociación de seguridad (SA) y es una combinación de una clave negociada, un protocolo de seguridad y el índice de parámetros de seguridad (SPI), que conjuntamente definen el método de seguridad utilizado para proteger la comunicación desde el remitente al receptor (el indice de parámetros de seguridad [SPI] es un valor único e identificable en la SA utilizado para distinguir entre múltiples asociaciones de seguridad que existen en el receptor).

Para garantizar una comunicación segura y con éxito, IKE funciona en fases. La confidencialidad y la autenticación se aseguran durante cada una de las funciones mediante el uso del cifrado y los algoritmos de autenticación acordados entre los dos equipos durante las negociaciones de seguridad. Al estar las tareas divididas entre las dos fases se agiliza la creación de claves.

En la primera fase, los dos equipos establecen un canal seguro y autenticado (es la denominada fase I o SA de modo principal). En ella IKE proporciona automáticamente la

protección de identidad necesaria para este intercambio.
En la segunda fase, las SA negocian en nombre del controlador de IPSec (es la denominada Fase II o SA de modo rápido).

5.8.6.- Funcionamiento de IPSec.

Para simplificarlo, este ejemplo ilustra el proceso que siguen los componentes entre dos equipos de una intranet:

1. El usuario 1 del equipo A envía un paquete IP de aplicación al usuario 2 que se encuentra en el equipo B.
2. El controlador IPSec del equipo A comprueba sus listas de filtros IP de salida y determina los paquetes que deben protegerse.
3. El controlador IPSec notifica a IKE para que inicie la negociación de seguridad con el equipo B.
4. El servicio IKE del equipo A completa una búsqueda de dirección utilizando su propia dirección IP como origen y la dirección IP equipo B como destino. La coincidencia del filtro de modo principal determina la configuración de SA de modo principal que el equipo A propone al equipo B. El equipo A envía el primer mensaje de IKE en modo principal mediante el puerto de origen UDP 500 y puerto destino UDP 500. Los paquetes de IKE reciben un procesamiento especial por parte del controlador IPSec para omitir los filtros.
5. El equipo B recibe un mensaje de modo principal de IKE. Utiliza la dirección IP de origen y la dirección IP destino del paquete UDP para realizar una búsqueda de directivas en modo principal y determinar la configuración de seguridad que se acordó. El equipo B tiene un archivo de modo principal que coincide y que responde para iniciar la negociación de la SA de modo principal.
6. El equipo A y el equipo B negocian opciones, intercambian identidades, comprueban la confianza de dichas identidades (autenticación) y generan una clave principal compartida. Han establecido una SA de modo principal de IKE. El equipo A y el equipo B deben confiar mutuamente entre sí.
7. El equipo A realiza una búsqueda de directiva de modo rápido de IKE utilizando el filtro completo con el que el controlador de IPSec hizo coincidir el paquete de

salida. El equipo A selecciona la configuración SA de modo rápido y la propone (junto con el filtro de modo rápido equipo B).

8. El equipo B realiza también una búsqueda de directiva de modo rápido IKE mediante la descripción del filtro ofrecida por el equipo A. El equipo B selecciona las opciones de seguridad requeridas por su directiva y compara con las ofrecidas por el equipo A. El equipo B acepta conjunto de opciones y completa el resto de la negociación de modo rápido de lKE para crear un par de SA, una SA es para el tráfico entrante y otra para el tráfico saliente. El SPI insertado en el encabezado IPSec de cada paquete enviado identifica las SA.
9. El controlador de IPSec del equipo A utiliza la SA saliente para firmar los paquetes y si es necesario cifrarlos. Si el adaptador de red puede realizar una descarga de hardware de funciones criptograficas de IPSec, el controlador IPSec da formato a los paquetes, pero no realiza las funciones criptográficas de IPSec.
10. El controlador de IPSec envía los paquetes al controlador del adaptador de red e indica si el adaptador debe realizar funciones criptográficas de IPSec. El adaptador de red transmite los paquetes a la red.
11. El controlador del adaptador de red del equipo B recibe los paquetes cifrados de la red. El receptor de un paquete IPSec utiliza el SPI para buscar la SA correspondiente, con las claves criptográficas necesarias para comprobar y descifrar los paquetes. Si el adaptador de red puede descifrar los paquetes en hardware, comprueba si puede reconocer el SPI. Si no puede descifrar los paquetes en hardware o no puede reconocer el SPI, pasa los paquetes al controlador IPSec.
12. El controlador IPSec del equipo B utiliza el SPI de la SA de entrada para recuperar las claves necesarias para validar la autenticación e integridad y si es necesario descifrar los paquetes.
13. El controlador IPSec convierte los paquetes de formato IPSec a formato de paquete IP estándar. Pasa los paquetes IP validados y descifrados al controlador TCP/IP que a su vez los pasa a la aplicación receptora del equipo B.
14. Las SA siguen ofreciendo una protección transparente muy segura para el tráfico de datos de la aplicación. Además se actualizan automáticamente a través de una negociación en modo rápido de IKE y da siempre que la aplicación envíe y reciba

datos. Cuando la aplicación deja de enviar y de recibir datos, las SA pasan a inactividad y se eliminan.

15. Normalmente, la SA de modo principal de IKE no se elimina (de manera predeterminada, tiene una duración de 8 horas pero puede configurarse para que dure desde 5 minutos hasta un máximo de 48 horas). Cuando se envíe más tráfico, se negociará automáticamente un nuevo modo rápido para crear dos nuevas SA que protejan el tráfico de la aplicación. Este proceso es rápido debido a que la SA de modo principal ya existe. Si una SA de modo principal caduca se vuelve a negociar automáticamente cuando sea necesario.

Todos los enrutadores o conmutadores del trayecto entre los equipos que se comunican, se limitan a reenviar los paquetes IP cifrados hacia su destino. Sin embargo, si hay un servidor de seguridad, un enrutador de seguridad o un servidor proxy entonces el trayecto es posible si el tráfico IPSec e IKE no se reenvían. Estos dispositivos deben configurarse para permitir que los paquetes IPSec y de protocolo IKE pasen a través de ellos. Si los paquetes IPSec no están cifrados, el servidor de seguridad o el enrutador de seguridad aún pueden inspeccionar los puertos TCP o UDP otro contenido de los paquetes. Si se modifica el contenido de los paquetes después de haber sido enviados, el equipo receptor detectará la modificación y descartará los paquetes.

5.8.7.- Establecer un plan de seguridad de IPSec.

Se trate de un dominio extenso ó de un grupo de trabajo pequeño, el hecho de implementar IPSec supone encontrar un equilibrio entre hacer que la información este disponible sin dificultades para el mayor número de usuarios y proteger la información delicada contra el acceso sin autorización.

Para encontrar el equilibrio adecuado es necesario:

- Valorar el riesgo y determinar el nivel de seguridad apropiado para la organización.
- Identificar la información de valor.
- Definir las directivas de seguridad que utilicen los criterios administrativos de riesgo y que protejan la información identificada.
- Determinar el modo de implementar las directivas dentro de la organización.

- Asegurar que los requisitos de administración y tecnología están vigentes.
- Proporcionar a todos los usuarios un acceso seguro y eficaz a los recursos adecuados.

No existe una definición exacta de las medidas que definen la seguridad estándar. Estas pueden variar mucho, dependiendo de las directivas e infraestructura de la organización. Los siguientes niveles de seguridad se pueden considerar como una base general para la planificación de la implementación de IPSec:

- Seguridad minima. En ella, los equipos no intercambian los datos confidenciales. Como valor predeterminado, IPSec no está activo y por tanto no es necesaria ninguna acción administrativa para deshabilitar IPSec.
- Seguridad estándar. Los equipos especialmente los servidores de archivos se utilizan para almacenar información de valor. La seguridad se ha de equilibrar para que no se convierta en una barrera para legitimar a los usuarios que intentan realizar sus tareas. Windows 2003 Server proporciona dos directivas de ejemplo que protegen los datos sin aplicar el máximo nivel de seguridad: Client (Respond Only) o Cliente (solo responder) y Server (Request Security) o Servidor (solicitar seguridad).
- Alta seguridad. Los equipos que contienen información muy confidencial están expuestos a robos, ataques accidentales o asaltos al sistema (especialmente en casos de acceso telefónico remoto o cualquier comunicación de red pública). Windows 2003 Server proporciona una directiva de ejemplo que aplica el máximo nivel de seguridad: Secure Server (Require Security) o Servidor seguro (requerir seguridad). Con ella no se permite la comunicación no segura con equipos no compatibles IPSec.
-

5.9.- El servicio de enrutamiento y acceso remoto.

El Servicio de enrutamiento y acceso remoto (RRAS) para Windows Ser 2003 es un enrutador de software provisto de toda clase de características y plataforma abierta para el enrutamiento e interconexión de redes.

Ofrece servicios de enrutamiento en entorno para redes de área local (LL extensa

(WAN), o a través de Internet mediante conexiones seguras de red privada virtual (VPN). Combina e integra los servicios independientes de enrutamiento acceso remoto (RAS) de Windows NT 4. O.

En lo sucesivo, se denominará servidor RAS (servidor de acceso remoto) a equipo que ejecuta Windows Server 2003 y el servicio RRAS suministrará servicios deenrutamiento LAN y WAN.

Un servidor que ejecuta el servicio RRAS ve el equipo instalado para la interconexión de redes como una serie de dispositivos (un dispositivo representa el hardware o el software que crea conexiones punto a punto físicas o lógicas) y puertos (un puerto es un canal de comunicación que admite una única conexión puno a punto).

El servidor RAS está diseñado para ser usado por administradores de sistemas familiarizados con los protocolos y servicios de enrutamiento. Mediante enrutamiento y acceso remoto, los administradores pueden ver a enrutadores y servidores de acceso remoto en sus redes.

Características RRAS

RRAS incluye las características siguientes:

- Enrutamiento de unidifusión multiprotocolo para el protocolo IP y AppleTalk.
- Protocolos estándar de enrutamiento IP de unidifusión: OSPF versiones 1 y 2.
- Servicios de multidifusión IP: IGMP en modo de enrutador IGMP para habilitar el reenvío de tráfico de multidifusión IP.
- Servicios de traducción de direcciones de red (NAT) IP para simplificar interconexión de redes domésticas y la conexión de redes de una oficina doméstica o pequeña (SOHO) a Internet.
- Filtrado de paquetes IP estáticos para seguridad y rendimiento.
- Enrutamiento de marcado a petición a través de vínculos WAN de acceso telefónico.
- Compatibilidad de VPN con el protocolo PPTP y el protocolo L2TP a través de IPSec.

- Compatibilidad estándar con el Agente relé de DHCP para IP.
- Compatibilidad estándar con el anuncio del enrutador mediante el protocolo ICMP.
- Una interfaz gráfica de usuario para la configuración y supervisión remotas.
- Una interfaz de línea de comandos para secuencias de comandos en ejecución, configuración automatizada y supervisión remota.
- Compatibilidad con funciones de administración de energía de Windows.
- Capacidades de administración del protocolo SNMP con compatibilidad con bases de datos de información de administración (MIB).
- Compatibilidad con medios, incluidos Ethernet, Token Ring, FDDI, ATM RDSI, X25, T-Carrier, Frame Relay, xDSL, módems por cable y módems analógicos.
- API para protocolos de enrutamiento, administración y la interfaz de usuario para habilitar el desarrollo de valor agregado.

5.9.1.- El enrutamiento de unidifusión.

El enrutamiento de unidifusión es el reenvío de tráfico destinado a una única ubicación de una interconexión de redes. Una interconexión de redes está compuesta mínimo por dos redes que se conectan mediante enrutadores (encaminadores).

Los equipos de una red pueden enviar paquetes a equipos de otras redes mediante el reenvío de dichos paquetes al enrutador. El enrutador examina el paquete y utiliza la dirección de red de destino del encabezado del paquete para decidir qué interfaz de enrutamiento utilizará para reenviarlo. Mediante los protocolos de enrutamiento (OSPF, RIP, etc.), aprende información de red de los enrutadores vecinos y a continuación, la propaga a enrutadores de otras redes para habilitar la conectividad entre todos los equipos de todas las redes.

El servidor RAS puede encaminar tráfico IP y AppleTalk.

5.9.2.- Enrutamiento IP.

El enrutamiento IP consiste en el reenvío de tráfico IP desde un equipo a través de encaminadores IP. En cada encaminador, el siguiente salto se determina al hacer coincidir la dirección IP de destino del paquete con la mejor ruta de la tabla de enrutamiento.

El servidor RAS incluye soporte para dos protocolos de enrutamiento unidifusión IP: RIP y OSPF (otros fabricantes pueden crear otros protocolos de enrutamiento IP adicionales, como IGRP o BGP).

5.9.3.- El enrutamiento de multidifusión.

La unidifusión es el envío de tráfico de red a un equipo especificado. La multidifusión es el envío de tráfico de red a un grupo de equipos. Únicamente aquellos miembros del grupo de equipos que estén escuchando el tráfico multidifusión (el grupo de multidifusión) procesarán dicho tráfico. Los demás nodos pasaran por alto el tráfico de multidifusión.
Se puede utilizar el tráfico de multidifusión para:

- Descubrir recursos en la interconexión de redes.
- Admitir aplicaciones de transmisión de datos como la distribución de archivos o la sincronización de bases de datos.
- Admitir aplicaciones multimedia de multidifusión como video y audio digitalizado.

Windows Server 2003 admite el reenvío de multidifusión (es el reenvió inteligente del tráfico de multidifusión) y el enrutamiento de multidifusión (es propagación de información de escucha de grupos de multidifusión).

5.10.- Compartir conexión a internet.

Con la opción Compartir conexión a Internet de Conexiones de red puede utilizar Windows Server 2003 para conectar una red local pequeña a Internet.
Al habilitar esta opción en un equipo, se proporcionarán servicios de traducción, direcciones de red (NAT), direccionamiento y servicios de nombres a todos equipos de la red.
Después de que se habilite la Conexión compartida a Internet y de que se prueben las opciones de red e Internet, los usuarios de redes pequeñas pueden utilizar Internet Explorer y Outlook Express como si estuvieran conectados a un Proveedor de servicios Internet (ISP). El equipo que comparte la conexión a Internet marca el número del ISP y crea la conexión para que el usuario pueda tener acceso a la dirección Web indicada (los equipos

deberán configurar TCP/IP en su conexión de área local para obtener automáticamente una dirección IP).

No deberá utilizar Conexión compartida a Internet en redes que se conecten directamente a redes de SOHO, para conectar redes dentro de una intranet; para conectar directamente las redes de una sucursal con una red.

Si los usuarios de una red pequeña necesitan acceder a una red corporativa que conectada a Internet a través de un servidor de túnel desde una red con conexión compartida a Internet, deberán crear una conexión de red privada virtual (VPN) desde el equipo de la red que tiene la conexión compartida a Internet hasta el servidor de tunel corporativo (la conexión VPN quedará autenticada y protegida, y la creación de la conexión mediante el túnel asigna las direcciones IP, direcciones de servidores DNS - servidores WINS apropiadas para la red corporativa).

5.10.1.- Traducción de direcciones de red (NAT).

Para comunicarse en Internet, deberán utilizarse direcciones asignadas por el de información de redes de Internet (InterNIC). Como éstas direcciones recibir tráfico de Internet, se conocen como direcciones IP públicas.

A una red pequeña se le asigna una dirección (o direcciones) IP pública desde su proveedor de servicios Internet (ISP) que ha contratado un intervalo de direcciones publicas.

Para permitir que varios equipos de una red pequeña se conecten a Internet, cada equipo deberá tener su propia dirección IP pública (este requisito supone un gran costo)

Para evitarlo, se pueden utilizar para la red privada un conjunto reservado de direcciones IP privadas para su utilización fuera de la red pública y realizar una conversión a una dirección IP pública. Dichas direcciones IP privadas pueden ser cualquiera dentro de los siguientes rangos:

- Desde la dirección 10.0.0.0 hasta la dirección 10.255.255.255 (máscara de red 255.0.0.0).
- Desde la dirección 172.16.0.0 hasta la dirección 172.31.255.255 (máscara de red 255.255.0.0).
- Desde la dirección 192.168.0.0 hasta la dirección 192.168.255.255 (máscara de red 255.255.255.0).

Con la traducción de direcciones de red (NAT), se puede configurar una red pequeña para compartir una única conexión a Internet. Consta de los componentes siguientes:

- Componente para la traducción. Traduce las direcciones IP privadas y los números de puerto TCP/UDP de los paquetes que se reenvían entre la red privada e Internet a una dirección IP pública.
- Componente para el direccionamiento. Proporciona información de configuración de las direcciones IP a los demás equipos de la red. Es un servidor DHCP simplificado que asigna una dirección IP, una máscara de subred, una puerta de enlace o gateway predeterminada y la dirección de un servidor DNS. Es necesario configurar los equipos de la red cormo clientes DHCP para recibir la configuración IP automáticamente.

- Componente para la resolución de nombres. Actúa como un servidor DNS para los demás equipos de la red. Cuando el equipo de traducción de direcciones de red recibe las peticiones de la resolución de nombres, las reenvía a los servidores DNS situados en Internet para los que esta configurado y devuelve las respuestas al equipo de la red interna.

Como la traducción de direcciones de red incluye componentes para el direccionamiento y la resolución de nombres que suministran servicios DHCP y DNS, los equipos de la red privada no podrán ejecutar:

- El servicio DHCP, ni el Agente de retransmisión DHCP, si es habilitado el direccionamiento de la traducción de direcciones de red.
- El servicio DNS, si está habilitada la resolución de nombres de red TCP/IP de la traducción de direcciones de red.

El servidor RAS admite el filtrado de paquetes IP que se utilizará para especificar el tipo de tráfico que se permite entrar y salir del enrutador. Se pueden establecer filtros de paquetes por interfaz y configurados para:

- Dejar pasar todo el tráfico excepto los paquetes prohibidos por filtros.
- Descartar todo el tráfico excepto los paquetes permitidos por filtros.

El Agente de retransmisión DHCP proporcionado con el servidor RAS es un agente de retransmisión con el protocolo Bootstrap (BOOTP) que retransmite mensajes entre los clientes DHCP y los servidores DHCP en distintas redes IP. En los segmentos de red IP que contienen clientes DHCP, se requerirá un servidor DHCP o un equipo que funcione como Agente de retransmisión DHCP.

5.10.2.-Servicio de Acceso Remoto (RAS).

El servicio de acceso remoto que forma parte de los servicios integrados de enrutamiento y acceso remoto (RRAS) permite conectar a los empleados que se encuentran en puntos remotos (o se desplazan con frecuencia) a las redes de la empresa. Los usuarios con acceso remoto pueden trabajar como si sus equipos estuvieran conectados físicamente a la red.

Los usuarios ejecutan software de acceso remoto e inician una conexión con el servidor de acceso remoto que utilizando el servicio de enrutamiento y acceso remoto, autentica las sesiones de servicios y usuarios hasta que el administrador de redes o el usuario las termine. Todos los servicios que estén habitualmente disponibles para un usuario conectado a una red (incluido el uso compartido de archivos e impresoras, acceso al servidor Web y la mensajería) estarán habilitados por medio de la conexión de acceso remoto.

Los servidores de acceso remoto que ejecutan Windows Server 2003 admiten dos tipos diferentes de conectividad de acceso remoto:

- Acceso telefónico a redes. Es una conexión de acceso telefónico permanente, realizada por un cliente de acceso remoto a un puerto físico de un servidor de acceso remoto mediante el servicio de un proveedor de telecomunicaciones (RTE, RDSI o X25).
- Redes privadas virtuales. La interconexión de redes privadas virtuales, la creación de conexiones seguras punto a punto a través de una red privada o una red pública como Internet. Los clientes de redes privadas virtuales utilizan protocolos especiales basados en TCP/IP (denominados protocolos de túnel) para realizar una llamada virtual a un puerto virtual de un servidor de red privada virtual. En contraste con el acceso telefónico a redes, la red privada virtual siempre es una conexión lógica e indirecta entre el cliente y el servidor de red privada virtual para garantizar la privacidad, se deberán cifrar los datos enviados a través la conexión.

5.10.3.- El Enrutamiento.

El enrutamiento que forma parte de los servicios integrados de enrutamiento y acceso remoto (RRAS) proporciona servicios de enrutamiento de multiprotocolo LAN a LAN, LAN a WAN, red privada virtual (VPN) y traducción de direcciones de red (NAT). Está destinado a administradores del sistema que ya estén familiarizados con protocolos y servicios de enrutamiento y con protocolos enrutables como TCP/IP y AppleTalk.

Cómo configurar el servidor RAS

Para configurar el servidor RAS deberán cumplirse los procesos siguientes:

1. Configurar el hardware (módem, cable de comunicaciones entre dos equipos, RDSI o X25). Esta opción no se desarrollará ya que al tener tantas variantes escapa a las posibilidades de este libro.
2. Configurar los puertos serie.
3. Instalar el módem.
4. Instalar y configurar el servidor RAS.
5. Configurar los clientes RAS.
6. Configurar las cuentas de usuario que lo van a utilizar.

5.11.- El servicio de autenticación de Internet (IAS).

El Servicio de autenticación de Internet (IAS) en Windows Server 2003, es la implementación de Microsoft de un servidor y un proxy del Servicio de usuario de acceso telefónico de autenticación remota (RADIUS).

Como servidor RADIUS, IAS se encarga de manera centralizada de la autenticación, autorización y de las cuentas de conexión de muchos tipos de accesos a red (por ejemplo, acceso inalámbrico, conmutación de autenticación, acceso remoto VPN, acceso telefónico y conexiones de enrutador a enrutador).

Como proxy RADIUS, IAS reenvía los mensajes de autenticación y cuentas a otros servidores RADIUS.

Cuando un servidor IAS forma parte de un dominio del Directorio Activo, utilizará el servicio de directorio como su base de datos de cuentas de usuario y de esa manera el

mismo conjunto de credenciales se utilizará para controlar el acceso a la red a iniciar una sesión en dicho dominio.

Características de IAS

IAS cuenta con las características siguientes:

- Varios métodos de autenticación. Es compatible con varios protocolos de autenticación y permite agregar métodos personalizados que cumplan los requisitos de autenticación. Los métodos de autenticación compatibles son:
- Protocolos de autenticación PPP basados en contraseñas como PAP, CHAP, MS-CHAP Y MS-CHAP v2 (se han descrito en apartados anteriores).
- Varios métodos de autorización. Admite una serie de métodos de autorización y permite agregar métodos personalizados que cumplan los requisitos de autorización. Los métodos de autorización compatibles son:
- Servicio de identificación del número marcado (DNIS) que proporciona al receptor de la llamada el número marcado.
- Servicio de identificación automática del número (ANI) que proporciona el número desde el cual se llama al usuario receptor (se conoce también como Identificador de llamada).
- Autorización de invitado. Permite la utilización de la cuenta Invitado para identificar al usuario cuando la conexión se realiza mediante el nombre de usuario y contraseña.
- Servidores de acceso heterogéneos. Además de admitir servidores de acceso remoto, es compatible con:
- Puntos de acceso inalámbrico. Mediante las directivas de acceso remoto y el tipo de puerto IEEE 802.11, IAS se puede emplear como servidor RADIUS en los puntos de acceso inalámbrico RADIUS para la autenticación y autorización de nodos inalámbricos.
- Conmutadores de autenticación. Si utiliza directivas de acceso remoto y el tipo de puerto Ethernet. IAS se puede emplear como servidor RADIUS en los conmutadores de red Ethernet RADIUS para la autenticación y autorización de nodos de conmutación.
- Proxy RADIUS IAS permite que las solicitudes RADIUS entrantes se reenvíen a

otro servidor RADIUS para el proceso de autenticación y autorización o cuentas.

- Acceso telefónico externo y acceso a la red inalámbrica. El acceso telefónico externo (también conocido como acceso telefónico mayorista) proporciona un contrato entre una organización y un proveedor de servicios Internet (ISP). El ISP permitirá a los empleados de la organización conectarse a su red para establecer un túnel VPN hacia la red privada de la organización. Cuando un empleado de la organización se conecta al NAS del ISP, los registros de autenticación y uso se dirigen al servidor IAS de la organización. El servidor IAS permite a la organización controlar la autenticación de usuarios, hacer un seguimiento del uso y decidir que empleados pueden tener acceso a la red del ISP.
- El acceso inalámbrico también puede ser externo. Un proveedor puede proporcionar acceso inalámbrico en una ubicación remota y utilizar su nombre de usuario para reenviar la solicitud de conexión a un servidor RADIUS que está bajo su control para el proceso de autenticación y autorización.
- Autenticación y autorización de usuarios centralizadas. Para autenticar una solicitud de conexión, IAS validará las credenciales de la conexión con las cuentas de usuario local, cuentas de un dominio de Windows NT Server 4.0 o de un dominio del Directorio Activo (en el caso de un dominio del Directorio Activo, IAS admitirá el uso de UPN y grupos universales).

5.12.- El Protocolo RADIUS.

El Servicio de usuario de acceso telefónico de autenticación remota RADIUS (Remote Authentication Dial-ln User Service) es un protocolo estandar que se describe en los documentos RFC 2865, y RFC 2866. RADIUS se utiliza para proporcionar servicios de autenticación, autorización y administración de cuentas. Un cliente RADIUS (por lo general, un servidor de acceso telefónico, un servidor VPN o punto de acceso inalámbrico) envía credenciales de usuario (nombre de usuario y contraseña) e información de parámetros de conexión en forma de un mensaje RADIUS a un servidor RADIUS. El servidor RADIUS autentica y autoriza la petición cliente RADIUS y devuelve un mensaje de respuesta RADIUS. Los clientes RADIUS también envían mensajes de administración de cuentas RADIUS a los servidores RADIUS.

Además, los estándares RADIUS admiten el uso de proxy RADIUS. Un proxy RADIUS es un equipo que reenvía mensajes RADIUS entre equipos compatibles con RADIUS.

Los mensajes RADIUS se envían como mensajes UDP, se utiliza el puerto UDP 1812 para los mensajes de autenticación RADIUS y el 1813 para los mensajes de administración de cuentas RADIUS. Puede que algunos servidores de acceso a la red utilicen el puerto UDP 1645 para los mensajes de autenticación RADIUS y el 1646 los mensajes de administración de cuentas RADIUS. De manera predeterminada, IAS admite la recepción de mensajes RADIUS destinados a ambos grupos de puertos UDP.

La carga UDP de un paquete RADIUS sólo incluye un mensaje RADIUS.

En los documentos RFC 2865 y 2866 se definen los siguientes tipos de mensajes RADIUS:

- Access-Request (solicitud de acceso). Es enviado por un cliente RADIUS para solicitar autenticación y autorización de un intento de conexión
- Access-Accept (aceptación de acceso). Es enviado por un servidor RADIUS como respuesta a un mensaje Access-Request. En él que se informa al cliente RADIUS de que se ha autenticado y autorizado el intento de conexión.

- Access-Reject (rechazo de acceso). Es enviado por un servidor RADIUS como respuesta a un mensaje Access-Request. En el se informa al cliente RADIUS de que se ha rechazado el intento de conexión. (un servidor RADlUS enviara este mensaje si las credenciales no son autenticas ó no se ha autorizado el intento de conexión).
- Access-Challenge (desafio de acceso). Es enviado por un servidor RADIUS como respuesta a un mensaje Access-Request (este mensaje es un desafío al cliente RADIUS que exige una respuesta).
- Accounting-Request (solicitud de administración de cuentas) enviado por un cliente RADIUS para especificar información de administración de cuentas de una conexión que se ha aceptado.
- Accounting-Response (respuesta de administración de cuentas) enviado por un servidor RADIUS como respuesta a un mensaje de Solicitud de administración de cuentas (en este mensaje se confirman la recepción y el procesamiento correctos del

mensaje de Solicitud de administración de cuentas).

Un mensaje RADIUS está formado por un encabezado RADIUS y cero atributos RADIUS (cada atributo RADIUS especifica una información determinada acerca del intento de conexión).

Cuando IAS se utiliza como servidor RADIUS, proporciona los siguientes apartados:

- Un servicio central de autenticación y autorización para todas las peticiones de acceso enviadas por los clientes RADIUS.
- Para autenticar las credenciales de usuario (nombre de usuario y contraseña) de un intento de conexión, utilizará las cuentas de local, las cuentas de un dominio de Windows NT Server 4.0 o de un dominio del Directorio Activo. Para autorizar la conexión, IAS utilizara las propiedades de marcado de la cuenta de usuario y las directivas de acceso remoto.
- Un servicio central de registros de administración de cuentas para todas las solicitudes de administración de cuentas enviadas por los clientes RADIUS.
- Las solicitudes de administración de cuentas se almacenan en un registro local para su posterior análisis.

Cuando se utiliza IAS como servidor RADIUS, los mensajes RADIUS proporcionan autenticación, autorización y administración de cuentas de las conexiones de acceso a la red de la manera siguiente:

- Los servidores de acceso (como los servidores de acceso telefónico a redes, servidores VPN y puntos de acceso inalámbricos) reciben peticiones de conexión de los clientes de acceso.
- El servidor de acceso (configurado para utilizar RADIUS como protocolo de autenticación, autorización y administración de cuentas) crea un mensaje de petición de acceso y lo envía al servidor IAS.
- El servidor IAS evalúa el mensaje de petición de acceso.
- Si es necesario, el servidor IAS envía un mensaje de desafío de acceso al servidor de acceso. El servidor de acceso procesa el desafío y envía una petición de acceso actualizada al servidor IAS.
- Se comprueban las credenciales de usuario y se obtienen las propiedades de acceso telefónico de la cuenta de usuario mediante una conexión segura a un controlador

de dominio.

- El intento de conexión se autoriza con las propiedades de acceso telefónico de la cuenta de usuario y las directivas de acceso remoto.
- Si se autentica y autoriza el intento de conexión, el servidor IAS enviará un mensaje de aceptación de acceso al servidor de acceso.
- Si no se autentica ni se autoriza el intento de conexión, el servidor IAS enviará un mensaje de rechazo de acceso al servidor de acceso.
- El servidor de acceso completa el proceso de conexión con el cliente de acceso y envía un mensaje de solicitud de administración de cuentas al servidor IAS, en el cual se registra el mensaje.
- El servidor IAS envía una respuesta de administración de cuentas al servidor de acceso.

El servidor de acceso también envía mensajes de solicitud de administración de cuentas en los siguientes casos:

- Durante el tiempo en que se establece la conexión.
- Cuando se cierra la conexión del cliente de acceso.
- Cuando se inicia y se detiene el servidor de acceso.

Se puede utilizar IAS como servidor RADIUS en los casos siguientes:

- Cuando se utilice un dominio de Windows NT Server 4.0, un dominio Directorio Activo o las cuentas de seguridad local como base de las cuentas de usuario de los clientes de acceso.
- Cuando se utilice el servicio Enrutamiento y acceso remoto de Windows Server 2003, Standard Edition, Enterprise Edition o Datacenter Editi, Windows 2000 en varios servidores de acceso telefónico, servidores o enrutadores de marcado a petición y se desea centralizar configuración de las directivas de acceso remoto y el registro de conexiones para la administración de cuentas.
- Cuando se subcontrate el acceso telefónico, VPN o inalámbrico a proveedor de servicios de Internet. Los servidores de acceso utilizan RADIUS para autenticar y autorizar las conexiones que realizan miembros de la organización.
- Cuando se desee centralizar la autenticación, la autorización y administración de cuentas en un grupo.

Conclusiones:

Una red intranet es un conjunto de ordenadores privados que utiliza la tecnología de Internet para compartir dentro de una organización parte de sus sistemas de información y sistemas operativos. Las redes internas corporativas son potentes herramientas que permiten divulgar información de la compañía a los empleados con efectividad, consiguiendo que estos estén permanentemente informados con las últimas novedades y datos de la organización. También es habitual su uso en centros de información y en universidades, ya que facilita la consulta de diferentes tipos de información.

También tiene un gran valor como reposición de documentos, convirtiéndose en un factor determinante para conseguir el objetivo de la oficina sin papeles, añadiéndoles funcionalidad como un buen buscador y organización adecuada. Se puede conseguir una consulta rápida y eficaz por parte de los empleados de un volumen importante de documentación. Los beneficios del uso de una red intranet pueden ser enormes. La cantidad de información está al alcance de los empleados de una empresa u organismo ahorrando tiempo en búsqueda.

Una red intranet cumple con tener una accesibilidad web permitiendo su uso a la mayor parte de las personas, gracias a esto, promueve nuevas formas de colaboración y acceso a los sistemas. Ya no es necesario reunir a todos en una sala para discutir un proyecto. Una red Intranet ayuda a que un equipo de personas alrededor del mundo puedan trabajar juntos sin tener que invertir en gastos de transportación y viajes. El resultado de esto es un aumento increíble en la eficiencia acompañada de una reducción de costos.

La red intranet lleva consigo distintos tipos de seguridad según el usuario. Estos niveles son asignados según la relevancia del puesto dentro de la organización, claro que existen niveles compartidos por todos. Ahora los niveles básicos de seguridad impiden la utilización de la red intranet por parte de personas ajenas a la empresa. Por lo que la vuelve mucha más segura.

Los grandes beneficios de una red intranet los podemos enumerar de la siguiente forma:

a) Capacidad de compartir recursos (escáner, impresoras, etc.) y posibilidad de conexión a Internet.

b) Alojamientos de páginas web, tanto de un servidor como de usuarios, que pueden consultarse con los navegadores desde todos los ordenadores del mismo o desde cualquier ordenador externo que esté conectado a internet.

c) Servicios de almacenamiento de información. Espacios de discos virtuales a los que se puede acceder para guardar y recuperar información desde los ordenadores del centro y también desde cualquier equipo externo conectado a Internet.

La evolución de la intranet ha sido vertiginosa, pasando de ser un canal de comunicación unilateral (transmitiendo información exclusiva de empresa a usuario) a un medio de comunicación bi-direccional, donde la interacción entre los empleados aporta mucho a objetivos como la innovación, la mejora permanente y la gestión del conocimiento.

Hoy la intranet empieza a incorporar modelos de comunicación web y redes sociales. Ellos son los verdaderos motores de esta nueva intranet empresarial.

Bibliografía

1.- Programa de la Academia de Networking de Cisco
CCNA 1: Copyright 2003, Cisco Systems, INc.

2.- Andrew S. Tanenbaum
Redes de Computadoras
Cuarta Edición
Perarson Prentice – Hall
México, 2003.

3.- William Stallings
Comunicaciones y Redes de Computadoras
7ª. Edición
Perarson Prentice – Hall
México, 2004.

4.- Microsoft Corporation. (1993-1998). **Redes de Comunicación,** Enciclopedia Microsoft Encarta 99.

5.- Stephen Grossberg. **"Teoría de Resonancia Adaptada".**
http://inf.udec.cl/~yfarran/web-redes/ind-redes.htm
6.- http://es.wikipedia.org/wiki/Topolog%C3%ADa_de_red.
7.- http://es.wikipedia.org/wiki/Red_en_%C3%
8.- www.iso.org/.
9.- www.ieee.org/.
10.- www.ansi.org/.
11.- www.eia.org/.
12.- www.fcc.gov/.
13.- http://www.cft.gob.mx/.

Memoria Técnica Proyecto Las Delicias 2001. Memoria Técnica Proyecto Salamanca II 230 y 400 KV. 2002/2004 Memoria Técnica Proyecto LT QRP – LDE 2002 Memoria Técnica Proyecto Modernización Conin 2003 Memoria Técnica Proyecto Santa Fe 2004 Memoria Técnica Proyecto San Juan Potencia 2005 Memoria Técnica Proyecto México – Guadalajara 2005 Introduction to Synchronous Sistems, Alcatel Bell, Código Docto. 14035, 1993,

Edición 1

Curso de Capacitación Universidad Alcatel – Lucent; **Fundamentos de Fibra Óptica.**

Trabajo de Ejercicio Profesional **Reestructuración y Optimización de la Red de Fibra Óptica;** Ing. Andrés Gómez Anguiano

http://www.itu.int
http://es.wikipedia.org/
http://www.cisco.com
http://www.abb.com.mx
http://www.alcatel-lucent.com/
http://www.siemens.com
http://www.google.com.mx/