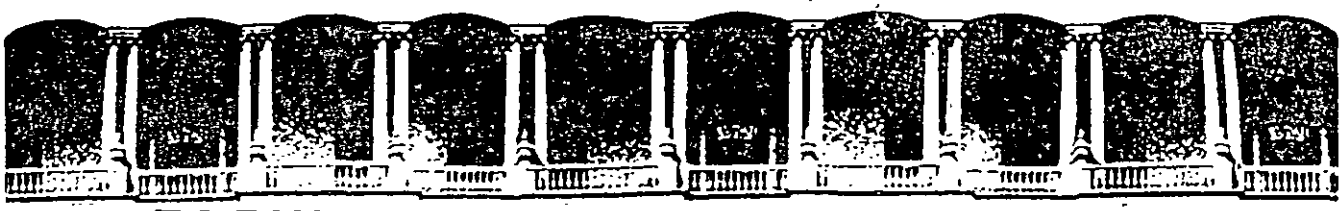


FACULTAD DE INGENIERIA U.N.A.M.
DIVISION DE EDUCACION CONTINUA

DIPLOMADO DE REDES (LAN) DE MICROCOMPUTADORAS

MODULO IV OPTATIVO

INTERNET/ SERVICIOS E IMPLEMENTACION DE SERVIDORES

MATERIAL DIDACTICO

OCTUBRE - NOVIEMBRE

Palacio de Minería Calle de Tacuba 5 Primer piso Deleg. Cuauhtémoc 06000 México, D.F. Tel. 521-40-20 Apdo. Postal M-2285

TEMARIO: INTERNET/ INTRANET
SERVICIOS E IMPLEMENTACION DE SERVIDORES

- INTRODUCCION
- QUE ES INTERNET
- DESARROLLO DE INTERNET
- ESTADISTICAS
- TIPOS DE ENLACES
- ARQUITECTURA CLIENTE-SERVIDOR

- PRINCIPALES SERVICIOS PROPORCIONADOS POR INTERNET
- **Servicios**
  - CORREO ELECTRONICO (e-mail)
  - CONEXION REMOTA (telnet)
  - NOTICIAS (usenet)
  - TRANSFERENCIA DE ARCHIVOS (ftp anónimo)
  - CONVERSACIONES (talk & y talk)
  - CONFERENCIAS (internet relay chat 'IRC')
  - MENUES DE ACCESO (gopher)
  - REVISTAS ELECTRONICAS
  - LISTAS DE CORREO
  - INTERNET BBS
- **Herramientas**
  - BUSQUEDA DE PERSONAS (finger)
  - BUSQUEDA DE ARCHIVOS (archie)
  - BUSQUEDA DE INFORMACION (WAIS)
  - BUSQUEDA DE DIRECCIONES (white pages)
  - BUSQUEDA DE RECURSOS (veronica & jughead)
- **Otros**
  - ACCESO INTEGRAL A INTERNET (WWW)
  - REALIDAD VIRTUAL (MUD)

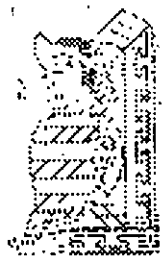
- TCP/IP
- **Conceptos de TCP/IP**
  - DIRECCIONES IP
  - SUBNET
  - SERVICIOS DE DHCP
  - NOMENCLATURA DE DOMINIOS

- CREACION DE SERVIDORES

- **Conceptos y configuraciones de servidores**
  - NDS
  - DHCP
  - WWW
  - FTP
  - TELNET
  - GOPHER
  - FIREWALL
- IMPLEMENTACION DE SERVIDORES BAJO:
- SCO UNIX
- WINDOWS NT
- NOVELL
- LINUX

INTERNET/INTRANET
SERVICIOS E IMPLEMENTACION DE SERVICIOS

INTRODUCCION



OCTUBRE 1997

A finales de los 70´s ARPANET se estaba acercando a su máximo soporte con 256 máquinas conectadas. El protocolo NCP no podía soportar el tráfico de la red, y era tangible que se necesitaba un sucesor de este protocolo.

En 1982, se logró concebir e implementar el diseño final de un nuevo protocolo, denominado IP (Internet Protocol). IP fué uno de los cuatro protocolos que fueron desarrollados, pero todos trabajaban sobre éste. Los otros protocolos fueron User Datagram Protocol (UDP), Transmission Control Protocol (TCP) e Internet Control Message Protocol (ICMP).

En 1985, la National Science Foundation (NSF) propuso extender la red para dar acceso fácil a investigadores y científicos, situando 5 supercomputadoras más a lo largo de Estados Unidos.

Una vez puesto en marcha este proyecto, la cantidad de conexiones excedía la capacidad de la red, aún con el nuevo protocolo IP. En 1987, NSF anunció una sociedad estratégica para solucionar los problemas de la red, anunciando a MERIT Inc., una compañia operadora de redes, a IBM, un gigante de la manufactura de las computadoras y a MCI, la compañia estadounidense de telefonía. Esta sociedad dió sus frutos en el verano de 1988, con la instalación de NSFNET.

Finalmente, en 1990 el ARPANET original se unió a NSFNET, además de otras pequeñas redes que se habían formado, dando como resultado de la unión de este laberinto de redes ahora conocido **INTERNET**.

No obstante el considerar a **INTERNET** como una RED de computadoras o un grupo de redes de computadoras interconectadas entre si es sólo tomar en cuenta el aspecto físico, porque **INTERNET** en sí, es el mundo de información al que tenemos acceso alrededor del mundo.

Para la mayoría de las personas lo más importante de **INTERNET** son las personas que en ella participan, que a través de ella se conocen, trabajan y se comunican, para algunas es tan importante o más que el mismo teléfono o el correo postal. **INTERNET** es el primer foro general y la primera biblioteca general, cualquiera puede participar a cualquier hora, no importa que religión se practique o que tipo de ropas utilicemos, siempre podremos participar en **INTERNET**.

Quizá lo más sorprendente de **INTERNET** es que no tiene líderes, nadie la gobierna, no existe una única organización que pague el costo. Más adelante comentaremos la forma en que la **INTERNET** está organizada y de algunos de los organismos que se dan a la tarea de tratar de organizar un poco las cosas, pero de momento no hay quién se encargue directamente de su estructura.

DEFINICIONES

Para comprender mejor algunos de los fenómenos que se suceden dentro de **INTERNET**, comenzaremos con establecer algunos conceptos comunes que se manejan dentro de **INTERNET.**

RED

El término RED significa dos o más computadoras conectadas entre sí. Hay un gran número de razones para unir las computadoras en redes, pero las dos importantes desde el punto de vista **INTERNET** son:

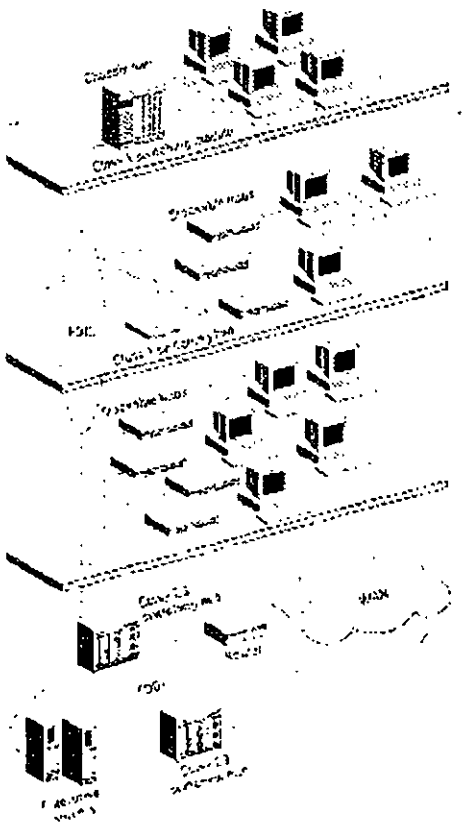
- Permité la comunicación entre las personas
- Compartir recursos

Una vez que estamos dentro de **INTERNET**, podemos enviar mensajes a otras personas que usan otras redes conectadas a **INTERNET**.

En cuanto a compartir, los administradores de sistemas conectan a las redes esos recursos que son caros o difíciles de mantener, haciéndolos disponibles para cualquier usuario de la red. Por ejemplo, un administrador puede conectar a la red una impresora muy costosa de forma que cualquiera que necesite imprimir pueda hacer uso de ella. En **INTERNET** se comparten recursos de información más que dispositivos hardware, esto significa que el tipo de recursos que podemos compartir a través de **INTERNET** son recursos lógicos. Por ejemplo en un catálogo de recursos podemos observar algunos temas que están desarrollados dentro de **INTERNET** alrededor del mundo.

Una red de área local (LAN), es una red en la que, las computadoras se conectan directamente a través de un medio de comunicación físico, normalmente con algún tipo de cable. Cuando conectamos unas LAN con otras, formamos lo que llamamos una red de área extendida o WAN. La mayoría de las redes de área extendida se interconectan utilizando líneas telefónicas que pueden ser dedicadas o conmutadas, aunque hay muchas otras tecnologías, como los enlaces por satélite, que también se usan.

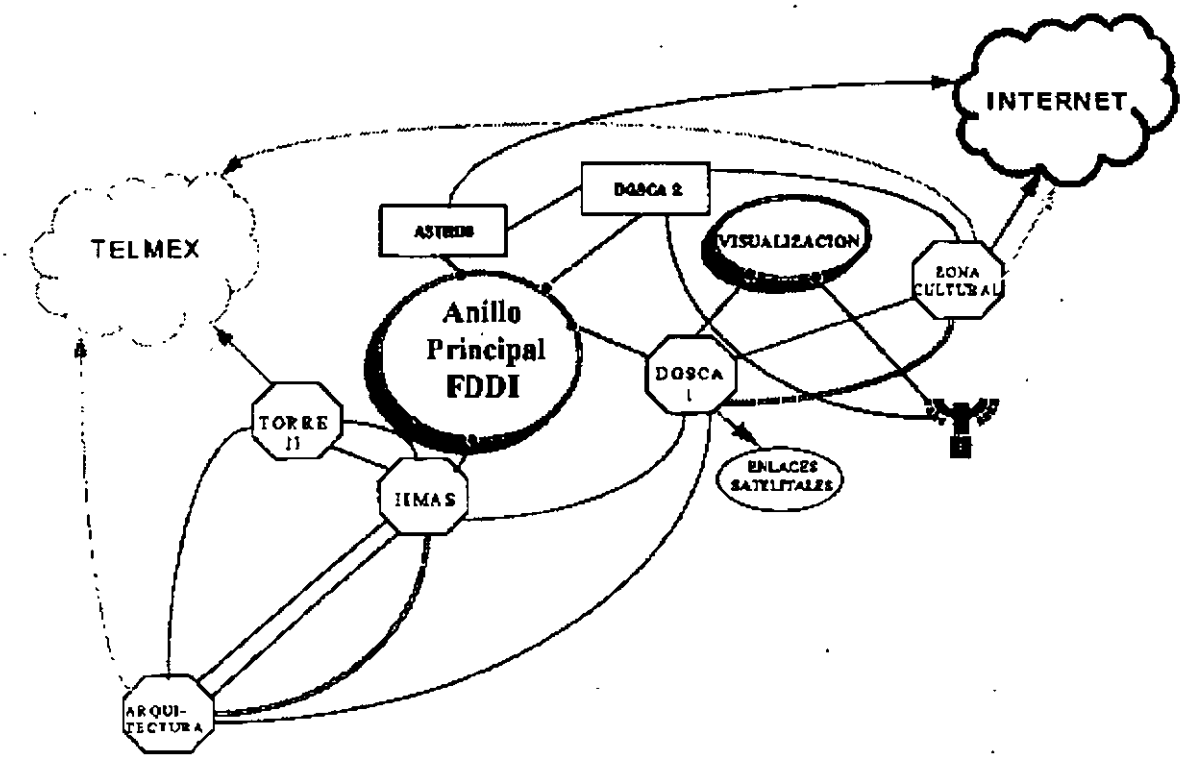
La mayoría de las conexiones de área extendida de **INTERNET** funcionan sobre algún sistema telefónico. En realidad, los cuellos de botella que se producen a veces en **INTERNET** son debidos normalmente a la falta de fiabilidad del sistema telefónico.



Veamos un ejemplo típico de red. Imagine que está sentado en una sala repleta de computadoras de la facultad de Ciencias Sociales de una universidad, su computadora está conectada a todas las computadoras de la sala y a todas las computadoras del edificio. Ahora bien hay otras LAN en el campus. Por ejemplo, la facultad de Psicología tiene su propia red de computadoras, lo mismo la facultad de Matemáticas, la facultad de Informática y el resto. Cada una de estas LAN están interconectadas entre si a través de un enlace de alta velocidad, para formar una WAN dentro del campus. Aunque hemos tomado como ejemplo una universidad, muchas otras organizaciones utilizan una estructura similar: empresas, gobiernos, centros de investigación, etc. Si la organización es pequeña, puede tener sólo una LAN. Las grandes organizaciones pueden constar de varias LAN, unidas entre si formando una o varias WAN. Estas organizaciones disponen de personal técnico para cuidar del buen funcionamiento de la red.

8

Para interconectar las LAN se utilizan dispositivos denominados ruteadores, cuya función principal es proporcionar un enlace de una red a otra. Utilizamos ruteadores para unir LAN's y formar WAN, o para unir WAN's para formar WAN's mayores. En otras palabras, se puede decir que las computadoras en **INTERNET** se conectan en LAN's y WAN's mediante un gran número de ruteadores.



Ahora bien, la mayoría de las redes que conforman a **INTERNET** están basadas en plataformas UNIX y algunos de estos sistemas son propiamente multiusuario. No obstante, existen algunos otros conceptos que debemos revisar.

HOSTS Y TERMINALES

Dentro de **INTERNET** cada computadora por sí sola se denomina host, independientemente de que pueda o no compartir recursos, es decir que la computadora desde la cual accesamos a **INTERNET** es un host, independientemente de que pueda no pueda poner a disposición de **INTERNET** algún recurso.

Otra de las acepciones que reciben las computadoras dentro de la RED es la de nodo, ya que si se dibuja un diagrama de puntos y líneas para representar las conexiones a una red, cada computadora estará representada por un punto y cada una de las líneas serán las conexiones. La parte de las matemáticas que trata este tipo de diagramas, denomina a cada uno de estos puntos un "nodo". Los especialistas en redes se han apropiado este término para hacer referencia a cualquier computadora conectada a una red. Por eso, "nodo" es un sinónimo más técnico de "host".

La palabra host dentro de los sistemas multiusuario tiene un significado ligeramente diferente, es el nombre que se le da al equipo central del sistema, al cual se le conectan computadoras de capacidades físicas generalmente menores, y que reciben el nombre de terminales.

Una computadora central muy potente puede actuar como host para cientos de usuarios al mismo tiempo. De igual modo una minicomputadora actuará como host para un grupo reducido de usuarios. El sistema operativo UNIX es un sistema multiusuario. Aunque podemos utilizar computadoras Unix como estaciones de trabajo, la mayoría de la computadoras Unix trabajan como host para soportar múltiples usuarios.

En un sistema multiusuario, cada usuario accesa al equipo central a través de su propia terminal, la cual consta de un teclado, una pantalla y quizá de un ratón. Todas las terminales están conectadas al host, que suministra su potencia de cálculo a todo el mundo.

En consecuencia, hay dos acepciones para "host". En **INTERNET**, cada computadora es un host. En un sistema multiusuario, la computadora principal que soporta a cada usuario conectado a través de una terminal, también se llama host. Desde luego, si una de estas computadoras se conecta a **INTERNET**, sería un host multiusuario y un host de **INTERNET**, y cada usuario desde su terminal puede también tener acceso a **INTERNET**.

SISTEMAS CLIENTE/SERVIDOR

Como sabemos, una de las principales funciones de una red es la posibilidad de compartir recursos. De una forma muy simple, la mayoría de las veces esta compartición de recursos se lleva a cabo por dos programas distintos ejecutándose en computadoras diferentes. Uno de los programas llamado servidor, proporciona un recurso en particular, mientras que el otro programa llamado cliente, utiliza ese recurso y se ejecuta en otra computadora.

En redes de área local, es muy común utilizar la palabra "servidor" para referirse a la propia computadora que ejecuta el programa servidor. En **INTERNET**, normalmente los términos "cliente" y "servidor" hacen referencia a los programas que solicitan y proporcionan los servicios.

Veamos un ejemplo muy común. Muchos nodos de **INTERNET** proporcionan un servicio llamado *"gopher"*, el cual permite seleccionar opciones de una serie de menús. Cada vez que se selecciona una opción, *gopher* ejecuta la tarea indicada. Por ejemplo, si la opción del menú describe una determinada información (como 'Noticias del Día'), *gopher* recupera esta información y la mostrará en pantalla.

Cuando se utiliza *gopher*, dos programas interactúan entre si, primero, hay un programa que proporciona una interfaz de usuario, es decir que interpreta las instrucciones que se dan a través de las teclas que se pulsan, muestra los menús y generalmente asegura que las peticiones se lleven al cabo. Este programa se denomina cliente *gopher*. El otro programa es el que suministra cualquier cosa que el cliente *gopher* solicita. Este programa se denomina servidor *gopher*.

Lo importante de este esquema es que los programas cliente y servidor se ejecutan en computadoras diferentes. Por ejemplo, podría estar sentado en su PC en México utilizando *gopher* para leer las 'Noticias de Día" de la Agencia de Seguridad Nacional de Virginia, en Estados Unidos. En este caso, el cliente *gopher* se ejecuta en su PC, mientras que el servidor *gopher* es un programa que se ejecuta en una supercomputadora de otro país.

Todos los servicios de **INTERNET** hacen uso de esta relación cliente/servidor. **Aprender a "navegar" por INTERNET, significa aprender a usar cada uno de los programas clientes disponibles.**

Por esta razón para utilizar un servicio INTERNET, hay que entender

- Cómo ejecutar un programa cliente para este servicio
- Cómo decirle al programa cliente qué servidor se quiere utilizar
- Qué instrucciones se pueden utilizar con cada tipo de cliente

Lo que el usuario tiene que hacer es ejecutar el programa cliente y decirle lo que tiene que hacer. El trabajo del programa cliente es conectar el servidor adecuado y asegurarse de que sus instrucciones sean enviadas correctamente.

Cada tipo de cliente de **INTERNET** tiene sus propias instrucciones y reglas. Por ejemplo, las instrucciones que pueden utilizar con un cliente *gopher* son diferentes de las que se puede usar con un cliente *archie* (otro servicio de **INTERNET**). La ventaja de los programas clientes de **INTERNET** es que tienen sus propias facilidades de ayuda interactiva.

X-WINDOW Y CLIENTES X

Existe un tipo especial de sistema cliente/servidor llamado X-Window, el cual ofrece ciertas ventajas cuando se utiliza **INTERNET**.

El sistema X-Window se utiliza con el sistema Unix y permite soportar interfaces gráficas para el usuario. Una interfaz gráfica de usuario (GUI Grafical User Interface), permite manejar una computadora utilizando además del teclado, un ratón u otro tipo de dispositivo apuntador. Con la ayuda de un ratón, se pueden seleccionar opciones de un menú y manejar objetos en pantalla. Se puede ejecutar más de un programa al mismo tiempo, cada uno de los cuales se ejecutan en su propia área rectangular llamada ventana.

El sistema X-Window fué desarrollado para proporcionar una herramienta estándar para los programadores que desarrollan aplicaciones gráficas y una interfaz estándar a los usuarios para que interactúen con esas aplicaciones.

En la terminología X-Window los tres dispositivos con los que nos comunicamos con la computadora (el teclado, la pantalla y el ratón) se denominan comúnmente display. X-Window nos permite ejecutar más de un programa al mismo tiempo en la misma pantalla. Como parte de la interfaz gráfica de usuario, para cambiarnos de un programa a otro basta utilizar el ratón y desplazarnos de una ventana a otra:

Cuando se utiliza X-Window, la interfaz gráfica de usuario (GUI) para todos los programas que se están ejecutando, son manejados por un programa llamado "display server" o "X server".

Por ejemplo, supongamos que tenemos cuatro programas ejecutándose al mismo tiempo, cada uno dentro de su propia ventana. Mientras trabajamos, podemos mover las ventanas de lugar o cambiar su tamaño. Ahora, supongamos que uno de los programas necesita dibujar un círculo en la pantalla. En lugar de que hacer el trabajo el mismo programa, éste envía un mensaje al servidor X del programa que está controlando la pantalla diciéndole que dibuje un círculo de un determinado tamaño en el lugar especificado. El servidor X ejecuta esa acción.

Esta forma de trabajar tiene muchas ventajas. La primera, significa que todo el entorno gráfico está controlado por un solo programa que garantiza que cada cosa funciona de forma correcta. Por ejemplo, la ventana en la que se está ejecutando un programa puede ser tapada parcialmente por otra ventana. El programa que se ejecuta dentro de la ventana no necesita saber esto, no es su tarea. El servidor X se ocupará de todos estos detalles.

Segundo, cuando un programador diseña una nueva aplicación, no tiene que preocuparse de la interfaz de usuario. Todo lo que se necesita es que el programa llame a las rutinas del servidor X cuando lo necesite. Esto permite hacer programas más pequeños, fiables y que son portables de un sistema X a otro.

Puesto que todos los servidores X proporcionan las mismas funciones, un programa que está escrito utilizando estas funciones, podrá ejecutarse en cualquier sistema X. Por ejemplo, puede encontrar programas X en cualquier lugar de **INTERNET**, copiarlos a su computadora, y ejecutarlos bajo su interfaz gráfica de usuario. Una vez que aprendamos a utilizar los servicios de transferencia de archivos de **INTERNET**, podremos encontrar muchos de estos programas gráficos de forma gratuita.

La parte del sistema X que proporciona el aspecto de interfaz se llama administrador de ventanas. (Técnicamente el administrador de ventanas es un programa que se ejecuta sobre X). Hay dos administradores de ventanas muy utilizados, llamados Motif y Open Look, sin embargo, los conceptos básicos son los mismos sin importar qué administrador de ventanas se utilice. Desde luego, los programas dentro de las ventanas no cambiarán. Básicamente, si se sabe utilizar un administrador de ventanas, se sabrá utilizarlos todos.

Dada la relación cliente/servidor los programas que se ejecutan son clientes y por lo tanto se les denominan Clientes X. Estos clientes X hacen peticiones de servicios al servidor X que se ejecuta en la computadora. En otras palabras, el término "cliente X" es un sinónimo para cualquier programa que se ejecuta bajo un sistema X-Window.

PRINCIPALES SERVICIOS PROPORCIONADOS POR INTERNET

CORREO ELECTRONICO (*e-mail*)

Un usuario de **INTERNET**, puede enviar y recibir mensajes de cualquier otro usuario de **INTERNET**. Más aún, puede enviar mensajes a otros sistemas de correo, como pueden ser CompuServe o MCI Mail, que tienen conexiones con **INTERNET**.

Sin embargo, correo electrónico no significa solamente mensajes personales. Cualquier cosa que se pueda almacenar en un archivo de texto puede ser enviado por correo electrónico: programas (fuente) de computadora, anuncios, revistas electrónicas, etc.

Cuando se necesite enviar un archivo binario que no se puede representar como texto habitual, como programas de computadora compilados o imágenes gráficas, existen facilidades para codificar los datos en texto. De igual forma, una vez que se reciben mensajes codificados, es posible decodificarlos para guardarlos con su formato original.

Por eso, desde un punto de vista práctico, se puede enviar por correo electrónico cualquier tipo de archivo a cualquier persona. El sistema de correo electrónico de **INTERNET** es la columna vertebral de la red.

CONEXION REMOTA (*telnet*)

Se puede hacer ***telnet*** a cualquier computadora remota de **INTERNET**. Una vez que se ha establecido la conexión, se puede utilizar esa computadora en la forma habitual (si se posee una cuenta válida). Puesto que la mayoría de las computadoras de **INTERNET** utilizan Unix, utilizaremos la misma terminología que Unix.

El nombre de una cuenta de usuario se denomina identificador de usuario (user-id). La palabra secreta que se debe introducir, para comprobar que la cuenta es la suya, se denomina password. Si se posee un identificador de usuario y una palabra clave válidos, se puede conectar con cualquier computadora de **INTERNET.**

Como un servicio público, muchos servicios de **INTERNET** permiten a cualquier usuario conectarse utilizando la cuenta especial *guest.* Por ejemplo, en los Estados Unidos, existe un sistema que proporciona información meteorológica de todo el país. Cualquier persona puede conectar con este sistema y comprobar cuál será el tiempo para el fin de semana.

BUSQUEDA DE PERSONAS (*finger*)

La mayoría de a computadoras de **INTERNET** tienen una utilería que permite buscar información sobre un usuario en particular. Este servicio es conocido con el descriptivo nombre de ***finger***. En **INTERNET** los usuarios se conocen por su identificador de usuario, se puede utilizar *finger* para encontrar el nombre de un usuario si se conoce su identificador de usuario. Por ejemplo, se puede comprobar que el identificador de usuario "harley" pertenece a Harley Hahn.

Dependiendo de como esté instalado el servicio *finger* en la computadora que utilice, puede encontrar más información sobre la persona que busca, como por ejemplo número de teléfono, dirección de la oficina, y algunas cosas más. Además, algunos servicios *finger* informarán de cuándo fue la última vez que esa persona utilizó la computadora y si tiene correo electrónico sin leer. Esto puede ser muy útil cuando se necesita comprobar si alguien ha recibido un mensaje importante que se le ha enviado.

Hay también formas de configurar parte de la información que otros usuarios ven cuando hacen un *finger* a su identificador de usuario. Se puede incluir la información que se quiera mostrar. Por ejemplo, un profesor puede indicar sus horas de oficina. Alguien que ofrezca una fiesta, puede dar la dirección de su casa. Se puede conocer esta información, sin más que hacer un *finger* a ese identificador de usuario.

También se puede hacer un *finger* a una máquina, en lugar de a un identificador de usuario. En este caso, la computadora responderá mostrando un resumen de todos los usuarios conectados en ese momento.

Por último, algunos sistemas utilizan el servicio *finger* para suministrar alguna información específica. Por ejemplo, en la Universidad de Washington en Seattle hay un usuario al que podrá hacer un *finger* para conocer información de los últimos terremotos.

NOTICIAS (*usenet*)

usenet contracción de "User's Network" (red de usuarios) es uno de los principales servicios de **INTERNET**. *usenet* no es una RED. Es un sistema de grupos de discusión en el que artículos individuales se distribuyen por todo el mundo, y actualmente tiene miles de grupos de discusión.

En cada nodo de **INTERNET**, el administrador de la red decide qué grupos de **INTERNET** quiere hacer públicos y qué grupos quiere recibir. Por esta razón, *usenet* no está disponible en todas partes.

TRANSFERENCIA DE ARCHIVOS (*ftp anónimo*)

FTP (File Transfer Protocol, Protocolo de Transferencia de Archivos) permite transferir archivos desde una computadora a otra, la mayoría de las veces es desde un host remoto a nuestra computadora, pero también se puede hacer en forma inversa.

El servicio ***ftp anónimo*** es un servicio público por el cual una organización pone a disposición de todo el mundo una serie de archivos. Podemos accesar a estas computadoras utilizando el identificador de usuario *anonymous*, este identificador de usuario no necesita palabra clave.

El *ftp anónimo* es el servicio más importante de **INTERNET**. Virtualmente cada tipo posible de información está almacenada en algún sitio y está disponible de forma gratuita. Por ejemplo, muchos de los programas utilizados en **INTERNET** son creados y mantenidos por personas o grupos que los distribuyen al mundo entero vía *ftp anónimo*. También se pueden encontrar revistas electrónicas, archivos de grupos de discusión de *usenet*, documentación técnica y muchas cosas más.

BUSQUEDA DE ARCHIVOS (*archie*)

Hay miles de servidores de *ftp anónimo* alrededor del mundo ofreciendo una cantidad inmensa de archivos. El papel de los servidores ***archie*** es ayudar a localizar donde se encuentra la información que se necesita.

Supongamos que se quiere un determinado archivo, por ejemplo, un programa sobre el que se ha oído hablar. Se puede utilizar un servidor *archie* para que nos indique los servidores de *ftp anónimo* que almacenan ese archivo.

Una vez que se conoce el nombre de estos servidores, se puede utilizar el servicio *ftp* para cargar el archivo.

Si se consideran los servidores de *ftp anónimo* de todo el mundo como una enorme biblioteca mundial, que está cambiando continuamente, se pueden considerar a los servidores *archie* como su catálogo. Realmente, sin los servidores *archie*, la mayoría de los recursos existentes en los servidores *ftp anónimo* serían inaccesibles.

CONVERSACIONES (*talk* & *ytalk*)

La utilidad ***talk*** establece una conexión entre dos computadoras específicas. Una vez establecida la conexión se pueden intercambiar mensajes de forma interactiva, pero la gran virtud de la utilidad *talk* de **INTERNET** es que es posible sostener una conversación con alguien sin importar la distancia que exista entre ellos. La otra persona ve en su pantalla lo que usted escribe, y ambos pueden teclear al mismo tiempo sin que los mensajes se mezclen.

Mientras que la utilidad ***ytalk*** permite además, la conversación entre más de dos computadoras al mismo tiempo, y lo que se despliega en la pantalla son las líneas que los demás escriben, permitiendo además escribir al mismo tiempo.

INTERNET RELAY CHAT (IRC)

La utilidad **INTERNET Relay Chat (IRC)** es análoga a la utilidad *talk* pero pueden utilizarla más de dos personas a la vez, se puede tomar parte en conversaciones públicas con un gran número de personas. Estas conversaciones se organizan sobre distintos temas o ideas, se puede utilizar IRC para organizar una conversación privada con las personas que se hayan elegido, de igual forma que una multiconferencia telefónica.

GOPHER

gopher proporciona una serie de menús desde los cuales se puede accesar virtualmente a cualquier tipo de información textual, incluyendo la que proporcionan otros recursos de **INTERNET**. Hay muchos sistemas *gopher* en torno a **INTERNET**, cada uno administrado localmente.

Cada *gopher* contiene cualquier información que las personas que administran el *gopher* local han decidido compartir.

Mientras algunos servidores *gopher* son sistemas aislados, la mayoría de los servidores *gopher* están instalados de forma que pueden conectar con otros servidores *gopher*. Por ejemplo, supongamos que se utiliza un *gopher* en California. Seleccionando una opción de un menú, se puede conectar con otro *gopher* en Africa o en Sudamérica.

Lo que hace al sistema *gopher* tan potente, es que no importa el *gopher* que se esté utilizando ni la información que se utilice, la interfaz de usuario es siempre el mismo sistema de menús.

VERONICA Y *JUGHEAD*

Nadie conoce realmente cuántos sistemas *gopher* hay en el mundo. Basta decir que hay muchos, ofreciendo cada uno de ellos su propia serie de opciones de menús que ponen a nuestra disposición información y servicios.

veronica es una herramienta que permite mantener la pista de muchos menús de *gopher* alrededor del mundo. Se puede utilizar *veronica* para realizar una búsqueda y localizar todas las opciones de menú que contienen ciertas palabras clave (cualquiera que se especifique). ***jughead*** hace lo mismo para un grupo específico de menús de *gopher*.

El resultado de una búsqueda con *veronica* o *jughead* es un menú, el cual contiene todos los elementos resultado de la búsqueda, si seleccionamos algún elemento de este menú, de manera automática nos conectamos con el *gopher* apropiado, dondequiera que esté. De hecho, a menos que se especifique lo contrario, no se sabrá qué computadora se está utilizando ni de que país.

SERVIDORES *WAIS*

Los servidores ***wais*** proporcionan otro método de búsqueda de información que se encuentra dispersa por **INTERNET**. *wais* puede accesar a un gran número de bases de datos, para lo cual es necesario indicarle a *wais* en qué base de datos se quiere hacer la búsqueda, después *wais* buscará cada palabra en cada artículo en todas las bases de datos que se le indiquen.

El resultado de una búsqueda *wais* es una lista de artículos seleccionados de las distintas bases de datos, *wais* presenta entonces un menú desde el cual es posible pedirle a *wais* que muestre cualquiera de los artículos elegidos.

El nombre *wais* proviene de "Wide Area Information Service" (Servicio de Información de Area Extensa).

WORD WIDE WEB

El servicio **World Wide Web** a menudo llamado **Web** o ***www*** es una herramienta basada en hipertexto que permite recuperar y mostrar información basada en búsquedas por palabras clave. Lo que hace al servicio World Wide Web tan potente es la idea de hipertexto: datos que contienen enlaces a otros datos incluyendo imágenes y sonido.

Por ejemplo, cuando se esté leyendo alguna información, aparecerán ciertas palabras y frases marcadas de una forma especial. Se le puede decir a Web que seleccione una de estas palabras, quién siguiendo el enlace, encontrará la información relevante y la mostrará. De esta forma, se puede saltar de un sitio a otro, siguiendo los enlaces lógicos en los datos.

DIRECTORIO DE PAGINAS BLANCAS

Dentro del abrumador mundo de **INTERNET**, nada es más importante que la dirección electrónica de una persona. Una vez que se conoce su dirección, es posible enviarle correo, mantener una conversación con *talk* o utilizar *finger* para obtener más información sobre esa persona. Los **Directorios de Páginas Blancas** nos permiten encontrar las direcciones electrónicas de alguien. Sin embargo, no hay un directorio único de **INTERNET**. Más bien, hay una serie de Directorios de Páginas Blancas de propósito especial en los que se puede buscar información sobre personas en **INTERNET**.

REVISTAS ELECTRONICAS

En **INTERNET** existe una gran cantidad de revistas que se publican electrónicamente. Esto es, los artículos se almacenan en archivos de texto que son accesibles para todo el mundo, Algunas de estas revistas electrónicas son periódicos sobre investigación de interés principalmente para especialistas en determinadas materias, algunas otras son de interés general.

Hay dos formas de distribuir las revistas electrónicas. Algunas se distribuyen a través de listas de correo. Cuando aparece un número nuevo, éste se envía a todos los suscriptores a través de correo electrónico. Otras revistas se almacenan en servidores de *ftp anónimo* muy conocidos. Pueden cargar los nuevos números en su computadora, incluso los números atrasados, cuando quiera.

LISTAS DE CORREO

Una **lista de correo** es un sistema organizado en el que un grupo de personas reciben y envían mensajes sobre un tema en particular. Estos mensajes pueden ser artículos, comentarios o cualquier cosa relacionada con el tema en cuestión.

Todas las listas de correo -y hay miles de ellas- tienen una persona que se ocupa de mantenerlas. Es posible subscribirse o eliminarse de esa lista, enviando un mensaje a la dirección apropiada. Muchas listas de correo están "moderadas", lo que significa que alguien decide qué mensajes se envían a la lista de correo y cuales no. Otras listas no son moderadas, de forma que se envían todos los mensajes sin censura alguna.

INTERNET BBS

Un **BBS**, o tablón de anuncios por computadora (**B**ulletin **B**oard **S**ystem), es una especie de almacén de mensajes y archivos, a menudo desarrollados para un tema en particular.

Para utilizar un BBS, hay que conectarse y seleccionar opciones de una serie de menús que irán apareciendo.

Típicamente, un BBS es administrado por una persona u organización en particular. Hay innumerables sistemas de BBS en el mundo, la mayoría de los cuales son accesibles por teléfono. En **INTERNET** hay muchos BBS que son accesibles por el más refinado servicio *telnet*.

MUD

Un ***mud***, o Multiple User Dimension, es una computadora que proporciona una realidad virtual. Para participar en un *mud*, se debe hacer un *telnet* a un servidor *mud*, asumir un papel y explorar, se interactúa con otros usuarios que están representando sus propios papeles.

DIRECCIONES INTERNET

Los sistemas de redes modernos están construidos con la filosofía de "niveles o capas de servicio", la primera capa mueve bits de un lugar a otro, este nivel se compone de cables y hardware. El siguiente nivel, agrega software básico que permite aislar los problemas del hardware. Para el tercer nivel, se incorpora otra capa de software para dar al software básico algunas características deseadas. Y conforme se agregan capas, agregamos funcionalidad e inteligencia a la red, capa por capa, hasta que obtenemos algo amigable y útil.

REDES DE CONMUTACION DE PAQUETES

Cuando tratamos de imaginar qué es **INTERNET** y cómo funciona, es normal pensar en un sistema telefónico. Después de todo, ambos son electrónicos, ambos permiten abrir una conexión y transferir información, e **INTERNET** está compuesta principalmente por líneas telefónicas permanentemente dedicadas a este uso. Desafortunadamente, esto crea una idea errónea y provoca mucha confusión sobre la forma en que funciona **INTERNET**. La red telefónica es una red de conmutación de circuitos es decir que cuando hablamos por teléfono, se separa una parte de la red para dedicarla a atender nuestra llamada. Aun cuando no estemos utilizando nuestra parte de la red (por ejémplo cuando la línea está en espera), ésta es inaccesible para otras personas, lo que provoca una subutilización de un recurso muy costoso: la red.

Un mejor modelo para entender el funcionamiento de **INTERNET** mediante analogías, es el servicio de correo, ya que se opera como una red de conmutación de paquetes. Nosotros no contamos con una parte de la red dedicada a nuestras actividades. Lo que queremos enviar se mezcla con los mensajes de otras personas, se pone en un conducto, se transfiere a otra oficina de correos y se clasifica todo nuevamente. Aunque las tecnologías son completamente diferentes, el servicio de correo es sorprendentemente similar, razón por la cual esta analogía la utilizaremos a lo largo del capítulo.

EL PROTOCOLO INTERNET, IP

Las diferentes partes de **INTERNET** están conectadas por un conjunto de computadoras llamadas *enrutadores o ruteadores,* que interconectan a las redes. La arquitectura de estas redes puede ser Ethernet, Token-Ring, líneas telefónicas o cualquier otro medio físico. No obstante ésta es equivalente a los camiones y aviones del servicio postal. Es el medio a través del cual el correo va de un lugar a otro.

Podemos decir que los ruteadores son las sucursales postales, ya que son los encargados de decidir cómo dirigir la información o "paquetes"; de la misma forma que una oficina de correos decide como distribuir los sobres por correo. No toda subestación o todo ruteador cuenta con una conexión a cada uno de los otros ruteadores de la red. Si envíamos un sobre de correo desde Baja California con destino al Distrito Federal, la oficina de correos no reserva un avión de Baja California a México para llevarlo, sino que envía el sobre a la sucursal de correo más cercana en dirección al destino y ésta a su vez lo envía a otra, y así sucesivamente hasta que nuestro sobre alcanza su destino final. Esto significa que cada subestación sólo necesita conocer las conexiones con las que cuenta y cual es el mejor "siguiente salto" para acercar el paquete a su destino. **INTERNET** trabaja de manera similar, un ruteador se fija en el destino de la información y decide a donde enviarla. El ruteador elige cual es el enlace más apropiado para enviar la información.

Ahora ¿Cómo sabe la red a donde se dirige la información? Si se quiere enviar una carta, no basta con poner el papel escrito en el buzón y esperar a que sea entregado. Es necesario poner el papel con la información en un sobre, escribir la dirección del destinatario y pegar los timbres postales.

De la misma manera que la oficina de correos tiene reglas que definen la operación de su red, también existen reglas que definen la operación de **INTERNET**. Las reglas son llamadas protocolos. El **PROTOCOLO/INTERNET** (IP) se hace cargo de establecer direcciones o se asegura de que los ruteadores sepan que hacer con la información que les llega. Si comparáramos al protocolo IP con la oficina de correos, éste trabajaría como un sobre, ya que una parte de la información de la dirección va al principio del mensaje. Estos datos le dan a la red información suficiente para hacer la entrega del *paquete.*

Los direcciones de **INTERNET** constan de cuatro números, cada uno menor que 256, y cuando dichos números se escriben, se separan por puntos, como se muestra a continuación:

- *125.111.66.5*
- *101.243.10.6*

Las direcciones **INTERNET** están formadas por varios campos, pero dado que **INTERNET** es una RED de redes, los primeros números de la dirección indican a los ruteadores cual es la dirección de la RED a la que pertenecemos, mientras que los últimos números indican cual computadora personal o equipo anfitrión de la red debe recibir el paquete. Bajo este esquema, cada computadora en **INTERNET** tiene un domicilio único.

Si consideramos la dirección "Av. Universidad 1810-A1, Coyoacán, D.F." la parte "Coyoacán, D.F." es como la parte de la dirección correspondiente a la red, la cual le permite al sobre llegar a la oficina de correos correcta, que es la que tiene la información acerca de las calles en un área determinada. La parte "Av. Universidad 1810-A1" es como la dirección del equipo anfitrión; éste identifica a un buzón particular en el área de servicio de la oficina de correos. La oficina de correos concluye su trabajo cuando entrega el correo a la oficina local correcta y ésta lo pone en el buzón correcto. De la misma forma, **INTERNET** concluye su trabajo cuando los ruteadores llevan la información a la red local correcta y ésta entrega dicha información a la computadora personal o equipo anfitrión correctos, localizados en dicha RED.

Por muchas razones prácticas (sobre todo por limitaciones de hardware), la información enviada a través de las redes IP se divide en segmentos de diferente tamaño llamados comúnmente *paquetes*. Y la cantidad de información que puede llevar un paquete normalmente se encuentra entre 1 y aproximadamente 1500 caracteres de largo. Esto previene que cualquier usuario monopolice la red, permitiendo que todos tengan un acceso equitativo. También significa que cuando la red se sobrecarga, su rendimiento afecta a todos los usuarios de la RED en forma distribuida, de tal suerte que desde el punto de vista usuario solamente se torna ligeramente mas lenta.

Una de las propiedades más impresionantes de **INTERNET** es que, en un nivel básico, el protocolo IP es todo lo que necesitamos para participar en la RED. Por supuesto el protocolo IP por si solo no es muy amigable, pero es lo suficientemente útil.

Pese a que con la dirección IP la RED tiene toda la información que necesita para llevar el paquete hasta su destino, Se tienen que resolver varios problemas:

- La mayoría de las transferencias de información es mayor que 1500 caracteres, estaríamos decepcionados si la oficina de correos sólo entregara tarjetas postales y rechazara cualquier cosa más grande.

- En ocasiones se presentan errores, ocasionalmente la oficina de correos puede perder una carta. De la misma forma algunas veces las redes pierden paquetes o éstos pueden dañarse durante la transmisión. A diferencia de lo que sucede con la oficina de correos, en **INTERNET** se pueden resolver estos problemas exitosamente.

- Los paquetes pueden llegar en desorden. Si se envían dos cartas al mismo lugar en días consecutivos no existe la garantía de que viajarán por la misma ruta o llegarán en el mismo orden. Lo mismo sucede con **INTERNET.**

Para corregir todo esto, la siguiente capa de la red nos permitirá enviar grandes cantidades de información y corregirá todas las alteraciones que puedan ser causadas por la red.

EL PROTOCOLO DE CONTROL DE TRANSMISION (TCP)

TCP es el protocolo que se menciona frecuentemente junto con el IP y que se utiliza para resolver los problemas mencionados. ¿Qué pasaría si queremos enviar un libro a alguien y la oficina de correos sólo aceptara cartas? Una de las soluciones sería arrancar todas las hojas del libro, ponerlas en un sobre cada una y depositarlas en un buzón. La persona que reciba las cartas tendrá que asegurarse de recibirlas todas y volverlas a empastar en el orden original. Aunque en términos prácticos postales es inviable, esto es precisamente lo que hace el protocolo TCP.

El protocolo TCP toma la información que se desea enviar y la divide en segmentos menores a 1500 bytes, enumera cada segmento para que el receptor pueda verificar la información y colocarla en el orden adecuado. Para que el protocolo TCP pueda enviar esta secuencia de números a través de la red, cuenta con su propio "sobre" en el cual escribe la información requerida para su reordenamiento. Un segmento de la información a transmitir se coloca en el sobre del protocolo TCP, el cual a su vez es puesto, dentro del sobre del protocolo IP y una vez que se pone algo en un sobre IP, la red lo puede transmitir.

Del lado del destinatario, una parte del software del TCP reúne los sobres, extrae la información de ellos y la pone en el orden adecuado. Si algún sobre se pierde en la transmisión, el receptor solicita su retransmisión al emisor. Una vez que el protocolo TCP tiene toda la información en el orden adecuado, la pasa a la aplicación del programa que esté utilizando sus servicios.

La descripción anterior del funcionamiento del protocolo TCP es ligeramente utópica. En la realidad, los paquetes no sólo se pierden, sino que además de esto, pueden ser modificados por el mal funcionamiento durante la transmisión a través de las líneas telefónicas o en cualquier otro segmento de la RED, el protocolo TCP también resuelve este tipo de problemas.

Como parte de la información que coloca dentro de su sobre, añade un número de verificación (Checksum) calculado a partir de la información que va a contener cada sobre TCP, y permite que el receptor TCP detecte errores en el paquete transmitido. Cuando un paquete llega a su destino, el receptor calcula el número de verificación y lo compara con el enviado por el transmisor. Si no coinciden, significa que ocurrió un error durante la transmisión. El receptor descarta ese paquete y solicita la retransmisión.

Cuando utilizamos el protocolo TCP, pareciera que tenemos una conexión permanente entre dos aplicaciones, garantizando de esta forma que lo que se transmite de un lado llega al otro. Lo que realmente sucede es que no tenemos un enlace directo entre emisor y receptor, ya que otras personas pueden usar los mismos ruteadores y la misma red de cableado en los lapsos que ocurren entre el envío de cada paquete.

Claro que manejar TCP implica inversión en tiempo, y si la información que requerimos transmitir cabe en un solo paquete (es menor a 1500 Bytes), y no necesitamos garantizar su entrega, podemos utilizar otros protocolos que sean mas sencillos de manejar.

Uno de estos protocolos es *el Protocolo de Datagramas de Usuario o UDP*, el cual substituye a TCP, es decir que en lugar de colocar la información en un sobre TCP para después ponerla en un sobre IP, esta aplicación pone la información en un sobre UDP y después en un sobre IP.

El protocolo UDP es mucho más sencillo, porque no se preocupa porque los paquetes se pierdan, ni por que la información llegue en orden, el UDP se usa comúnmente en programas que envían mensajes cortos y que sólo reenvían la información si no reciben una respuesta en un tiempo determinado. Por ejemplo, queremos desarrollar un programa que busca números telefónicos en una base de datos en algún lugar de la red. No existe ninguna razón para establecer una conexión de TCP con el objeto de transmitir 20 caracteres en ambas direcciones. Sólo es necesario poner un nombre en el paquete UDP, después en un paquete IP y por último enviarlo a la red. La otra aplicación recibirá el paquete, lee el nombre, busca el número telefónico, pone la información en otro paquete UDP y lo envía de regreso.

¿Qué pasa si el paquete se pierde en el trayecto? El programa tendrá que encargarse de esto: si espera por mucho tiempo sin obtener respuesta, simplemente envía otra solicitud.

Ahora que se tiene la habilidad de transferir información entre dos nodos de la red, es posible empezar a trabajar para hacer que **INTERNET** sea más amigable. Esto es posible utilizando el software adecuado para la tarea que se quiera realizar y poniendo nombres con letras en lugar de sólo números para referirse a las computadoras.

SISTEMA DE NOMENCLATURA DE DOMINIOS

Al principio, las personas aceptaban que las combinaciones de números como direcciones estaban bien para que las máquinas se comunicaran entre si, pero para los usuarios es preferible utilizar nombres. Por esto, a las computadoras de **INTERNET** se les asignaron nombres para la conveniencia de los usuarios, y las aplicaciones de **INTERNET** permiten el uso de nombres en lugar de una combinación de números para definir las direcciones de las computadoras.

Es un hecho que también los nombres tienen problemas implícitos, debemos asegurarnos de que nunca dos computadoras dentro de **INTERNET** se llamen igual, es necesario tener una forma de convertir los nombres a combinaciones numéricas. Es posible dar un nombre de computadora a un programa, pero es necesario que el programa tenga una forma de convertir el nombre en una combinación de números. Análogamente cuando buscamos en el directorio telefónico, realizamos la misma operación.

En un principio, cuando **INTERNET** era un lugar pequeño, el manejo de los nombres era sencillo. El NIC, Centro de Información de la Red (**N**etwork **I**nformation **C**enter), estableció un registro, en el cual una persona enviaba una forma electrónica y el NIC incorporaba la información en una lista de nombres y direcciones. Este archivo, llamado *hosts,* era distribuido en forma periódica a todos los nodos de la red. Los nombres eran simples palabras, no se podían repetir. Si se usaba un nombre, la computadora buscaba en la lista y lo convertía a un domicilio numérico. Cuando **INTERNET** creció y se multiplicó, lo mismo sucedió con la tabla de nombres, se requería mucho tiempo para que un nombre quedara registrado y se volvía más difícil encontrar nombres que no hubiesen sido utilizados, también se requería de mucho tiempo de red para poder distribuir el archivo de la lista a cada máquina de la red.

Era obvio que un sistema distribuido en línea era requerido para satisfacer la rapidez con que cambiaba la información del archivo de nombres. A este sistema se le denomina *Sistema de Nomenclatura de Dominios o DNS.*

ESTRUCTURA DEL SISTEMA DE DOMINIOS

El Sistema de Nomenclatura de Dominios es un método para administrar nombres distribuyendo en diferentes grupos la responsabilidad de subconjuntos de nombres. A cada nivel de este sistema se le llama *dominio*. Y al igual que a las direcciones IP los dominios se separan por puntos tal y como se muestra en los siguientes ejemplos:

- *martini.eecs.umich.edu*
- *glis.cr.usgs.gov*

Puede haber cualquier cantidad de dominios en un nombre, al leer un nombre de izquierda a derecha, cada dominio será más vasto que el dominio que tenga a la izquierda. En el nombre martini.eecs.edu, *martin* es el nombre del equipo anfitrión, una computadora con una dirección IP. El nombre para esa computadora se asigna y mantiene por el grupo *eecs*, que puede ser el departamento donde ésta se localiza. El departamento *eecs* es parte de la University of Michigan (umich). *umich* a su vez, es parte de un grupo nacional de instituciones educativas (edu). De esta forma, el dominio *edu* está compuesto por todas las computadoras de las instituciones educativas, el dominio *uiuc.edu* contiene a todas las computadoras de la University of Michigan y así sucesivamente.

Cada grupo puede crear o cambiar todo lo que esté dentro de él. Si *umich* decide crear otro grupo que se llame *ncsa*, lo puede hacer sin solicitar ningún permiso. Sólo tiene que agregar el nuevo nombre a su parte de la base de datos mundial y tarde o temprano todo aquel que lo necesite descubrirá el nuevo nombre *ncsa.umich.edu*, de igual manera, el departamento *eecs* puede comprar una nueva computadora, asignarle un nombre y conectarla a la red sin pedir permiso a nadie. Si cada grupo a partir de *edu* respeta las reglas y se asegura de que los nombres que asigne sean únicos, ningún nombre en **INTERNET** se repetirá.

Hemos dicho que la mejor forma de entender una dirección es leerla de derecha a izquierda. El dominio de primer nivel será la especificación más general. Existen dos tipos de dominios de primer nivel: el formato antiguo *dominios de organizaciones* y el nuevo *dominios geográficos.*

Los dominios de organizaciones están basados en un esquema de direcciones que fué desarrollado antes de que aparecieran las redes internacionales. Fue proyectado principalmente para utilizarse dentro de los Estados Unidos.

La idea era que el dominio de primer nivel debería indicar el tipo de organización que era responsable de la computadora. La tabla 1-1 muestra las distintas categorías. Todas estas categorías existen desde el comienzo de **INTERNET**, excepto *int*, que es de reciente creación para determinadas organizaciones que traspasan las fronteras nacionales (como la OTAN).

Una vez que **INTERNET** se extendió internacionalmente, se hizo necesario crear nuevos dominios de primer nivel que fueran más específicos. Para enfrentarse a esta necesidad, se desarrolló un sistema nuevo de dominios geográficos, en el que una abreviación de dos letras representan un país entero. Hay muchos dominios de primer nivel de este tipo -uno por cada país en **INTERNET**- como ejemplo en la tabla 1-2 aparece un resumen.

Tabla 1-1 Dominios de primer nivel de tipo organización.

Dominio	Significado
com	organización comercial
edu	institución educativa
gov	gobierno
int	organización internacional
mil	organización militar
net	gestión de redes
org	organización no lucrativa

Como podemos observar en la Tabla 1-2, los Estados Unidos tienen un dominio geográfico *us*, aunque no se suele utilizar, generalmente ahí se utiliza la nomenclatura organizacional, sin embargo, los dominios geográficos son los que se utilizan en los demás países dentro de **INTERNET**.

Tabla 1-2 Ejemplos de dominios de primer nivel de tipo geográfico.

Dominio	Significado
at	Austria
au	Australia
ca	Canadá
de	Alemania
dk	Dinamarca
es	España
fr	Francia
gr	Grecia
ie	República de Irlanda
jp	Japón
mx	México
nz	Nueva Zelanda
uk	Reino Unido
us	Estados Unidos

Cuando se usa un nombre como *martini.eecs.umich.edu*, la computadora necesita convertir el nombre de la dirección en una dirección numérica, para hacerlo, empieza a hacer peticiones de ayuda a los servidores DNS, empezando por el extremo derecho y recorriendo la dirección hacia la izquierda. Primero, se pregunta por la dirección al servidor DNS local, si el servidor local conoce el domicilio, automáticamente nos conectará hasta la dirección deseada, si no lo conoce entonces el software del servidor local debe comunicarse con el servidor raíz, quien conoce las direcciones de los *servidores de nombres* que tienen a su cargo los dominios de jerarquía superior (los dominios de la derecha, como por ejemplo *edu*). Un servidor de nombres pregunta al servidor raíz la dirección de la computadora responsable de la zona *edu*. Con esta información, se comunica con ese servidor y le pide la dirección del servidor *umich*, después, contacta a esa computadora y le solicita la dirección del servidor eecs, finalmente se comunica también con esa máquina y obtiene la dirección de martini, que es la máquina con la que originalmente nos deseábamos comunicar.

CONEXIONES INTERNET

¿Qué significa tener acceso a **INTERNET**? Significa utilizar una computadora que es parte de una red unida a **INTERNET**. De una forma práctica, significa que se pueden utilizar los recursos de **INTERNET** que se han descrito anteriormente, cuando utilizamos esta computadora, decimos que estamos en **INTERNET**.

Antes de mencionar las distintas formas en las que se puede tener acceso a **INTERNET**, necesitamos conocer las dos formas de conectarse a **INTERNET**. Primero, se puede utilizar una computadora que esté conectada directamente a **INTERNET**, por ejemplo es pbsible utilizar una estación de trabajo que es parte de una red conectada a **INTERNET**. En este caso la computadora será un *host* de **INTERNET**, con su propia dirección electrónica. La otra forma de conectarse a **INTERNET** es utilizar una terminal (o una estación de trabajo emulando terminal) conectada a un host de **INTERNET**. En este caso, la propia terminal no está en **INTERNET**, simplemente se hace uso de una terminal que tiene acceso a una computadora que está en **INTERNET**.

Veamos un ejemplo, si dentro de un edificio tenemos un laboratorio de cómputo, en el que hay 40 computadoras conectadas en RED, la cual está conectada a **INTERNET**, entonces.todos los usuarios de estas PC's pueden tener acceso directo a **INTERNET**. Ahora, si entramos a la sala de terminales y tenemos ahí 40 terminales, todas ellas conectadas a un equipo central, el cual también está conectado a **INTERNET**, cada usuario de las terminales tendrá acceso a **INTERNET**.

En ambos casos los usuarios tienen acceso a **INTERNET**, la diferencia es que cada PC es un host de **INTERNET**, es decir que cada PC tiene su propia dirección **INTERNET** y es autosuficiente, mientras que en la sala de terminales los usuarios accesan a **INTERNET** conectándose a la computadora central que proporciona la conexión a **INTERNET**. De este modo, todos comparten la misma computadora que tiene una sola dirección **INTERNET**.

Lo que ambas soluciones tienen en común es que los dispositivos computadoras y terminales están conectados directamente por algún tipo de cable. Este tipo de conexión se denomina *conexión directa*. La ventaja principal de este tipo de conexión es su permanencia, ya que todo lo que tenemos que hacer es encender la PC o la terminal y la conexión está lista para ser utilizada. Como contraparte la principal desventaja, es la falta de flexibilidad, ya que si queremos cambiar la ubicación física de alguna máquina es necesario desplazar también los cables.

CONEXIONES TELEFONICAS

Un sistema mucho más flexible que el esquema anterior es aquel en el que la computadora o terminal utiliza una *conexión telefónica* sobre una línea de teléfono, en estos casos se puede trabajar en cualquier lugar, siempre y cuando se tenga acceso a una línea de teléfono. Para utilizar una conexión telefónica, es necesario un dispositivo de hardware para convertir las señales de computadora en señales telefónicas y viceversa.

En términos técnicos, las señales que envía una computadora son "digitales" y las de una línea telefónica son "analógicas". Un aparato que convierte señales digitales a analógicas se llama *modulador*, mientras que un aparato que convierte señales analógicas a digitales se llama *demodulador*. Cuando se conecta una computadora a través de una línea telefónica, hay que enviar datos en ambas direcciones, razón por la cual utilizamos un *módem* (*mod*ulador -*dem*odulador).

Existen en el mercado diferentes tipos de modems, sin embargo independientemente del módem que utilicemos para conectarnos, siempre necesitaremos de un módem en cada extremo de la línea telefónica.

CONEXION DE UNA TERMINAL A UNA LINEA TELEFONICA

Es muy común, utilizar una PC para accesar a una computadora remota a través de una línea telefónica. Por ejemplo, es posible tener un host de **INTERNET** en el trabajo o en la universidad que se quiera utilizar desde casa. Estos host están normalmente instalados de forma que aceptan conexiones de una terminal. Esto es, se puede conectar una terminal a la línea telefónica (utilizando un módem) y llamar al host remoto. Una vez que se ha establecido la conexión, se puede trabajar en la terminal de la forma habitual.

Dado que la PC es una computadora completa y no meramente una terminal, necesitamos ejecutar en la computadora un programa que *emule* una terminal, ya que el host remoto está configurado de forma que sólo puede comunicarse con terminales. La mayoría de los programas que nos permiten hacer esto son los programas de comunicaciones, los cuales además de inicializar nuestro módem, nos permiten emular diferentes tipos de terminales.

Sin importar el tipo de terminal que emulemos, en lo que debemos tener cuidado es en que sea el mismo tipo que soporta el host, ya que de lo contrario en la pantalla de nuestra máquina veremos solamente caracteres ASCII sin ningún sentido.

Dos de los parámetros a considerar para seleccionar un programa de comunicaciones son el buffer de desplazamiento el cual se refiere a la capacidad de mostrar caracteres que han desplazado hacia arriba en la pantalla, y la posibilidad de trabajarlo al tiempo que ejecutamos otro programa, es decir que lo podamos ejecutar bajo Microsoft Windows o bajo OS/2 por ejemplo, ya que además de poder hacer otras tareas podemos cortar y pegar la información.

CONEXION DE UNA COMPUTADORA A UNA LINEA TELEFONICA

La mayoría de las veces, la mejor forma para conectarse a un host de **INTERNET** sobre una línea telefónica consiste en utilizar una computadora que emule una terminal, no obstante debemos recordar que estamos actuando como una terminal, no somos un host de **INTERNET**. En ocasiones tenemos la necesidad de trabajar como un host real de **INTERNET**, en estos casos, existe una solución para establecer una conexión completa a **INTERNET** sobre una línea telefónica.

Primero debemos disponer de algún host de **INTERNET** que actúe como punto de conexión. Entonces instalamos algún programa de comunicaciones que nos permita utilizar el protocolo PPP (**P**oint to **P**oint **P**rotocol) o SLIP (**S**erial **L**ine INTERNET **P**rotocol), los cuales nos permiten enlazar las dos computadoras a través de un módem sin emular terminal, y una vez que se establece la conexión entre las dos computadoras estos programas nos darán capacidades TCP/IP, con lo que nuestra computadora se convertirá en un host real de **INTERNET**, con su propia dirección electrónica oficial.

Cuando se instalan estos sistemas, debemos de tomar en cuenta el tipo de línea telefónica que vamos a utilizar, si usamos una línea conmutada o normal, aunque la computadora sea considerada como un host real de **INTERNET**, no estará conectada todo el tiempo a la RED, por lo que es necesario indicar a la computadora que actúa como punto de conexión, que almacene los mensajes de correo electrónico que llegan cuando no está conectada.

La otra alternativa es utilizar una línea telefónica dedicada o privada, la cual estará permanentemente conectada, con la consecuencia directa de un aumento en el costo, sin embargo, para algunas empresas, una línea telefónica dedicada usando PPP, puede ser una forma relativamente económica para establecer un acceso a **INTERNET**, ya que esta conexión puede proporcionar acceso a **INTERNET** al resto de computadoras de la empresa.

INTERNET

Cronología

- 1957 Lanzamiento del satélite Soviético "Sputnik".
- 1960 El Gobierno de E.U. se prepocupa en como mantener la comunicación después de un ataque.
- 1960 J. LICKLIDER.- Propone interconectar computadoras de gobierno.
- 1962 Paul Rand (RAND Corporation) sugiere utilizar líneas telefónicas, para transmitir paquetes de Información.
- 1967 La Universidad de Michigan toma el proyecto ARPANET (**A** dvanced **R**esearch **P**rojects **A**gency **Net**work).

Notas:

INTERNET

Cronología

- 1968 BBN (Bolt Beranek and Newman, Inc), la concesión del proyecto. Dos objetivos: Militar e Investigación.
- 1969 Universidad de California (Los Angeles) primer Nodo ARPANET.
- 1969 Universidades de California (Santa Bárbara), Stanford Research Institute y Utah, se integraron como Nodos.
- 1970 ARPANET tiene 7 Nodos, bajo el protocolo NCP (Network Control Protocol).
- 1973 25 Nodos, se acumula un mayor número de investigadores y científicos.

Notas:

INTERNET

Cronología

- 1979 256 Nodos, el protocolo NCP no soporta el tráfico en la Red.
- 1982 Se crea un nuevo Protocolo IP (Internet Protocol).
- 1985 La National Science Foundation (NSF) propone extender la red a más investigadores y científicos, se integran 5 supercomputadoras.
- 1987 La Red se satura NSF encarga a : Metir, Inc (Compañía Operadora de Redes), e IBM y MCI (Compañía telefónica) el proyecto NFSNET.
- 1990 ARPANET, NSFNET y Redes pequeñas se unen, para conformar INTERNET.
- 1994 Comienza Boom Mundial de INTERNET.

Notas:

INTERNET

Definición

- Permite la comunicación entre personas
- Compartir recursos

Notas:

INTERNET

Definición

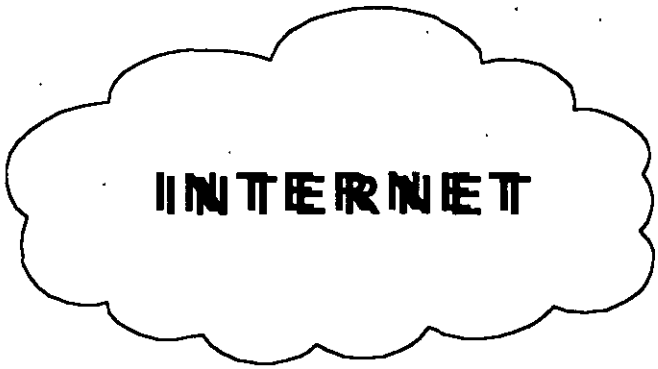
En Internet se comparten recursos lógicos

- Archivos
- Bancos de Información
- Noticias
- Foro de discusiones
- " Conocimientos "

Notas:

INTERNET

Conformación



Notas:

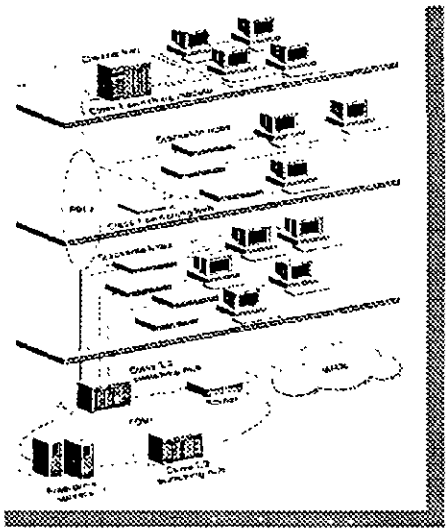
INTERNET

Conformación

Redes Lan

Redes Wan

Internet



Notas:

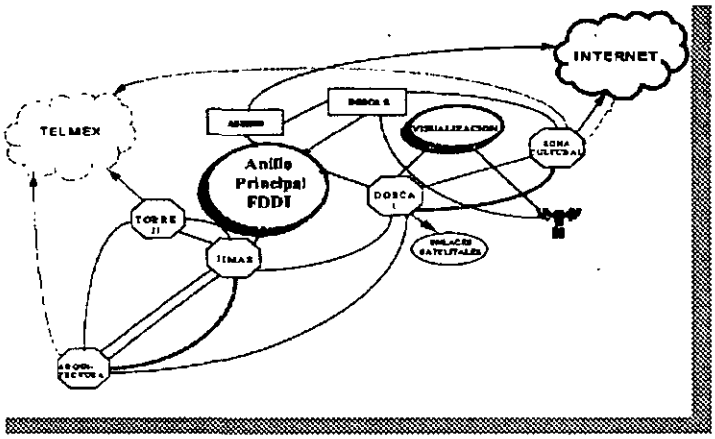
INTERNET

Conformación

Redes Lan

Redes Wan

Internet



Notas:

4/0

INTERNET

Definiciones

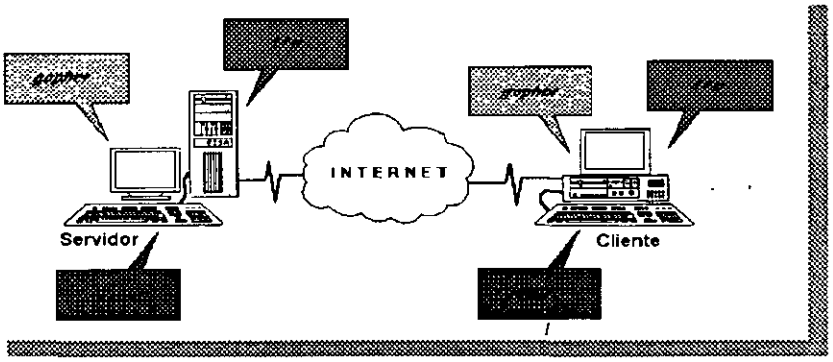
- **Host** Cualquier computadora que accesa a INTERNET.
- **Nodo** Sinónimo técnico de Host.
- **Terminal** Teclado y Video conectado a un Host Unix, que a su vez puede ser un Host INTERNET.
- **Servidor** Host que contiene el software y la información para proporcionar un servicio.
- **Cliente** Nodo que contiene el software para accesar la información de un servicio de un servidor INTERNET.

Notas:

4/1

INTERNET

Sistema Cliente/Servidor



Notas:

42

INTERNET

Cliente

" Aprender a navegar por INTERNET, significa aprender a usar cada uno de los programas clientes disponibles "

Notas:

INTERNET

Uso Servicios:

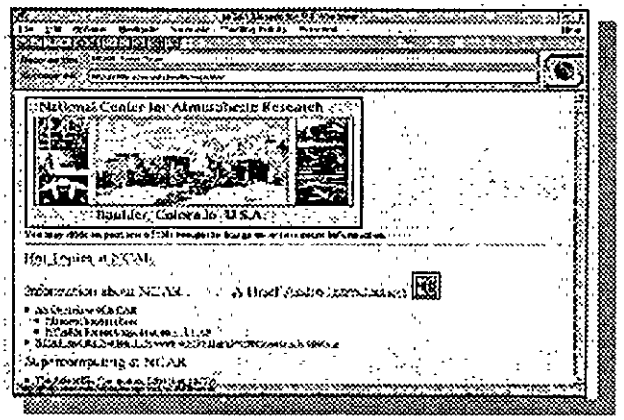
Para utilizar un servicio INTERNET, hay que entender:

- Como ejecutar el programa cliente para este servicio.
- Como decirle al programa cliente que servidor se requiere utilizar.
- Que instrucciones se pueden utilizar con cada tipo de cliente.

Notas:

INTERNET

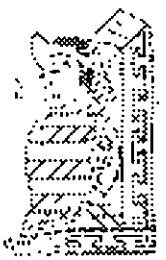
X - Window, Cliente X



Notas:

INTERNET/INTRANET
SERVICIOS E IMPLEMENTACION DE SERVICIOS

PRINCIPALES SERVICIOS PROPORCIONADOS POR INTERNET



OCTUBRE 1997

INTERNET

Clasificación de servicios

- Servicios.
- Herramientas.
- Otros.

Notas:

47

INTERNET

Servicios:

- Correo Electrónico (*e-mail*).
- Conexión remota (*telnet*).
- Noticias de la Red (*usenet*).
- Transferencia de archivos (*ftp)* .
- Conversaciones en la red (*talk, ytalk*).
- Conferencia en la Red (*Internet Realy Chat IRC*).
- Menués de Acceso (*gopher*).
- Revistas Electrónicas
- Listas de correo
- Internet BBS

Notas:

INTERNET

Herramientas:

- **Búsquedas:**
  - **De personas (*finger*).**
  - **De archivos (*archie*).**
  - **De recursos (*veronica & jughead*).**
  - **De información (servidores *wais*).**
  - **Directorio de páginas blancas**

Notas:

INTERNET

Otros

- Acceso total a INTERNET (*World Wide Web*).
- Juegos multiusuario (*MUD*).

Notas:

INTERNET

Tipos de Redes de Computadoras

- Conmutación de circuitos.
  - Analogía: Red telefónica .
- Conmutación de paquetes.
  - Analogía: Servicio postal de correo.

Notas:

INTERNET/INTRANET
SERVICIOS E IMPLEMENTACION DE SERVICIOS

TCP/IP

OCTUBRE 1997

INTERNET

Protocolos

T ransmission

C ontrol

P rotocol

I nternet

P rotocol

Notas:

INTERNET

TCP/IP Arquitectura

Protocolo a nivel de Transporte

- **TCP** Transmission Control Protocol.
- **UDP** User Datagram Protocol.
- **NVP** Network Voice Protocol.

Notas:

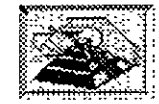
TCP/IP Arquitectura

Protocolo a nivel de Red

- **IP** Internet Protocol.
- **ICMP** Internet Control Message Protocol.
- **ARP** Address Resolution Protocol.
- **RARP** Reserver Address Resolution Protocol.
- **RIP** Routing Information Protocol.
- **EGP** External Gateway Protocol.
- **OSPF** Open Shortes Path First.

Notas:

INTERNET



TCP/IP

IP: INTERNET PROTOCOL

Brinda dos servicios básicos:

- Enrutamiento
- Fragmentación/Re-ensamblaje

Utiliza direcciones IP para decidir el ruteo.
Aisla los protocolos superiores de las características
Específicas de la Red.

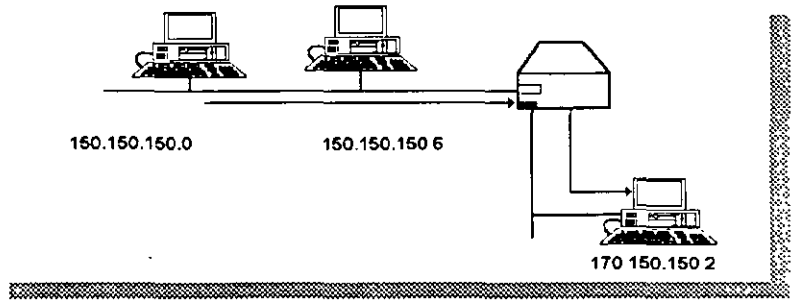
Notas:

INTERNET

TCP/IP

IP: INTERNET PROTOCOL

ENRUTAMIENTO



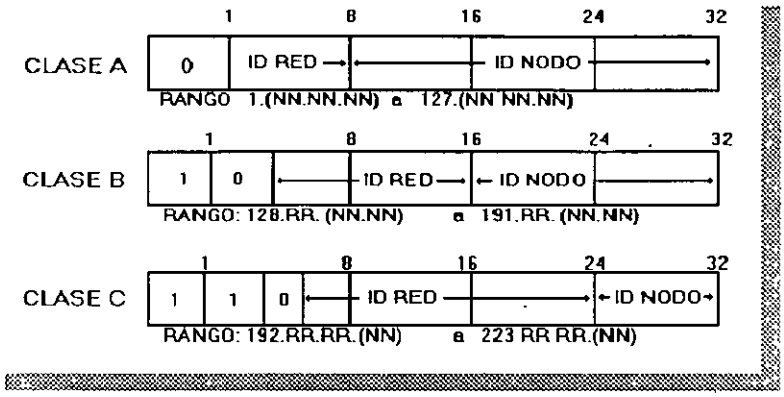
Notas:

57

INTERNET

TCP/IP

Formato de las direcciones IP



Notas:

57

INTERNET

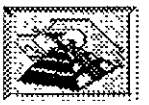
TCP/IP

PROTOCOLO TCP
Transmission Control Protocol

- Asignación de números de puerto para transmisión de datos
- Reconocimiento de datos recibidos
- Regulación de flujo de datos
- División de los mensajes en datagramas
- Verificación de los datagramas
- Administración
  - Establecimiento
  - Mantenimiento
  - Terminación

Notas:

INTERNET



TCP/IP

PROTOCOLO NVP
Network Voice Protocol

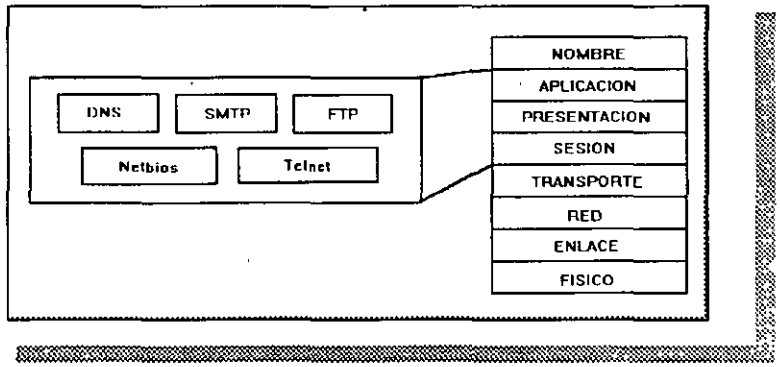
- Servicio para transporte de voz digitalizada.
- Protocolo de transacción de tiempo real.
- Utiliza IP para transmitir información.
- Emplea algoritmos de compresión.
- Es connection less.

Notas:

INTERNET

TCP/IP

Nivel 5-7 Sesión - Aplicación



Notas:

INTERNET

TCP/IP

D N S
Domain Name Service

- Protocolo de nombramiento.
- Brinda traducción de nombre-dirección IP.
- Dominio: Grupo de Host.
- " Domain Name Server ".

- Información del servidor.
  - Dirección Internet.
  - Tipos de Computadoras.
  - Lista de servicios brindados por computadoras.

- Servidor
  - Servidores Maestros.
  - Primario.
  - Secundario.

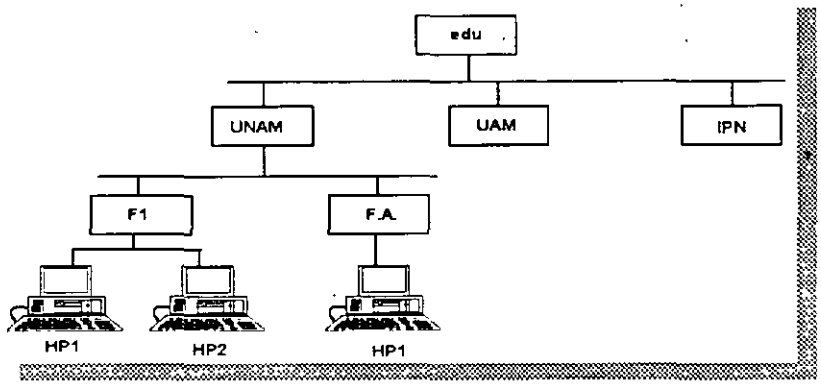
Notas:

02

INTERNET

Estructura del Sistema de Dominios

Dominios de organizaciones



Ejemplos:

Hp1.F1.UNAM.edu
Hp1.Fa.UNAM.edu
***gopher* .gsfc.nasa,gov**

Notas:

63

INTERNET

Estructura del Sistema de Dominios

Dominios Geográficos

Dominio	Significado.	Ejemplo:
at	Austria.	ftp.vmars.tuwien.ac.at
ca	Canadá.	debra.dgbt.doc.ca
fr	Francia.	grasp.insa.lyon.fr
mx	México.	telecom.mty.ltesm.mx
uk	Reino Unido.	puffin.doc.ic.ac.uk
us	Estados Unidos.	gopher.well.sf.ca.us

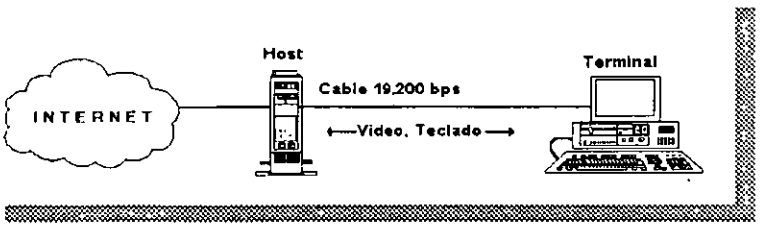
Nota: En E.U. se utilizan los dominios organizacionales y en el resto del mundo la estructura geográfica.

Notas:

INTERNET

Conexión Directa

Tipos de Conexiones



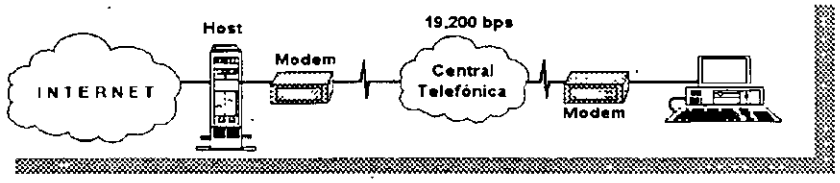
Protocolo físico (1,2 OSI): Rs-232
CSMA/CD

Notas:

INTERNET

Línea Telefónica Conmutada (Dial up)

Tipos de Conexiones



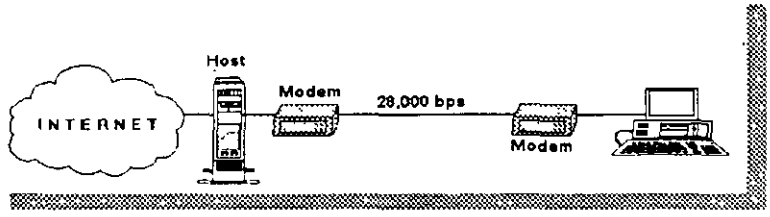
Protocolo físico (1,2 OSI): SLIP/PPP

Notas:

INTERNET

Línea Telefónica Privada

Tipos de Conexiones



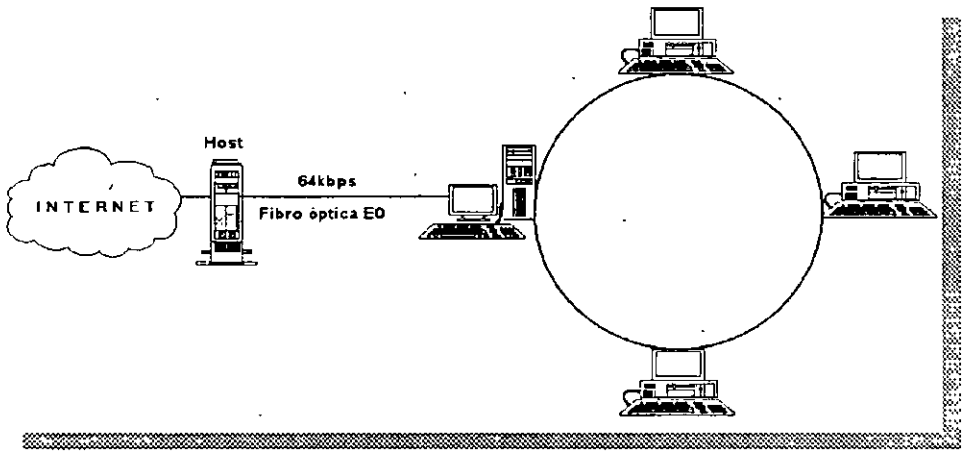
Protocolo físico (1,2 OSI): SLIP/PPP

Notas:

INTERNET

Fibra Optica

Tipos de Conexiones



Protocolo físico (1,2 OSI): SLIP/PPP

Notas:

Velocidades Típicas de Acceso

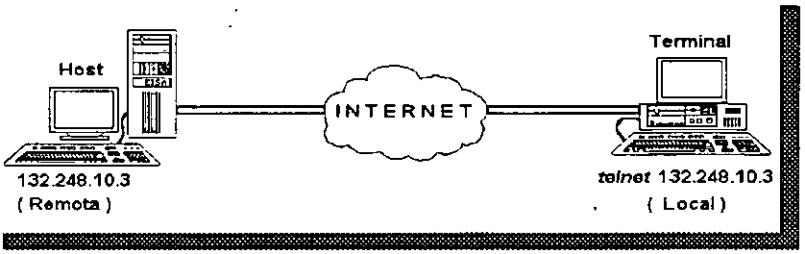
Tipo de Acceso	Medio	Velocidad Máxima
Dial	Línea Conmutada	19.2 kbps
Enlace	Línea dedicada	28.8 kbps
E0	Canal E0	64 kbps
ISDNB	Línea ISNDB	128 KBPS
E1	Canal E1	2.2 mbps
T1	Canal T1	1.544 mbps
T3	Canal 3	44.746 mbps
SONET	OC -n = 1,3,12,24,48	51./2,488.2 mbps

Notas:

INTERNET

Sesión Remota Interactiva

telnet : Emulación de terminal



Notas:

telnet : Puertos Virtuales

telnet 132.248.10.3 23

Puerto virtual

telnet downwing.sprl.umich.edu 3000

- Se utiliza para servicios especiales.
- El default es el puerto 23.

Notas:

INTERNET

***telnet* :**

```
% telnet lpi.jsc.nasa.gov
Trying 192.101.147.11 ...
Connected to lpi.jsc.nasa.gov.
Escape character is '^]'.

        VAX/VMS V5.4

Username: LPI

          VAX/VMS V5.4
Last interactive log in on Wednesday, 1-DEC-1993 12:28
Last non-interactive log in on Wednesday, 1-DEC-1993 06:35
LUNAR AND PLANETARY INSTITUTE MAIN MENU

 x  General Information
 x  Information and Research Services
 x  Lunar and Planetary Bibliography
 x  Image Retrieval and Processing System (IRPS)
 x  Meeting Information and Abstracts
 x  Venus and Mars: Gravity and Geophysics
 x  Mars Exploration Bulletin Board
 x  Lunar and Planetary Information Bulletin
 x  Help
 x  Exit and Logout
```

Notas:

Transferencia de archivos

ftp: file transfer protocol

- Permite copiar un archivo desde cualquier host Internet a otro host Internet.
- Uno de los servicios más importantes de Internet.
- Arquitectura cliente/servidor.
- Usuario general : *anonymous*.
- Clave de acceso: dirección de correo electrónico.
- También se le conoce como *ftp anónimo*.
- Existe la opción *ftp mail*.

Notas:

INTERNET

f t p, *ejemplo*

```
% ftp rtfm.mit.edu
Connected to CHARON.MIT.EDU.220 charon    ftp server
(Versión 6.6 Web Arp 14 21:00:27 EDT 1994) ready.

Name (rtfm.mit. edu:pedro): anomymous
331 Guest login ok, send   e-mail address as password.
Password: 230 Guest login ok, access restrictions apply.

ftp> cd / pub /  usenet / news.answers
250 CWD command successful.

ftp> hash
Hash mark printing on (8192 bytes/hash mark).

ftp> get folklore-faq
200 PORT  command successful.
150 Opening ASCII mode data connection for folklore-faq (84701 bytes).
######################
226 Transfer complete.local: folklore-fag remote: folklore-faq 86113 bytes
received in 17 seconds (4.9 Kbytes/s).

ftp> quit
221 Goodbye.
```

Notas:

INTERNET

f t p, ejemplo

```
% mail ftpmail@decwrl.dec.com
Subjet: Ejemplo de transferencia binaria con uuencode
reply pedro.huerta@industry.net
connect ftp.uu.net
binary
uuencode
chdir / doc / literary / obi / DEC / humor
get Lawyer.jokes.Z
quit
CTRL-D
EOT
```

Notas:

INTERNET

Localización de artículos en f t p

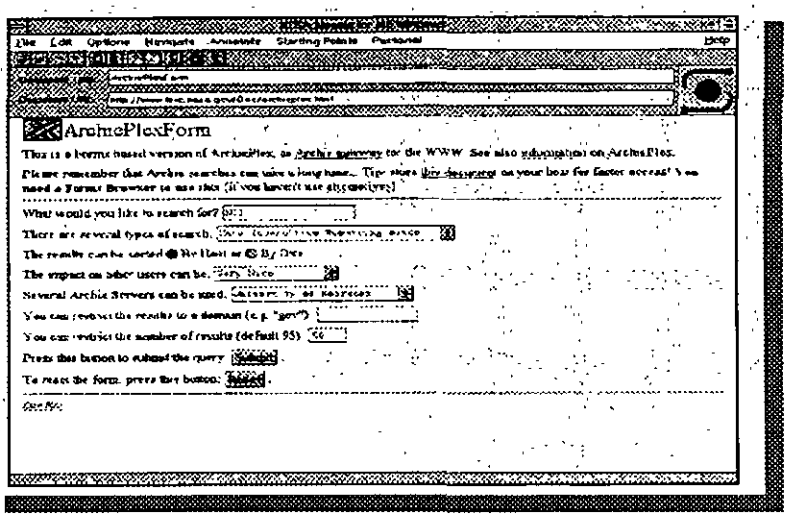
archie:

- Herramienta de búsqueda de archivos.
- Permite accesar el cátalogo de la biblioteca de archivos más grande del mundo.
- Existen servidores y clientes *archie.*

Notas:

INTERNET

archie:



Notas:

archie:

Existen tres formas de utilizarlo

- *telnet* a un servidor *archie*.
  Identificador de usuario: *archie.*
  - Se puede utilizar el servicio *" whatis ".*
- Utilizar un cliente *archie.*
- Enviar por correo peticiones a un servidor *archie.*

Notas:

78

INTERNET

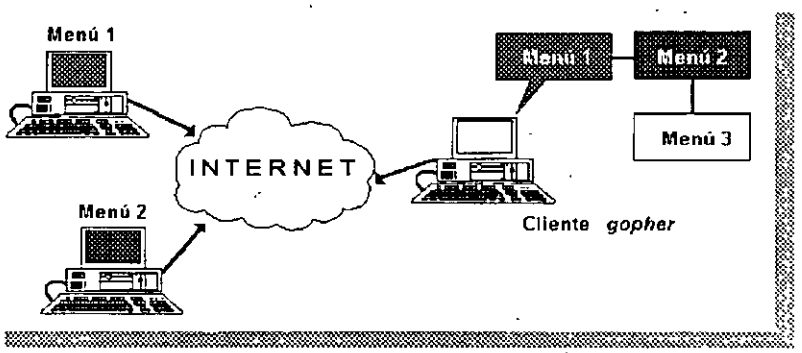
gopher

- Permite accesar los recursos de Internet a través de menués.
- Los recursos enumerados en un menú pueden estar en cualquier parte de Intenet.
- Arquitectura cliente/servidor.
- La mayoría de los servidores *gopher* son públicos.
- Se define el término *gopherespacio.*

Notas:

INTERNET

gopher: Búsqueda por menués

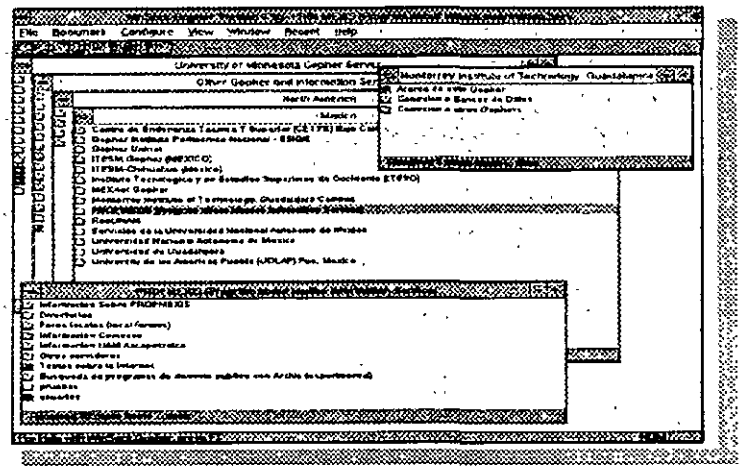


Notas:

80

INTERNET

gopher: Ejemplo



Notas:

81

Servicios basados en *gopher*

- *veronica:*
  - Busca menués que contengan una palabra determinada.
- *jughead* :
  - Similar a *veronica* , pero busca en un área moderada del *gopherespacio.*

Notas:

INTERNET

World Wide Web

- Conocido también como:
  - *WWW*
  - W3
  - Web
- Objetivo:

  Ofrecer una interface simple y consistente a la inmensidad de recursos que prorporciona Internet.

Notas:

83

INTERNET

World Wide Web

- Está basado en el Hipertexto.
- Un documento de Hipertexto contiene datos y Posiblemente enlaces a otros documentos.
- Los datos pueden ser textos, imágenes, sonidos y animaciones.
- Surge la hipermedia.

Visualizador o browser.- Programa para leer un documento de Hipertexto.

Notas:

INTERNET

World Wide Web

- Intento por organizar toda la información de Internet.
- El Web no es perfecto.
- Existen algunas limitaciones.
- Arquitectura cliente/servidor.

Notas:

INTERNET

World Wide Web

Visualizadores:

- **Modo lineal.**
- **X-Window.**
  - **Mosaic.**
- **Windows y Mac.**
  - **Netscape (PC´s, Mac´s).**

Notas:

INTERNET

World Wide Web

Formato de entrada

http: // *www.* njit.edu

Notas:

87

INTERNET

World Wide Wed

```
                                                    Overview of the Web (23/27)
                                  GENERAL OVERVIEW

   There is no "top" to the World Wide Web.  You can look at it from
   many points of view.  If you have no other bias, here are some places
   to start:

     by Subject[1]          A classification by subject of interest.
                            Incomplete but easiest to use.

     by Type[2]             Looking by type of service (access protocol,
                            etc) may allow you to find things if you know
                            what you are looking for.

     About WWW[3]           About the World Wide Web global information
                            sharing project.

Starting somewhere else

     To use a different default page, perhaps one representing your field
     of interest, see  "customizing your home page"[4]

1-8, Up, <RETURN> for more, Quit, or Help:
```

Notas:

88

INTERNET

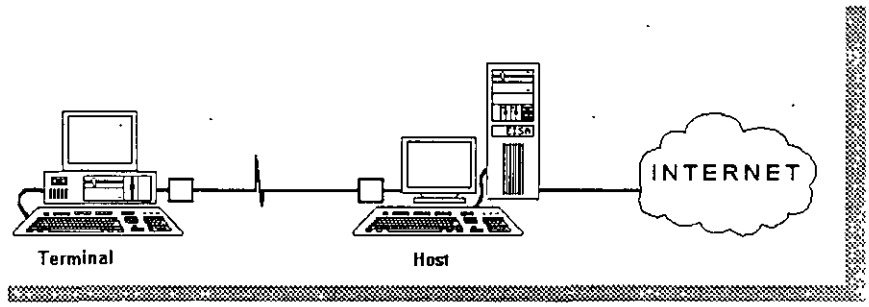
Tipos de Archivos

- Compactados.
  - (Unix: compress, uncompress, *.z)
  - (Dos: pkzip, pkunzip, *.zip)
- Recopilados.
  - (Unix: tar, *.tar. *.tar.z)
  - (Dos: , *.taz)
- Texto o Binarios.
  - (binario a texto: uuencode)
  - (texto a binario: uudecode, *.uue, *.uue.z)
- Tipo *shar*.
  Ejecutable que se desempaqueta.
  - (*.*shar*, *.*shar*.z)
  - (sh, unshar)

Notas:

INTERNET

Transferencia de Archivos



Notas:

90

INTERNET

Transferencia de Archivos

- Comandos Unix, emulando terminal
  - sz.- Carga un archivo desde un Host remoto
  - rz.- Descarga un archivo a un Host remoto
- Utilizan el protocolo *zmodem*

Ejemplos:

```
sz -a document
sz -b picture.gif
rz -a document
```

-a → tipo texto.
-b → tipo binario.

Notas:

INTERNET

Lista de Correos

- Se agupan personas en una lista de un tema de interes común, para el manejo de mensajes de correo electrónico.
- Se define un Alias para un grupo de personas.

Notas:

INTERNET

Servicio *wais*

Wide **A**rea **I**nformation **S**ervice

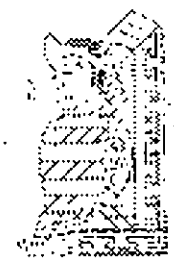
- Servicio de información de área extensa.
- Hace búsquedas en base a palabras.
- Arquitectura cliente/servidor.

Notas:

93

INTERNET/INTRANET
SERVICIOS E IMPLEMENTACION DE SERVICIOS

CREACION DE SERVIDORES



OCTUBRE 1997

Installation and Administration Guide

Microsoft Knowledge Base

How To Install and Configure Microsoft DNS Server

Last reviewed: August 28, 1997
Article ID: Q172953

The information in this article applies to:

- Microsoft Windows NT Server version 4.0

SUMMARY

This article is designed as an introduction to the Microsoft Domain Name Service (DNS) included with Microsoft Windows NT Server 4.0. This guide will take you through the steps needed to install and configure DNS on your Windows NT Server.

For additional information on Domain Name Service, please see the following white paper available on the Microsoft anonymous ftp server:

```
File Name: Dnswp.exe
Location : ftp://ftp.microsoft.com/bussys/winnt/winnt-docs/papers/
Title    : "DNS and Microsoft Windows NT 4.0"
```

MORE INFORMATION

Installing Microsoft DNS

Use the following steps to install DNS on your Windows NT 4.0 Server:

1. Click the Start button, point to Settings, and then click Control Panel. Double-click the Network icon, and then click the Services tab.
2. Click Add, select Microsoft DNS Server from the Select Network Service dialog box, and then click OK.
3. Type the location of your Windows NT source files, click OK, and then click Close.

NOTE: If you have any service packs installed, you will need to re-apply your service pack before restarting your computer.

1. Restart your computer.

Configuring Microsoft DNS

Gathering Information:

Before you actually begin configuring the DNS server, there is some basic information you will need. Some of this information must be approved by Internic for use on the Internet, but if you are configuring this server for internal use only, you can then decide what names and IP addresses to use. You will need:

- Your domain name (must be approved by Internic)
- The IP address of each server for which you wish to provide name resolution
- The host names of each of the servers in step above

NOTE: The servers in the step above may be your mail servers, any public access servers, FTP servers, WWW servers, and so on.

For example, use the following information (substitute your actual information where appropriate):

```
Domain Name: <Domain.com>
Servers:    192.168.50.11   <Mail1.domain.com>
            192.168.50.12   <Ftp1.domain.com>
            192.168.50.12   <WWW.domain.com> (notice the same IP address)
            192.168.50.15   <DNS1.domain.com>
```

Creating Your DNS Server:

Using the information above, configure your Microsoft DNS server by doing the following:

1. Click the Start button, point to Programs, point to Administrative Tools, and then click DNS Manager.
2. From the DNS menu, click New Server.
3. Type the IP address of your DNS server in the Add DNS Server dialog box (192.168.58.15 in the example information), and then click OK.

NOTE: It is not necessary to restart the DNS server for changes to your zones to take effect. All that is required is for the server data files to be updated using the following step:

- In DNS Manager, right-click your DNS server, and click Update Server Data Files.

Creating Your Reverse Lookup Zone:

Some applications use a reverse query to a DNS server to find the host name of a host when it has the IP address of the computer. You must configure a reverse lookup zone to provide this capability.

NOTE: Reverse lookup zones may not be necessary in your network, but it is recommended that one be present.

To create a reverse lookup zone, perform the following steps:

1. In DNS Manager, right-click your DNS server, and then click New Zone.
2. Click Primary from the "Creating New Zone for" dialog box, and then click Next.
3. The Zone Name is derived from your IP network address. In the example information, the Zone Name is 58.168.192.in-addr.arpa. Type your reverse zone name (the least significant part of the IP address, and work toward the most significant part of the address). For example:

```
If your network ID is:          Then your reverse zone is:

10.0.0.0                        10.in-addr.arpa
130.20.0.0                      20.130.in-addr.arpa
250.30.203.0                    203.30.250.in-addr.arpa
```

NOTE: The syntax of the reverse lookup zone is imperative to its operation.

4. After you type the reverse lookup zone name, press Tab and the reverse lookup zone file name will automatically fill in using the zone name in step 3 appended by ".dns" (without the quotes).
5. Click Next, and then click Finish.

Creating Your Forward Lookup Zone:

1. In DNS Manager, right-click your server, and then click New Zone.
2. Click Primary Zone, and then click Next.
3. Type the Zone Name for your DNS domain. This is the domain name that is registered with Internic (<Domain.com> in the example).
4. Press Tab, click Next, and then click Finish.

When you have created the forward lookup zone, you should see three records automatically created in that zone: the NS record, the SOA record, and an A record. If you do not have all three of these, you may want to verify that your DNS settings in your TCP/IP properties are configured correctly (click the Start button, point to Settings, click Control Panel, and then double- click the Network icon).

Adding Host Records to Your Forward Lookup Zone:

The A record for your DNS server should have been automatically created. However, DNS Manager does not automatically create the PTR record in the reverse zone for the DNS server. The simplest way to correct this is to use the following steps:

1. Right-click the A record for your DNS server, and then click Delete Record.
2. Click Yes in the confirmation dialog box.
3. Right-click your forward zone, <Domain.com>, and then click New Host.
4. Type the host name of your DNS server and the IP address.
5. Click Create Associated PTR Record to enable it and click Add Host.
6. Click Done.

NOTE: Repeat steps 3-5 above for all of the servers that you want to add to your DNS domain.

To verify the PTR records are created successfully, right-click the reverse lookup zone 58.168.192.in-addr.arpa, and then click Refresh.

Configuring Other Record Types

A DNS server can be responsible for several different record types. Some of them include, but are not limited to the following: A, CNAME, HINFO, MX, NS, and SOA. For details on these and other record types, please refer to the DNS white paper mentioned earlier in this article.

Creating A CNAME Record:

A CNAME record allows you to use multiple names for the same IP address. This way, you can have users access the same server for separate functions, such as FTP1.domain.com and WWW.domain.com. Before you can create the CNAME record, you must first have an A record, as described earlier.

To create a CNAME record, perform the following steps:

1. Right-click your forward zone, <Domain.com>, and click New Record.
2. Select CNAME Record from the Record Type list box in the New Resource Record dialog box.
3. Type an alternate name for access to this computer. For example, in the sample information earlier in this article, WWW is an alternate name for FTP1.domain.com.
4. Type the original host name in "For Host DNS Name." For example, <FTP1.domain.com>.

   NOTE: It is important to use the fully-qualified domain name (FQDN) for the originating host DNS name.
5. Click OK.

Now when your users make a query for either of these host names, your DNS server will return the same IP address.

Creating an MX Record:

An MX Record is a Mail Exchange record that points mail programs to your mail servers. To create an MX record, perform the following steps:

1. Right-click your forward lookup zone, <Domain.com> and then click New Record.
2. Select MX Record from the Record Type list box in the New Resource Record dialog box.
3. The Host Name (Optional) field is used for the host name of the mail server. However, if you want users to be able to send mail to your domain using the format USER@Domain.com, then leave the Host Name field blank.
4. Enter the FQDN of the mail server in the Mail Exchange Server DNS Name, for example, Mail1.domain.com.
5. The Preference Number is any number from 0 to 65535. In the case of multiple mail servers, this number identifies which mail server is to be used first. The lower the preference number, the higher the priority.
6. Click OK.

```
Keywords          : kbhowto kbinfo nthowto ntnetserv NTSrv nttcp kbnetwork
Version           : WinNT:4.0
Platform          : winnt
Issue type        : kbhowto kbinfo
Solution Type     : Info_Provided
```

Did this information help answer your question?

◯ **Yes** ◯ **No** ◯ **It didn't apply** Submit

INCIDENTAL DAMAGES SO THE FOREGOING LIMITATION MAY NOT APPLY.

Last reviewed: August 28, 1997

CHAPTER 1

Installing Internet Information Server

This chapter will help you quickly and easily install Microsoft Internet Information Server for Windows NT Server.

All you need to do is connect your Windows NT–based computer to the Internet or your intranet (your local or wide area network), install Microsoft Internet Information Server software and specify your home directory. This chapter tells you how.

Important To publish on the World Wide Web (WWW) and the Internet, you must contact an Internet Service Provider (ISP) to obtain an Internet connection. Your ISP will provide your server's Internet Protocol (IP) address, subnet mask, and the default gateway's IP address. (The default gateway is the computer through which your computer will route all Internet traffic.)

Installation Overview

You can easily install Internet Information Server while you install Windows NT Server. When prompted to install Internet Information Server, make sure the check box is selected and click **OK**. That's it! If you already have the necessary Internet or intranet connection, you can accept all of the default settings during setup and then add your Hypertext Markup Language (HTML) content files to the Wwwroot folder. Your files will be immediately available to users. The default setup configurations are suitable for many publishing scenarios without any further modifications.

This section defines the installation requirements and explains how to.

- Configure Windows NT before installation
- Run the Setup program
- Set up files to publish

- Test your installation.

Installation Requirements

Microsoft Internet Information Server requires.

- A computer with at least the minimum configuration to support Windows NT Server; see "Windows NT Configuration and Security Checklists," later in this chapter.
- Windows NT Server version 4 0.

  Note You can administer a server running Internet Information Server from a remote computer running Windows NT Workstation. Install the Peer Web Services Internet Service Manager on that computer, and then connect to the server you want to administer.

- Transmission Control Protocol/Internet Protocol (TCP/IP) (included with Windows NT). Use the Network application in Control Panel to install and configure the TCP/IP protocol and related components.
- A CD-ROM drive for the installation compact disc.
- Adequate disk space for your information content It is recommended that all drives used with Microsoft Internet Infomation Server be formatted with the Windows NT File System (NTFS).

To publish on an intranet, you will need

- A network adapter card and local area network (LAN) connection.
- The Windows Internet Name Service (WINS) server or the Domain Name System (DNS) server installed on a computer in your intranet. This step is optional, but it does allow users to use "friendly names" instead of IP addresses.

To publish on the Internet, you will need

- An Internet connection and Internet Protocol (IP) address from your Internet Service Provider (ISP).
- DNS registration for that IP address This step is optional, but it does allow users to use "friendly names" instead of IP addresses when connecting to your server. For example, microsoft com is the domain name registered to Microsoft Within the microsoft.com domain, Microsoft has named its World Wide Web (WWW) server www.microsoft com Most ISPs can register your domain names for you.
- A network adapter card suitable for your connection to the Internet

Windows NT Configuration and Security Checklists

You must configure the Windows NT Server networking component so that your Web server can operate on the Internet. Microsoft recommends that you also enhance the Windows NT default security settings and implement other Windows NT security measures to prevent users from tampering with your computer or network. For more information about security, see Chapter 5, "Securing Your Site Against Intruders."

Windows NT Configuration Checklist

Use the Network application in Control Panel for all configuration tasks mentioned in this section.

- **Obtain an Internet Connection.** To publish on the Internet, you must have a connection to the Internet from an ISP. To find an ISP, look in the telephone book under Computers-Networking or in your local newspaper's business or technology section.

- **Install Windows NT Server.** Install Windows NT Server version 4.0 and Microsoft Internet Information Server

- **Configure the TCP/IP Protocol.** Install the Windows NT TCP/IP Protocol and Connectivity Utilities. Your ISP must provide your server's IP address, subnet mask, and the default gateway's IP address. (The default gateway is the ISP computer through which your computer will route all Internet traffic)

  Note If the FTP service provided with Windows NT has been installed, remove it. Also remove any other previously installed Internet services.

- **Configure the Site's Domain Name** (also called Host Name). On the Internet, your IP address (for example, http.//10.138 59.1/homepage.htm) can always be used to contact your Web server. However, if you register a domain name in the DNS, your server can be contacted by using a "friendly" domain name (for example, http.//www.company com/homepage.htm) ISPs can usually register domain names for you

- **Configure Name Resolution.** You need a name resolution system to map IP addresses to computer names or domain names On the Internet, Web sites usually use the Domain Name System Once you have registered a domain name for your site, users can type your site's domain name in a browser to contact your site ISPs can register domain names for you

  On an intranet, you can use either DNS or the Windows Internet Name Service (WINS) Your network must have DNS or WINS servers to match IP addresses to host names, and client computers must know the IP address of the DNS or WINS server to contact

An alternative to DNS is to use a HOSTS file. On intranets an alternative to WINS Servers is to use an LMHOSTS file. Use the Network application in Control Panel to make the appropriate Advanced TCP/IP Configuration setting for this server's name resolution. For more information on installing and configuring WINS or DNS, see the Windows NT online Help.

- **WWW Virtual Servers.** Optionally, if you have registered multiple domain names (such as www.company1.com and www company2.com), you can host multiple domain names on the same computer running Microsoft Internet Information Server. You use Advanced TCP/IP Configuration settings to assign multiple IP addresses to the network adapter card connected to the Internet. You should register a domain name for each IP address on your adapter.

Windows NT Security Checklist

Several steps can be taken to enhance the security of a computer publishing information on an intranet or the Internet. For further information on these checklist topics, see Chapter 5, "Securing Your Site Against Intruders."

User Accounts

- Review the IUSR_*computername* account's rights.
- Choose difficult passwords.
- Manage strict account policies.
- Limit the membership of the Administrators group.

NTFS File Security

- Use Access Control Lists (ACLs), available with NTFS
- Enable auditing to track file access.

Running Other Network Services

- Run only the services that you need
- Unbind unnecessary services from your Internet adapter cards.

Warning Make sure to check with your system administrator because unbinding services could have undesirable effects

---

- Check permissions on network shares.

Before Installing Internet Information Server

Before installing the Internet Information Server services, disable any other Internet services.

If your server has another version of File Transfer Protocol (FTP), gopher, or World Wide Web (WWW) services installed (such as the FTP service included with Windows NT or the European Microsoft Windows Academic Centre [EMWAC] services included in the Windows NT Resource Kit), disable these services before you install the Microsoft Internet Information Server services. See the documentation for each service to see how to disable it.

FTP Guest Account Access

During the setup process, a screen will appear, asking you whether you want to disable access by the Guest account to your FTP server

Microsoft recommends that you select **Yes** to protect the contents of your system. If you choose the **No** option and enable guest access to your server, all existing files and any new files will be available to the Guest account through FTP. You will need to disable access to each file or folder individually to prevent unauthorized access. Disabling FTP access for the Guest account will not affect the IUSR_*computername* account that is created during setup.

Administrator Privileges Required

To install the services for Internet Information Server, you must be logged on to the server with administrator privileges. You also need administrator privileges to configure the services remotely through Internet Service Manager

Installation Folder

By default, Internet Information Server is installed from the compact disc to C:\Winnt\System32\Inetsrv. If you change the default, be sure to enter a fully qualified path name, including a drive letter. Relative paths and paths without drive letters can be misinterpreted by Setup

Remove All Button

When setting up a new version of Internet Information Server from your computer, click the **Remove All** button to delete the previous version

Event Log Availability

If you remove Internet Information Server, you will be unable to review IIS events in the Event Log.

Content Folders and Files

The **Remove All** button in Setup removes all Internet Information Server program files but does not remove the directory structure or any content or sample files. This setting protects your content files from unintentional deletion. If you want to remove these folders and files after completing the Remove All process, delete them by using Windows NT Explorer.

Converting 16-Bit ODBC Drivers to 32-Bit during Setup

If there are data sources referring to 16-bit Open Database Connectivity (ODBC) drivers on the system, Setup will detect them and ask you if you want to convert them to 32-bit. If you choose **Yes**, these data sources will be converted to refer to the 32-bit ODBC drivers

---

Installing Internet Information Server

You can install Internet Information Server while installing Windows NT Server or after you have installed Windows NT Server

To install Internet Information Server during Windows NT Server Setup

1. When prompted, make sure the **Install Microsoft Internet Information Server** check box is selected and click the **Next** button.

   The Internet Information Server Setup program begins.

2. Follow the instructions on the screen If you have questions, click the **Help** button in any dialog box.

If you do not install Internet Information Server while setting up Windows NT Server, you can install it separately any time afterward To install Internet Information Server separately, you must be logged on with administrator privileges

To install Internet Information Server after installing Windows NT Server

1. Insert the Windows NT Server compact disc into the CD-ROM drive.

2. Double-click the Install Internet Information Server icon on the Windows NT Server Desktop.

3. Follow the instructions on the screen If you have questions, click the **Help** button in any dialog box

You can also install Internet Information Server by using the Windows NT Control Panel.

1. Insert the Windows NT Server compact disc into the CD-ROM drive

2. On the Windows NT taskbar, click **Start**, point to **Settings**, and then click **Control**

Panel.

3. In Control Panel, double-click the Network icon.

4. On the **Network** property sheet, click the **Services** tab.

5. Click the **Add** button.

6. From the **Network Services** list, select **Microsoft Internet Information Server**, and then click the **OK** button.

7. In the **Installed from** box, type the letter of the drive where your compact disc is located, and click the **OK** button

8. Follow the instructions on the screen. For information about any of the Setup dialog boxes, click the **Help** button

Alternatively, you can install Internet Information Server directly from the Windows NT Server compact disc.

1. Insert the Windows NT Server compact disc into the CD-ROM drive.

2. In Windows NT Explorer or at the command prompt, change to the drive containing the compact disc

3. Start Setup:

- To start Setup from Windows NT Explorer, double-click the file named Inetstp exe in the Inetsrv folder of the compact disc
- To start Setup from the command prompt, change to the Inetsrv folder of the compact disc and then type **inetstp**.

4. Follow the instructions on the screen If you have questions, click the **Help** button in any dialog box

Setup Process for Internet Information Server

This section walks you through the setup process and gives guidelines for setting up Internet Information Server

1. When you start the Setup program, the Microsoft Internet Information Server **Welcome** dialog box appears. Click the **OK** button

2. All of the options in the second dialog box are selected by default. Click the **OK** button to install them all. If you do not want to install a particular item, clear the box next to it and then click the **OK** button to install the rest

Internet Service Manager installs the administration program for managing the services.

World Wide Web Service creates a WWW publishing server.

Gopher Service creates a gopher publishing server.

FTP Service creates an FTP publishing server.

ODBC Drivers and Administration installs Open Database Connectivity (ODBC) drivers. These are required for logging to ODBC files and for enabling ODBC access through the Internet Database Connector (IDC) from the WWW service.

Important If you want to provide access to databases though the Microsoft Internet Information Server, you need to set up the ODBC drivers and data sources by using the ODBC application in Control Panel. Please see Chapter 8, "Publishing Information and Applications," for specific instructions

---

If you are running an application that uses ODBC, you may see an error message telling you that one or more components are in use. Before continuing, close all applications and services that use ODBC

Sample files installs sample Hypertext Markup Language (HTML) files.

You can use the Setup program later to add or remove components. Setup can also remove all Internet Information Server components.

3. Accept the default installation folder (C:\Winnt\System32\Inetsrv) or click the **Change Directory** button and enter a new folder

Note If you have installed Internet Information Server, but want to reinstall it into another folder, you must remove the following key from the registry: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\INetStp. If you do not delete this key, the **Change Directory** button will be dimmed and you will be unable to change the default folder.

4. Choose the **OK** button When prompted click **Yes** to create the installation folder.

The **Publishing Directories** dialog box appears

Accept the default folders for the publishing services you have installed, or change the folders

Note If you already have files ready to publish, you can enter the full path to their current location, or move them into the default folders later. If your files are on a network drive, you should accept the default folder. After setup is completed, use

Internet Service Manager to change your default home directory to the path for the network folder containing your files; for example, *Servername**Sharename*\WWWfiles. Be sure to carefully check the permissions on the network drive; there may be security implications. See Chapter 5, "Securing Your Site Against Intruders."

5. Choose the **OK** button.

6. When prompted to create the service folders (Wwwroot, Gophroot, and Ftproot by default), click **Yes**.

7. Setup copies all remaining Internet Information Server files.

8. If the **ODBC Drivers and Administration** option box was selected, the **Install Drivers** dialog box appears.

To install a driver, select it from the **Available ODBC Drivers** list box, and choose the **OK** button.

Setup completes copying files.

9. When the Setup completion dialog box appears, click the **OK** button to complete Setup.

This final step completes Peer Web Services Setup. Now you must close the **Services** property sheet and restart your computer for the changes to take effect.

The preceding steps are all that is required for a simple installation You are now ready to publish on the Internet or your intranet. There is no need to start Internet Service Manager unless you want to make advanced configuration changes (If so, refer to Chapter 3, "Configuring and Managing Internet Information Server ") Use the Services application in Control Panel to confirm successful installation of the publishing services.

Unattended Setup When Installing from a Network Folder

If you are using Microsoft Internet Information Server on a network you can copy the contents of the Inetsrv folder on the Windows NT compact disc to a folder on your network and perform unattended installations over the network from that folder. (You can start an unattended setup from the compact disc itself, however, only the default configuration can be installed in this case) This is useful for installing the services software on several computers in your network

In the Inetsrv folder, there is an Unattend txt file Unattend txt is a sample configuration file used by the program for unattended installation. You modify the values in the file to configure setup. In general, the value 1 represents TRUE and the value 0 represents FALSE It is suggested that you copy Unattend txt to the folder containing the Inetstp.exe file you will use, then modify it to meet your installation requirements.

To start unattended setup you must use the command prompt. Change to the folder containing both Inetstp.exe and Unattend.txt and type

inetstp -b unattend.txt

where Unattend.txt is the file you have modified. See Unattend.txt on the compact disc for more information about unattended setup.

The IUSR_*computername* Account

Setup automatically creates an anonymous account called IUSR_*computername*. This account has a randomly generated password and privilege to log on locally. On domain controllers, this account is added to the domain database. This process is fully automatic. After installation is complete, you can change the user name and password for this account from the **Service** property sheet in Internet Service Manager, as long as the new user name and password match the same user name and password in the Windows NT User Manager.

Note If you change the anonymous user name account (IUSR_*computername*) in the Windows NT User Manager for Domains, Microsoft suggests you copy the IUSR_*computername* account and then give it a new name and password, rather than create an entirely new account. By copying the IUSR_*computername* account you are sure to carry over all the privileges and user rights granted to that account. Then change the anonymous user name and password in the Internet Service Manager, making sure it is the exactly same as the new user name and password created in the User Manager for Domains.

The WWW, FTP, and gopher services use the IUSR_*computername* user account by default when anonymous access is allowed To set the rights for IUSR_*computername*, use User Manager. To set file permissions on NTFS drives for IUSR_*computername*, use Windows NT Explorer. To change the account used for anonymous logons for any of the Internet Services, select the **Service Properties** option from the **Properties** menu in Internet Service Manager.

How to Publish Information

Now that Microsoft Internet Information Server is installed and running, you are ready to publish on the Internet or your intranet Publishing information with Internet Information Server is easy. If your files are in HTML format, just add them to the appropriate home directory For example, to make files available to a Web browser using the WWW service, place the files in the Wwwroot folder.

For more extensive information on creating and publishing content files, see Chapter 8, "Publishing Information and Applications " Note that you can also create and publish highly interactive systems by writing programs that use ISAPI.

Note If you provide files with the gopher or FTP services, you can share those files instantly.

Users can navigate through the files much as they do in Windows NT Explorer or at the command prompt. With gopher, you can customize how your folders and files appear to browsers; you can also include links to other servers in your files. FTP can be used to accept files from or send files to Internet users.

Attempting to Publish from Redirected Network Drives

The FTP, gopher, and WWW services cannot publish from redirected network drives (that is, from drive letters assigned to network shared folders). To use network drives, you must use the server and share name (for example, *Computername**Sharename**Wwwfiles*). If you require a user name and password to connect to a network drive, all requests from remote users to access that drive must be made with the user name and password you specified, not the anonymous IUSR_*computername* account or another account you may have specified

Consider security issues carefully when using this feature Remote users could possibly make changes to a network drive by using the permissions of the user name specified to connect to the network drive.

Default.htm and the Internet Information Server Home Page

By default, Internet Information Server uses a file named Default htm as the home page for the various samples, tools, and demonstrations that come with the product. If the Wwwroot folder of your Web server already contains a file named Default.htm when you install Internet Information Server, your file will not be overwritten with our file. As a result, you will not have immediate access to our sample home page and the links it provides when you run Internet Information Server

In this case, to view our version of Default htm and the links it provides, type the following Uniform Resource Locator (URL) in the Internet Explorer **Address** box.

http://*computername*/samples/default.htm

This command loads the file Default.htm from the Wwwroot\Samples folder.

You can also rename or move your version of Default.htm to a different folder and then copy the file Default.htm from the Samples folder This approach will make our version of Default htm your Web server's home page

How to Test Your Internet Information Server Installation

You can test your installation by using Internet Explorer to view the files in your home directory.

To test a Web server connected to the Internet

1. Ensure that your Web server has HTML files in the Wwwroot folder.

2. Start Internet Explorer on a computer that has an active connection to the Internet. This computer can be the computer you are testing, although using a different computer is recommended.

3. Type in the URL for the home directory of your new Web server.

The URL will be "http://" followed by the name of your Web server, followed by the path of the file you want to view. (Note the forward slash marks.) For example, if your server is registered in DNS as "www.company.com" and you want to view the file Homepage.htm in the root of the home directory, in the **Address** box you would type:

http://www.company.com/homepage.htm

then press the ENTER key The home page should appear on the screen.

To test a Web server on your intranet

1. Ensure that your computer has an active network connection and that the WINS server service (or other name resolution method) is functioning.

2. Start Internet Explorer.

3. Type in the Uniform Resource Locator (URL) for the home directory of your new server.

The URL will be "http //" followed by the Windows Networking name of your server, followed by the path of the file you want to view. (Note the forward slash marks.) For example, if your Web server is registered with the WINS server as "Admin1" and you want to view the file Homepage htm in the root of the home directory, in the **Address** box you would type

http://admin1/homepage.htm

then press the enter key The home page should appear on the screen.

CHAPTER 2

Understanding the Internet and Intranet Services

Prior to planning and implementing your Web site, you should understand each of the components required to establish a Web site on a computer running Windows NT Server

This chapter answers the following questions.

- What is the Internet?
- What is an intranet?
- What is Internet Explorer?
- What is Internet Information Server?

What is the Internet?

The Internet is a global network of computers that communicate using a common language. It is similar to the international telephone system — no one owns or controls the whole thing, but it is connected in a way that makes it work like one big network

The World Wide Web (WWW or simply the Web) gives you a graphical, easy-to-navigate interface for looking at documents on the Internet These documents, as well as the links between them, comprise a "web" of information

Files, or *pages*, on the Web are interconnected You connect to other pages by clicking special text or graphics, which are called *hyperlinks*

Pages can contain text, images, movies, sounds —just about anything. These pages can be located on computers anywhere in the world When you are connected to the Web, you have equal access to information worldwide

Hyperlinks are words or graphics that have Web addresses embedded in them. By clicking a

hyperlink, you jump to a particular page in a particular Web site. You can easily identify a hyperlink. Hyperlink text is usually a different color from the rest of the text on a Web page, and hyperlink graphics often have a colored border.

Each Web page, including a Web site's home page, has a unique address called a Uniform Resource Locator (URL), for example, http://www.microsoft.com/home.htm. The URL specifies the name of the computer on which the page is stored and the exact path to the page.

What is an Intranet?

In this book, *intranet* refers to any TCP/IP network that is not connected to the Internet but uses Internet communication standards and tools to provide information to users on the private network. For example, a company can set up Web servers that are accessible only by employees to publish company newsletters, sales figures, and other corporate documents. Employees access information by using Web browsers.

Web servers can be configured to provide an intranet with the same features and services found on the Internet, such as serving hypertext pages (which can contain text, hyperlinks, images, and sounds), responding to Web client requests for information, and accessing a database. In this guide, these publishing services are described as "Internet services" whether they are running on an intranet or on the Internet.

What is Internet Explorer?

Microsoft Internet Explorer is a Web browser. Just as Microsoft® Word is a tool to create and format documents, or Microsoft® Excel is a tool to create spreadsheets and perform calculations, Internet Explorer is a tool to navigate and access, or "browse," information on the Web

The Internet Explorer toolbar provides a range of detailed functions and commands for managing the browser. The address bar below the toolbar displays the address of the current Web page To go to a new Web page, you type the page's URL directly into the white space on this bar and then press ENTER on your keyboard You can also go to a new page by clicking a hyperlink that jumps to the new page

The Microsoft Windows NT® operating system includes Internet Explorer for Windows NT. Internet Explorer is also available for Windows® for Workgroups, Windows version 3 1, and Windows 95

What is Internet Information Server?

Microsoft® Internet Information Server is a Web server that enables you to publish

information on a corporate intranet or on the Internet. Internet Information Server transmits information by using the Hypertext Transfer Protocol (HTTP). Internet Information Server can also be configured to provide File Transfer Protocol (FTP) and gopher services. The FTP service enables users to transfer files to and from your Web site. The gopher service uses a menu-driven protocol for locating documents. The gopher protocol has been largely superseded by the HTTP protocol.

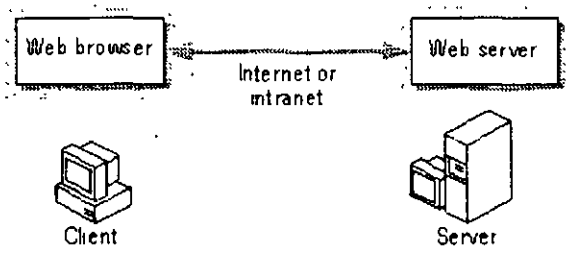
What Can I Do with Internet Information Server?

The creative possibilities of what you can offer on an Internet Information Server Web site are endless. Some familiar uses are to:

- Publish a *home page* on the Internet for your business featuring a newsletter, sales information, or employment opportunities.
- Publish a catalog and take orders from customers.
- Publish interactive programs
- Provide your remote sales force easy access to your sales database.
- Use an order-tracking database.

How Does Internet Information Server Work?

The Web is fundamentally a system of requests and responses. Web browsers request information by sending a URL to a Web server. The Web server responds by returning a Hypertext Markup Language (HTML) page



The HTML page can be a static page that has already been formatted and stored in the Web site, a page that the server dynamically creates in response to information provided by the user, or a page that lists the available files and folders on the Web site

Web Browser URL Request

Every page on an intranet or on the Internet has a unique URL that identifies it. Web browsers request a page by sending a URL to a Web server. The server uses the information in the URL to locate and display the page

URL syntax is a specific sequence of protocol, domain name, and path to the requested information. The protocol is the communication method used to gain access to information;

for example, Hypertext Transport Protocol (HTTP). Internet Information Server supports the HTTP, FTP, and gopher protocols. The domain name is the Domain Name System (DNS) name of the computer that contains the information. The path is the path to the requested information on the computer. The following table shows examples of different URLs:

Protocol	Domain Name	Path to Information
http://	www.microsoft.com	/backoffice
https:// (secure HTTP)	www.company.com	/catalog/orders.htm
gopher://	gopher.college.edu	/research/astronomy/index.htm
ftp://	orion.bureau.gov	/stars/alpha quadrant/starlist.txt

A URL can also contain information that the Web server must process before returning a page. The data is added to the end of the path. The Web server passes the data to a program or a script for processing and returns the results in a Web page. Example request types are listed in the following table:

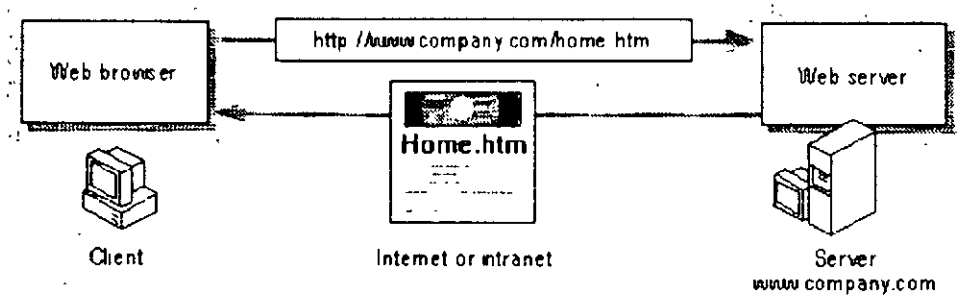
Request Type	URL
Static HTML page	http://www.microsoft.com/backoffice/home.htm
ISAPI application	http://www.msn.com/custom/page1.dll?CUST=on
Internet Database Connector	http://www.microsoft.com/feedback/input.idc
Common Gateway Interface (CGI) script	http://www.company.com/calculator/add.pl?2.2

Web Server Response

A Web server responds to a Web browser request by returning an HTML page. The returned page can be one of three types. a static HTML page, a dynamic HTML page, or a directory-listing page

Static Pages

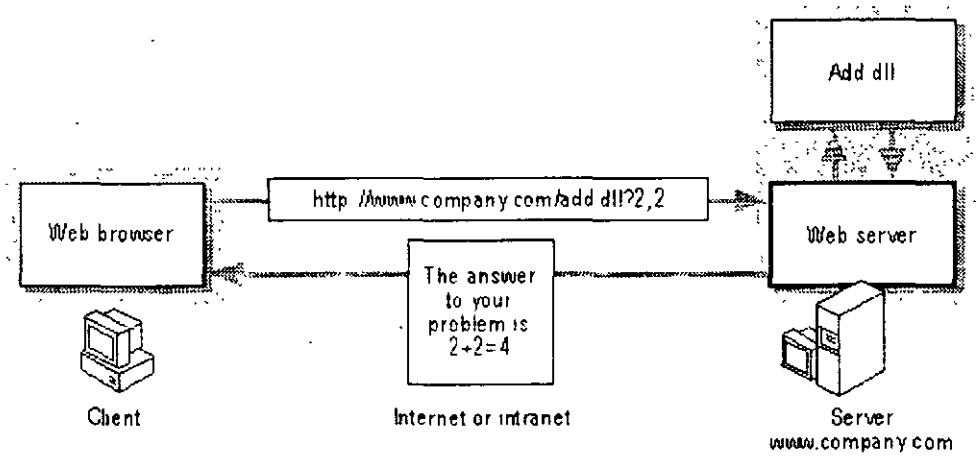
Static pages are static HTML pages that are prepared in advance of the request. The Web server returns the HTML pages to the user, but takes no special action. The user requests a static page by typing in an URL (in the following illustration, http //www company com/home.htm) or by clicking a link pointing to an URL. The URL request is sent to the server The server responds by returning the static HTML page.



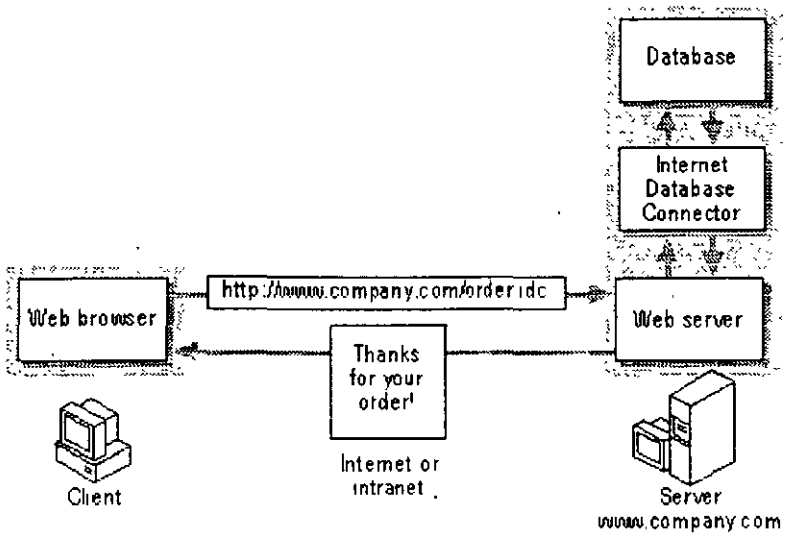
Dynamic Pages

Dynamic pages are created in response to a user's request. A Web browser collects information by presenting a page with text boxes, menus, and check boxes that the user fills in or selects. When the user clicks a button on a form, the data from the form is sent to the Web server. The server either passes the data to a script or application to be processed, or it queries or posts data to a database. The server returns the results to the user in an HTML page.

The following illustration shows how a user can send a query to an Internet Server API (ISAPI) application that adds two numbers. The user types the two numbers to be added, then clicks a button, which in turn sends the two numbers to the Web server The Web server calls the ISAPI application to add the numbers, then returns the results to the user in an HTML page



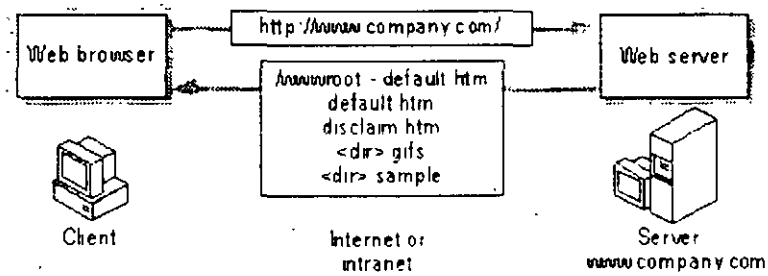
The following illustration shows a user posting an order to a database using the Internet Database Connector The user completes a form, then clicks a button, which in turn sends the data in the form to the server The server posts the data to a database, then confirms the order by sending an HTML page



For information about using scripts, applications, or database queries to create dynamic HTML pages, see Chapter 8, "Publishing Information and Applications."

Directory Listing

If users might send queries without specifying a particular file, you can either create a default document for a Web site or for a particular directory, or you can configure your server for directory browsing. If no default document is created for a directory and directory browsing is configured, a directory listing (a hypertext version of a Windows Explorer or File Manager listing) is returned to the user in the form of an HTML page. The user can then jump to the appropriate file by clicking it in the directory listing



Rather than using directory listings, you can provide a default document. For more information on default documents, see Chapter 6, "Planning Your Content Directories and Virtual Servers."

How Do I Use Internet Information Server?

Internet Information Server is flexible enough to perform many important functions for your organization. It is scalable from supporting a single-server site to supporting large multi-server installations. For example, www.microsoft.com and www.msn.com are among the busiest

Web sites on the Internet today, and both use multiple servers running Microsoft Internet Information Server.

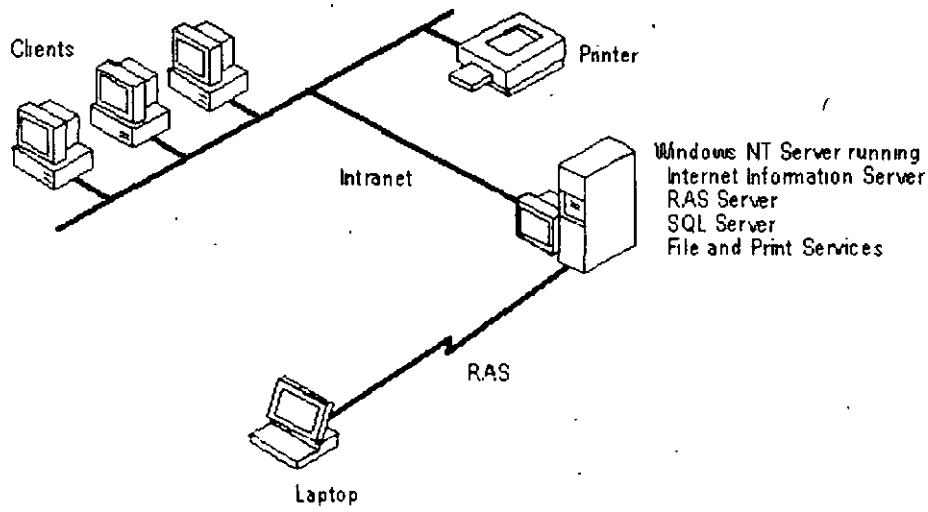
One of the primary factors that determines the configuration and use of Internet Information Server is whether it will be used internally by employees on your intranet, or if it will be connected to the Internet.

The following scenarios are intended to help you understand the range of possibilities for using Internet Information Server.

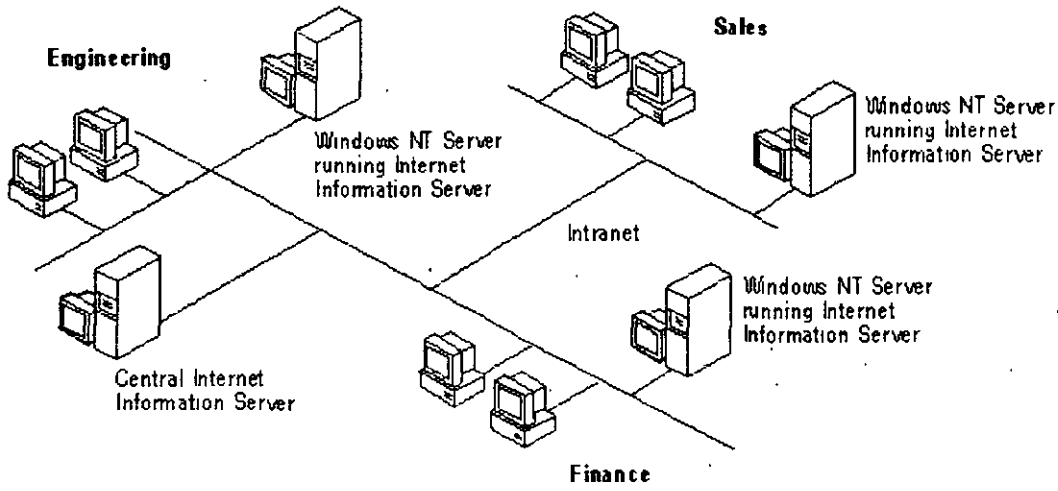
Intranet Scenarios

Internet Information Server integrates well into almost any existing environment. Because Internet Information Server integrates Windows NT security and networking, you can often add the software to an existing computer and use existing user accounts. It is not necessary to use a dedicated computer to run Internet Information Server.

For example, in a small workgroup you can add Internet Information Server to an existing file and print server. The workgroup's Web server can host personal Web-style pages, customized workgroup applications, serve as an interface to the workgroup's Structured Query Language (SQL) database, or use Remote Access Service (RAS) to provide dial-up access to the workgroup's resources from remote sites.

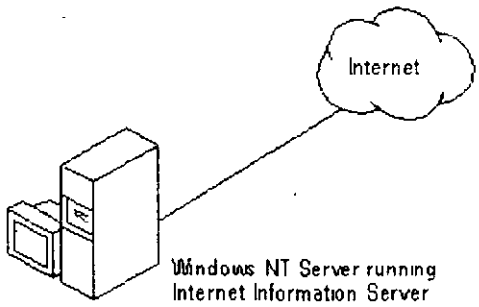


In a larger business with multiple departments or workgroups, each department might run Internet Information Server on an existing file server for workgroup-specific information A central information server might be used for company-wide information, such as an employee manual or company directory

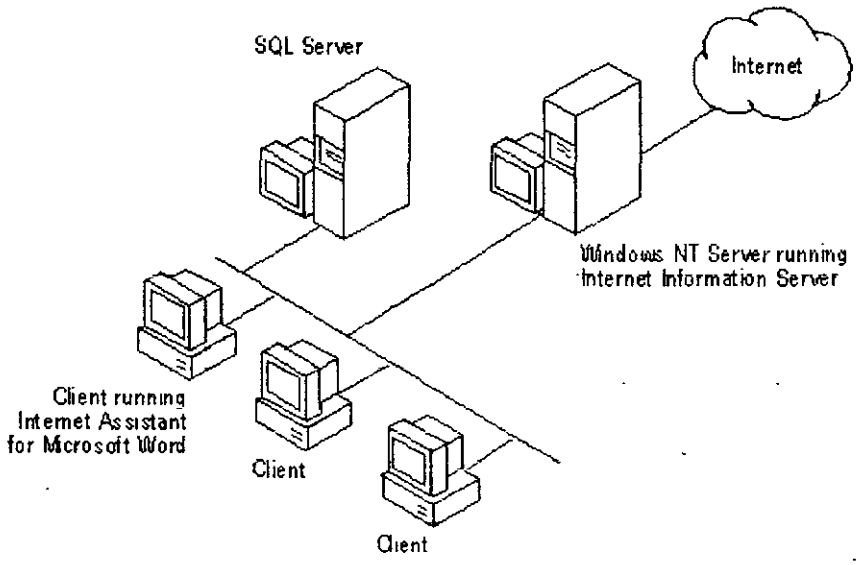


Internet Scenarios

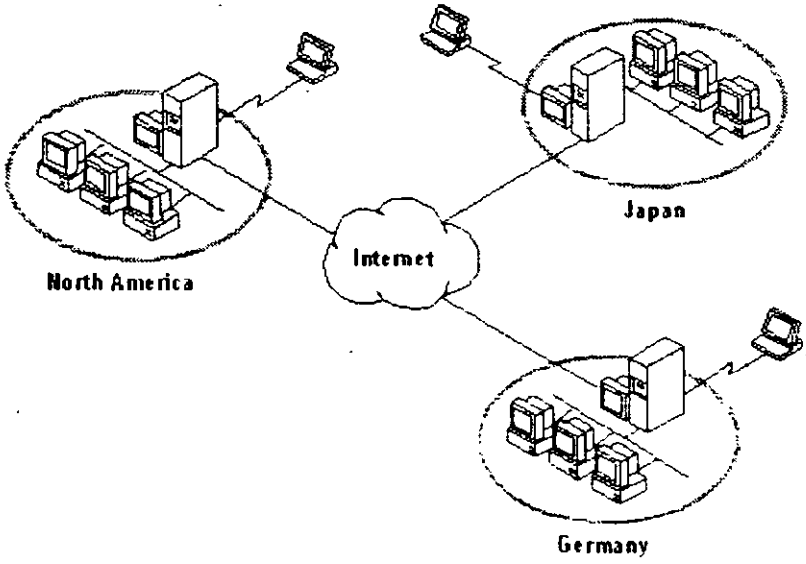
Internet Information Server can function as a simple dedicated Web server on the Internet, as shown in the following illustration.



In larger sites you can provide access from your internal network to the Internet Information Server, allowing employees to browse the server or to use authoring tools, such as Microsoft FrontPage™, to create content for your server



Internet Information Server's integration with all of the Windows NT services can also create servers with multiple functions. For example, a company with sites in different parts of the world can use Internet Information Server to provide communication between sites, with the added flexiblity of Internet access. You can even add RAS to an Internet Information Server to provide dial-up access to your intranet or the Internet.



Note Many scenarios for connecting to the Internet involve third-party routers or security devices that filter network packets between your computer and the Internet Routers and other security devices are not indicated in the preceding illustrations

CHAPTER 3

Configuring and Managing Internet Information Server

Internet Information Server provides a graphical administration tool called Internet Service Manager that you can use to monitor, configure, and control the Internet services.

Internet Service Manager is the central location from which you can control all of the computers running Internet Information Server in your organization. You can run Internet Service Manager on any computer that is running Windows NT Workstation or Windows NT Server and that is connected through the network to your Web server. With remote administration you can administer your Web servers from the server computer itself, from a management workstation on the corporate local area network (LAN), or even over the Internet

Internet Service Manager uses the Windows NT security model, so only validated administrators are allowed to administer services, and administrator passwords are transmitted in encrypted form over the network.

In addition to Internet Service Manager, Internet Information Server provides an HTML-based Internet Service Manager that you can run from any Web browser. You can perform the same administration tasks by using either version of Internet Service Manager. In this guide, any reference to *Internet Service Manager* refers to both versions of the tool unless otherwise noted

This chapter tells you how to:

- Use Internet Service Manager to view and configure the WWW, FTP, and gopher services
- Start, stop, and pause services
- Sort the services view
- Use Internet Service Manager property sheets to configure the Internet services

- Limit network use by constraining the network bandwidth allowed for the Internet services.
- Use other Windows NT tools to configure Internet Information Server.

Microsoft Internet Service Manager

Internet Service Manager helps you configure and monitor all the Internet services running on the Windows NT–based computers in your network.

Connecting to a Web Server

You can administer any Internet Information Server on your network by connecting to it in Internet Service Manager. You can specify a Web server by typing the computer's Domain Name System (DNS) host name, its Internet Protocol (IP) address, or its NetBIOS name (or computer name)

You can also find all the computers on your network that are running Internet Information Server.

To connect to a Web server

1. From the **Properties** menu in Internet Service Manager, select **Connect to Server**
2. In the **Server Name** box, type the Web server's host name, IP address, or NetBIOS name.

To connect by selecting a Web server from a list

1. From the **Properties** menu in Internet Service Manager, select **Find All Servers**.
2. From the list of servers displayed, double-click the one you want to connect to

Selecting a View

Internet Service Manager displays a graphical view of the services running on your servers You can view a complete report, or you can sort information by the service type or by computer name. Views enable you to tell at a glance which services are running. You can also display or hide services and sort services by their state (running, paused, or stopped).

To select a view

- From the **View** menu, choose **Servers View**, **Services View**, or **Report View**. Views are described in the following sections

To sort information in a view

- From the **View** menu, choose **Sort by Server**, **Sort by Service**, **Sort by Comment**, or **Sort by State**. For example, you should sort by state to quickly see which services are currently running.

To display or hide services

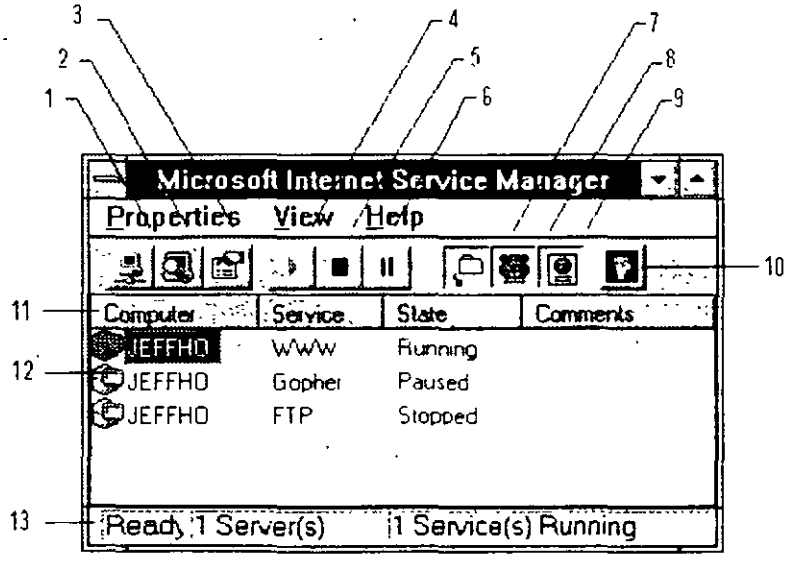
- From the **View** menu, choose the service that you want to display or hide (FTP, gopher, or WWW).

Report View

Report view is the default view Report view alphabetically lists the selected computers, with each installed service shown on a separate line. Click the column headings to sort the entire list alphabetically. Report view is probably most useful for sites with only one or two computers running Internet Information Server

Note If you are running other Internet services, such as Network News Transfer Protocol (NNTP) and Simple Mail Transfer Protocol (SMTP), they will be listed in the Report view of Internet Server Manager, along with the WWW, FTP, and gopher services.

The following illustration lists the functions of the buttons and icons in Internet Service Manager; you can also use the **Properties** and **View** drop-down menus for the same functions.



Connect to servers and view property sheets

1 Connects to one specific Web server

2 Finds all Web servers on the network

3 Displays property sheets to configure the selected service

Start, stop, or pause a service

4 Starts the selected service.

5 Stops the selected service.

6 Pauses the selected service.

Select which services should be displayed

7 Displays the FTP service in the Internet Service Manager main window.

8 Displays the gopher service in the Internet Service Manager main window.

9 Displays the WWW service in the Internet Service Manager main window.

Start Key Manager to create a Security Sockets Layer key

10 Displays the Key Manager window.

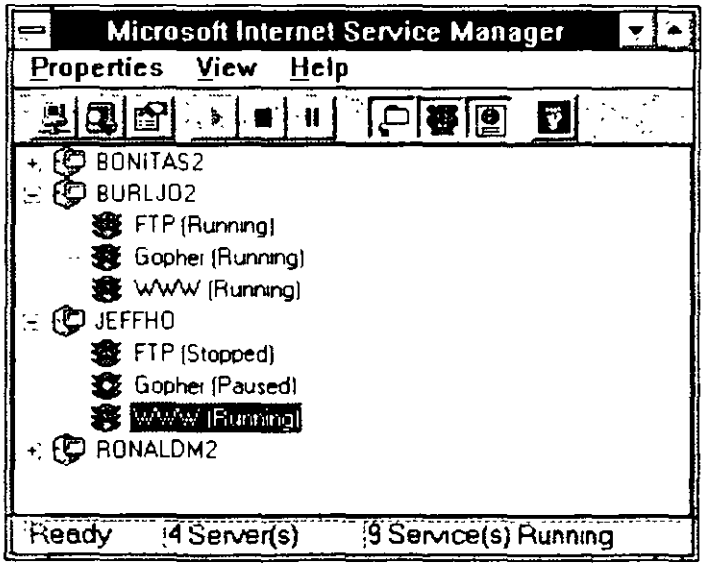
Make any necessary adjustments to services

11 Sorts the listings when you click a column heading.

12 Displays the property sheets for a service when you double-click it.

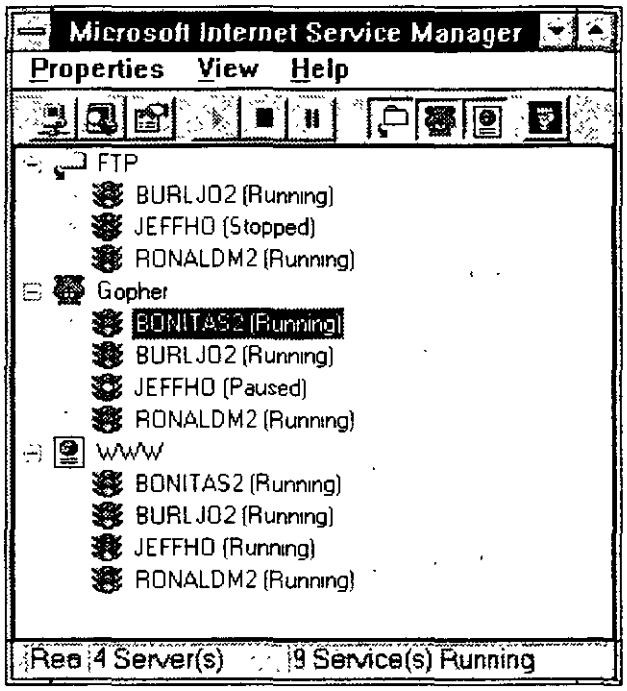
13 Displays server and service status

Servers View



Servers view displays services running on network computers by computer name. Click the plus symbol next to a computer name to see which services that computer is running. Double-click a service name to see its property sheets. Servers view is most useful for sites running multiple Web servers when you need to know the status of the services installed on a specific computer.

Services View



Services view lists the services on every selected computer, grouped by service name Click the plus symbol next to a service name to see the computers running that service Double-click the computer name under a service to see the property sheets for the service running on that computer Services view is most useful for sites with widely distributed Web servers when you need to know which computers are running a particular service

Starting, Stopping, and Pausing Services

You can quickly start, stop, or pause a service from Internet Service Manager

To start, stop, or pause a service

1. In Internet Service Manager, select the service you want to start, stop, or pause
2. From the **Properties** menu, choose **Start Service**, **Stop Service**, or **Pause Service**

Configuring and Managing Services

You can configure and manage the WWW, FTP, and gopher services by using Internet

Service Manager. The following information focuses on the WWW service, the most commonly used service.

In Internet Service Manager, double-click a computer name or a service name to display its property sheets. Click the tab at the top of each property sheet to display the properties for that category. After setting the properties for the service, click **OK** to return to the main Internet Service Manager window. Detailed information about each property sheet is included in later chapters on security, directories, and logging.

Note In special circumstances, you may need to use Registry Editor (Regedt32.exe) to configure Internet Information Server or Windows NT Server. See Chapter 10, "Configuring Registry Entries," for information on registry entries and when you need to use them.

The Service Property Sheet

You use the **Service** property sheet to control what kind of authentication is required to gain access to your Web site and to specify the account used for anonymous client requests to log on to the server Most Internet sites allow anonymous logons. See Chapter 5, "Securing Your Site Against Intruders," for more information.

The Directories Property Sheet

You use the **Directories** property sheet to specify which directories (folders) are available to users and to create a Web site composed of folders that reside on different computers You can also designate a default document that appears if a remote user does not specify a particular file, or instead enable directory browsing Directory browsing means that the user is presented with a hypertext listing of the directories and files so that the user can navigate through your directory structure For more detailed information, see Chapter 6, "Planning Your Content Directories."

The Logging Property Sheet

You use the **Logging** property sheet to log service activity. Logging provides valuable information about how a Web server is used You can send log data to text files or to an Open Database Connectivity (ODBC)–supported database If you have multiple Web servers or services on a network, you can log all their activity to a single database on any network computer

By using the **Logging** property sheet, you can also select the format you want for logging, either Standard format or National Center for Supercomputing (NCSA) Common Log File format

See Chapter 7, "Logging Server Activity," for more information

The Advanced Property Sheet

You use the **Advanced** property sheet to prevent certain individuals or groups from gaining

access to your Web site. You control access by specifying the IP address of the computers to be granted or denied access. For more information, see Chapter 5, "Securing Your Site Against Intruders."

You can also set the maximum network bandwidth for outbound traffic, to control (throttle) the maximum amount of traffic on your site. For more information, see the following section.

Limiting Network Use

You can constrain your Internet services by limiting the network bandwidth allowed for all of the Internet services on your Web server

Limiting the bandwidth dedicated to users of Microsoft Internet Information Server is especially useful if your Internet line has multiple purposes. Limiting bandwidth allows other operations (such as e-mail and remote logons) to use the same line without being slowed down by too much activity on the Web server.

To change bandwidth

1. In Internet Service Manager, double-click any service on the computer for which you want to change the bandwidth usage allowed.
2. Click the **Advanced** tab.
3. Select **Limit Network Use by all Internet Services on this computer**.
4. Select the number of kilobytes per second you want to allow for Internet services
5. Click **Apply** and then click **OK**

If the bandwidth being used remains below the level you set, client requests for information are answered. If the bandwidth is close to the value you set, client requests are delayed until the network traffic decreases Delaying responses enables the Web server to smooth out network traffic volumes without actually denying browser requests If the bandwidth exceeds the level you set, client requests to read files are rejected and requests to transfer files are delayed until the bandwidth equals or falls below the set value.

Using a Browser to Administer Internet Information Server

The HTML Internet Service Manager program performs the same administrative functions as Internet Service Manager You can use HTML Internet Service Manager with your Web browser to administer Internet Information Server over the Internet. To use HTML Internet Service Manager, use your Web browser to open http *//computername*/iisadmin. To administer any of the services, you must be logged on to a user account that has Administrator privileges on the computer being administered. If you are using a browser that is capable of

Windows NT Challenge/Response authentication (such as Microsoft Internet Explorer version 2.0 or later), you can use Windows NT Challenge/Response authentication. If you are not using a browser capable of Windows NT Challenge/Response authentication, then you must use Basic authentication (although this is not recommended).

Important When remotely administering a Web server through a browser, there are three actions you should guard against.

- If your browser supports only Basic authentication, do not turn off Basic authentication while you are administering Internet Information Server.
- If you stop a service, you will be disconnected and will not be able to restart it using the HTML Internet Service Manager
- If you delete the Iisadmin virtual directory on the server you are administering, you will be unable to use the HTML Internet Service Manager on that computer.

Using Other Windows NT Tools

In addition to Internet Service Manager, you can use other Windows NT utilities to configure, control, and monitor the Internet services. You might use the Windows NT utilities instead of Internet Service Manager for some tasks if you are already familiar with the standard Windows NT tools. This section explains how you can use Windows NT utilities to monitor or configure Internet Information Server.

Configuring Server Options with Control Panel

Use Control Panel to set Windows NT systems and options.

The Network Application

The Network application in Control Panel configures your Transmission Control Protocol/Internet Protocol (TCP/IP) settings, including IP address, subnet mask, and default gateway. Double-click **TCP/IP Protocol** in the **Installed Network Software** listing to display the **TCP/IP Configuration** dialog box.

Click the **DNS** tab to configure DNS settings, such as hostname, domain names, and DNS servers, to resolve names.

The Services Application

The Services application is used to start, stop, and pause the WWW, gopher, and FTP services. You can also use Internet Service Manager to start, stop, and pause the services.

Use the **Startup** button to specify whether the service starts automatically when your server restarts. If you have a specific reason, you can also use this dialog box to override the account used by the WWW service as set in the **Service** property sheet of Internet Service Manager. You should change this setting only if it is part of your security strategy; otherwise, use the default settings in the **Log On As** box.

The ODBC Application

The ODBC application in Control Panel is used to set up ODBC connectivity See Chapter 8, "Publishing Information and Applications," for more information about using the ODBC application.

Setting File Access with Windows Explorer

Use Windows Explorer to set directory and file permissions on Windows NT File System (NTFS) drives. Use the **Permissions** item in the **Security** dialog box to set permissions Setting directory and file permissions is an important part of securing your Web site For more information, see Chapter 5, "Securing Your Site Against Intruders."

File access control is not available on file allocation table (FAT) file systems. You can convert your file system to NTFS with the Convert.exe utility See the Windows NT documentation for more information.

Managing User Accounts with User Manager for Domains

User Manager for Domains, in the **Administrative Tools** submenu of the **Start** menu, is a tool that you can use to manage security for a Windows NT Server computer. With User Manager for Domains you can

- Create and manage user accounts.
- Create and manage groups
- Manage the security policies
- Manage servers individually or as members of a domain

Tracking Problems with Event Viewer

Event Viewer, in the **Administrative Tools** submenu of the **Start** menu, is a tool that you can use to monitor events in your system You can use Event Viewer to view and manage System, Security, and Application event logs Event Viewer can notify administrators of critical events by displaying pop-up messages, or by adding event information to log files. The information allows you to better understand the sequence and types of events that led up to a particular state or situation.

Monitoring Services with Performance Monitor

You can monitor a Web site to analyze the site's use and improve its performance. Windows NT includes a utility called Performance Monitor that measures the performance of Windows NT objects, such as processes, memory, and cache. Each object has an associated set of counters that provide information about the object. With Performance Monitor, you can create charts that provide a snapshot of a service's activity. You can also create logs of the service's performance, prepare reports that provide performance measurements, and generate alerts when a service counter meets a threshold. For more information on using Performance Monitor, see the Windows NT Help system.

Internet Information Server automatically installs Windows NT Performance Monitor counters for the WWW, FTP, and gopher services, as well as Internet Information Services Global. You can use these counters with the Windows NT Performance Monitor for real-time measurement of your Internet service use. A list of these counters and their descriptions follows. Except where noted otherwise, each counter is available to monitor any of the three services. (For example, you can monitor Connection Attempts for WWW, FTP, or gopher; but you can monitor Current CGI Requests for the WWW service only.

Note The WWW service appears in the Windows NT Performance Monitor as the HTTP Service.

Counter	Description
Aborted Connections	Total number of connections disconnected due to error or over-the-limit requests made to gopher service
Bytes Received/sec	Rate at which data bytes are received by service
Bytes Sent/sec	Rate at which data bytes are sent by service
Bytes Total/sec	Rate of total bytes transferred by service (sum of bytes sent and received)
CGI Requests	The total number of Common Gateway Interface (CGI) requests executed since WWW service startup; CGI requests invoke custom gateway executables, which the administrator can install to add forms processing or other dynamic data sources
Connection Attempts	Number of connection attempts made to service
Connections/sec	Rate at which HTTP requests are currently being handled
Connections in Error	Total number of connections (since service startup) that resulted in errors when processed by gopher service
Current Anonymous Users	Number of anonymous users currently connected to service
Current CGI Requests	Current number of CGI requests simultaneously being processed by WWW service (includes WAIS index queries)
Current Connections	Current number of connections to the service (sum of anonymous and non-anonymous users)
Current ISAPI Extension Requests	Current ISAPI extension requests simultaneously being processed by WWW service
Current NonAnonymous Users	Number of non-anonymous users currently connected to a specific (WWW, FTP, or gopher) service
Files Received	Total files received by (uploaded to) service since service startup (WWW or FTP only)
Files Sent	Total files sent by (downloaded from) service since service startup
Files Total	Total files transferred by server since service startup (WWW or FTP only)
Get Requests	Total number of HTTP GET requests received by WWW service; GET requests are generally used for basic file retrievals or image maps, though they can be used with forms
Gopher Plus Requests	The total number of Gopher Plus requests received by gopher service since service startup
Head Requests	Total number of HTTP HEAD requests received by WWW service. HEAD requests typically indicate that a client is querying the state of a document they already have to see if it needs to be refreshed
ISAPI Extension Requests	Total number of HTTP ISAPI extension requests received by WWW service; ISAPI Extension Requests are custom gateway dynamic-link libraries (DLLs), which the administrator can install to add forms processing or other dynamic data sources
Logon Attempts	Number of logon attempts made by service since service startup
Maximum Anonymous Users	Largest number of anonymous users simultaneously connected to service since service startup
Maximum CGI Requests	Largest number of CGI requests simultaneously processed by the WWW service since service startup
Maximum Connections	Largest number of users simultaneously connected to service since service startup
Maximum ISAPI	Largest number of ISAPI extension requests simultaneously

Extension Requests	processed by WWW service since service startup
Maximum NonAnonymous Users	Largest number of non-anonymous users simultaneously connected to service since service startup
Not Found Errors	Number of requests that could not be satisfied by service because requested document could not be found; typically reported as HTTP 404 error code to client
Other Request Methods	Number of HTTP requests that are not GET, POST, or HEAD methods; may include PUT, DELETE, LINK, or other methods supported by gateway applications
Post Requests	Number of HTTP requests using POST method; generally used for forms or gateway requests
Total Anonymous Users	Total number of anonymous users that have ever connected to service since service startup
Total NonAnonymous Users	Total number of non-anonymous users that have connected to service since service startup

Select **Internet Information Services Global** in the **Object** list box in the Windows NT Performance Monitor **Add to Chart** dialog box to monitor general-use and cache-use information about Internet Information Server. Counters for this object are:

Counter	Description
Cache Flushes	Total number of times since service startup that cache has been flushed
Cache Hits	Total number of times since service startup a file-open, directory-listing, or service-specific object's request was found in the IIS cache
Cache Hits %	Ratio of cache hits to all cache requests
Cache Misses	Total number of times since service startup a file-open, directory-listing, or service-specific object's request was not found in the cache
Cache Size	Configured maximum size of the shared HTTP, FTP, and gopher memory cache
Cache Used	Current number of bytes containing cached data in shared memory cache (includes directory listings, file handle tracking, and service-specific objects)
Cached File Handles	Current number of open file handles cached by all Internet Information Server services
Current Blocked Async I/O Requests	Current number of asynchronous I/O requests blocked by bandwidth throttling
Directory Listings	Current number of cached directory listings cached by all Internet Information Server services
Measured Async I/O Bandwidth usage	Measured bandwidth in bytes of asynchronous I/O averaged over one minute
Objects	Current number of objects cached by all of Internet Information Server services (includes file-handle tracking objects, directory-listing objects, and service-specific objects)
Total Allowed Async I/O Requests	Total asynchronous I/O requests allowed by bandwidth throttling since service startup
Total Blocked Async I/O Requests	Total asynchronous I/O requests blocked by bandwidth throttling since service startup
Total Rejected Async I/O Requests	Total asynchronous I/O requests rejected by bandwidth throttling since service startup

Contents | Index | ◁ | △ | ▷

CHAPTER 4

Networking for the Internet or an Intranet

The Internet is a network of networks. An intranet is a smaller, contained network, such as that found within a corporation

This chapter explains:

- Routers and security devices
- Typical network configurations.
- Administering servers by using Internet Service Manager.
- Using the discovery mechanism to find other computers on your network.
- Microsoft Internet publishing requirements
- Issues involved in publishing on a private intranet
- Internet Explorer for network users
- Using Simple Network Management Protocol (SNMP) monitoring

General Networking Issues

This section explains the basic Transport Control Protocol/Internet Protocol (TCP/IP) networking requirements for nearly all Web sites, especially those with multiple Web servers For issues specific to the Internet or to intranet publishing, see those sections later in this chapter

Routers and Security Devices

TCP/IP is a routeable protocol, meaning that each piece of information (packet) has a specific

address that it is routed to. Dedicated routers connect two networks and route packets between them. The routers check the destination for each packet on one network, and if the destination is on the router's other network, it routes the packet to its destination.

Routers can be configured to allow only certain packets between networks, a process called *packet filtering*. Packet filtering can be used to prevent users from seeing or connecting to internal computers and resources.

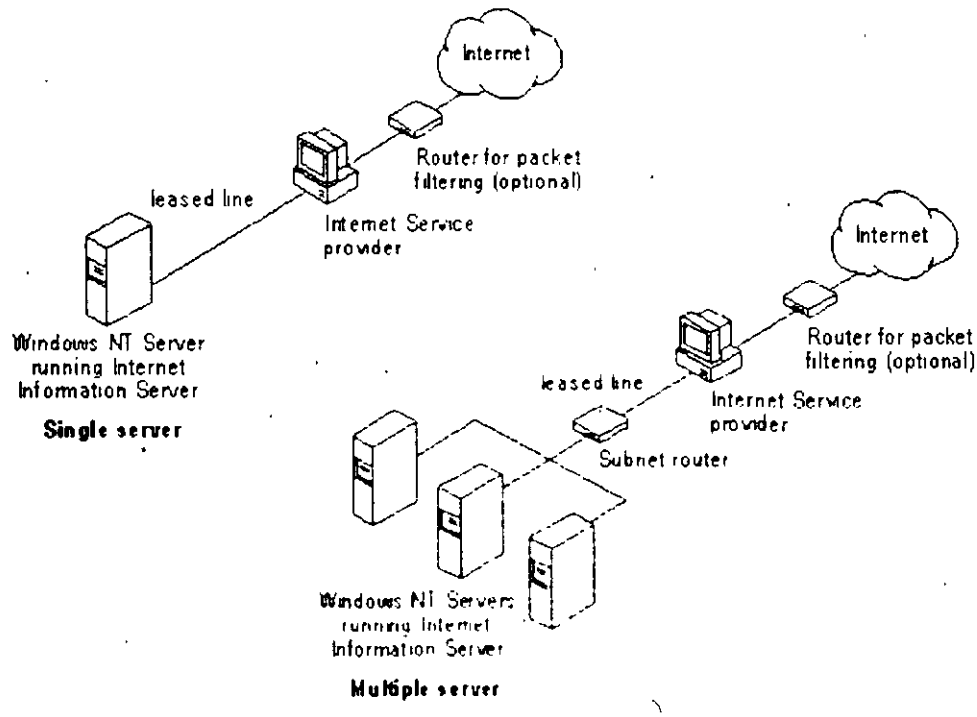
If you have a TCP/IP network you probably have routers in your network already. Often an Internet Service Provider (ISP) will install a router between the Internet and your Web server. You can often use this router to filter the incoming and outgoing packets. See your ISP or router documentation for more information about configuring routers or similar security devices.

Typical Network Configurations

This section describes typical network configurations for an intranet site or an Internet site.

Intranet Sites

If you are publishing only to your own intranet, Internet Information Server can be integrated into any TCP/IP network. If Dynamic Host Configuration Protocol (DHCP) and Windows Internet Name Service (WINS) are enabled on your network, clients can use the Web server's computer name to connect with the server. If Domain Name System (DNS) is enabled on your network, you will use host names

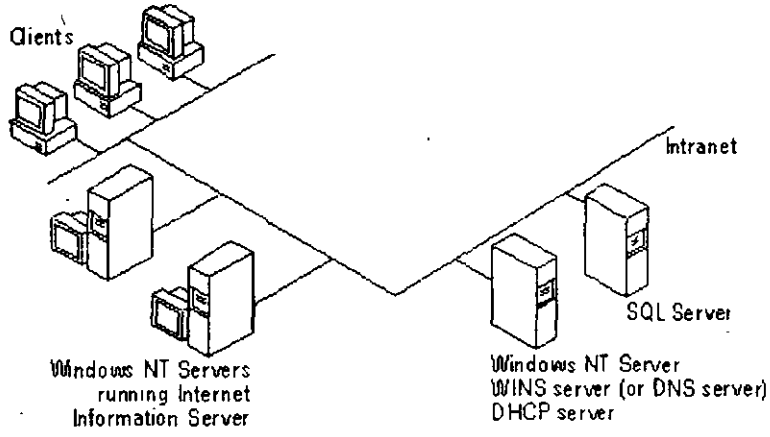


Internet Sites

If you will have only one computer running Internet Information Server at your site, your Internet Service Provider (ISP) can help you with many details, such as router configuration and the IP address of the default gateway that your Web server will use.

If you have multiple computers running Internet Information Server on your network, you must configure their TCP/IP settings to operate correctly through your Internet connection configuration, including any routers used between your servers and the default gateway.

Typically, sites with more than one computer running Internet Information Server will add another router. With the addition of another router, the servers can be grouped into a single subnet isolated from your private network, as shown in the following diagram.



To create a subnet you will need:

- One computer with two network adapter cards and Windows NT TCP/IP routing enabled, or a dedicated router for your subnet.

  See Help in Windows NT for the procedure to create a simple router on a computer running Windows NT and for the procedure to set routing tables by using the **route** command

- Valid IP addresses for every network adapter card in your subnet and the correct subnet mask

- Correct default gateway IP address configurations

  Your ISP will provide you with the Internet IP addresses, subnet mask (if any), and your default gateway configuration

Integrating Your Intranet with the Internet

You can just connect your entire intranet to the Internet, rather than connecting a subnet containing only your IIS servers to the Internet However, there are many security

implications to connecting an intranet to the Internet. You should thoroughly understand the security implications and understand TCP/IP networking before you decide to integrate your entire network with the Internet. Integrating a network with the Internet requires information that is outside the scope of this manual See Chapter 5, "Securing Your Site Against Intruders," for more information about security, and consult the Internet or other sources for additional information about Internet security, firewalls, and TCP/IP networking.

Administering Servers with Internet Service Manager

You can install Internet Service Manager on Windows NT–based computers from which you will administer computers running Internet Information Server on your network. Internet Service Manager can be installed on computers running Windows NT Workstation or Windows NT Server.

For over-the-network installation, use File Manager or Windows NT Explorer to create a network share containing the Admin folder on the compact disc. You can then install Internet Service Manager to administer the services from any computer on the network running version 4 0 or later of Windows NT Workstation or Windows NT Server ¤. You can also administer Internet servers over the network by using your Web browser. For more information, see Chapter 3, "Configuring and Managing Internet Information Server."

Finding Other Computers on Your Network or Subnet

Microsoft Internet Service Manager has a discovery mechanism that finds computers running Microsoft Internet services on your network You can choose **Find All Servers** in the **Properties** menu to discover the Microsoft Internet Information Server computers on your network.

If WINS servers are used on your network, the discovery process used by Microsoft Internet Server is automatic.When Microsoft Internet Information Server starts, it automatically registers its available services with your WINS servers Thus, when Internet Service Manager queries the network for computers running Microsoft Internet services, the WINS servers return the registered services Internet Service Manager then displays the returned services

Notes You will only be able to administer sites for which you are a registered administrator

This feature is not available in the HTML version of Internet Service Manager.

If WINS servers are not available, discovery uses TCP/IP broadcasts to perform the same functions Discovery will not work if you do not have WINS servers, or if the servers reside across routers and cannot be discovered by using broadcasts

Publishing on the Internet

For the world to reach your site, you must have an Internet connection. Connections to the Internet are usually leased from ISPs. In addition to providing your physical Internet connection and IP address (and subnet mask if appropriate), your ISP can provide many of the Internet services, such as domain name registration, routers, and DNS service.

How to Choose the Right Internet Connection

Your connection to the Internet will be through a network adapter card or other network device, such as a modem or Integrated Services Digital Network (ISDN) card. Internet bandwidth is measured in bits per second (bps)

Your server configuration and Internet bandwidth determine how fast data gets to your computer and how many requests can be serviced simultaneously. As the number of computers getting data through your Internet connection increases, delays or failures will occur unless you have enough bandwidth.

When you lease an Internet connection a network cable is installed by your ISP to your site. Leased connection speeds in the United States range from 56,000 bps (with Frame Relay) to 45,000,000 bps (with a T3 connection). A dial-up ISDN line can offer speeds up to 128,000 bps

Internet Connection Types

The connection types described in the following table represent typical levels of service for full Internet connections in North America and Japan. The Internet services offered through Internet service providers in other countries may differ significantly You may observe further differences, depending on the nature of your hardware, the content you make available from your site, and other variables.

Connection Types

Connection	Maximum BPS	Simultaneous Users Supported
Frame Relay	56,000	10–20
ISDN	128,000	10–50
T1	1,500,000	100–500
Fractional T1	varies as needed	
T3	45,000,000	5000+

A light-duty server can use Frame Relay or ISDN. A server with medium traffic might have a T1 line or some fraction of a T1 line installed Large businesses that expect heavy Internet traffic may need fractional or multiple T1 lines or even T3 service in order to handle thousands of users

Modem connections to the Internet are available, but are typically used for individual client browsing, and are not recommended for servers A connection to the Internet using a phone line and modem can service only two or three simultaneous users. (Modem connections might

be used for text-only Internet servers with only a small number of potential users) Modem connections are often called "slow links" because data is transmitted at the speed of the modem, typically from 9,600 to 28,800 bps, far too slow for efficient operation of an Internet server

IP Addresses and DNS

The Internet is a world-wide collection of individual Transmission Control Protocol/Internet Protocol (TCP/IP) networks. Each computer on the Internet has a unique address (IP address). Information is transmitted on the Internet in data packets. Each packet is addressed to a specific computer's IP address, such as 10.212.57.189.

Because IP addresses are difficult to use and remember, the Domain Name System (DNS) was created to pair a specific IP address, such as 10.189.54.1, with a friendly domain name, such as microsoft.com. When a user browses the Internet by using a domain name, the browser first must contact a DNS server to resolve the domain name to an IP address, then contact the computer with that address.

This has two implications for your Internet Information Server

- You must have a permanent IP address assigned to a server on the Internet
- You must register a domain name in the DNS for your permanent IP address.

Your ISP will generally provide your IP addresses and may also register your domain names Contact the Internet Network Information Center (InterNIC) or your ISP for more information about DNS registration

Other Internet Client Services

Your ISP must provide you with a connection, one or more IP addresses (and subnet mask, if appropriate), and usually the IP address of at least one DNS server Internet service providers often offer additional client services You will need additional software to use these services.

Mail services are used to exchange electronic mail The Simple Mail Transfer Protocol (SMTP) is used for Internet mail

News services give you access to a Network News Transfer Protocol (NNTP) server Using a news reader, you can read messages posted in the thousands of available news groups Usenet is one of the more popular public news services

Publishing on an Intranet

Microsoft Internet Information Server can also be used on any private TCP/IP network to

provide files and applications to network users. This section explains how to plan for publishing on a private intranet. Issues to be considered include:

- Name resolution systems
- Using DHCP
- Using computer names in URLs
- SNMP monitoring (if used at your site)

Name Resolution Systems

If you want intranet clients to be able to use friendly names with Internet Explorer when browsing Web servers, you must provide a name resolution system for clients.

Windows NT Server offers you the advantage of automatic IP address administration with the DHCP server and WINS server methods for name resolution offered by WINS servers

Using Computer Names with WINS Servers

A WINS server is a Windows NT Server–based computer running Microsoft TCP/IP and WINS server software. A WINS server maintains a database that maps TCP/IP addresses to Windows Networking NetBIOS computer names.

Microsoft Internet Information Server uses WINS server software to map TCP/IP addresses to computer names on the network. WINS uses Microsoft Networking computer names, which makes it much more flexible than DNS for name resolution WINS also provides a dramatic reduction of IP broadcast traffic in internetworks, while allowing client computers to easily locate remote systems across local or wide area networks. If you use WINS servers on the Internet, your computers must be using valid Internet IP addresses.

Using Computer Names and LMHOSTS

An LMHOSTS file is a simple text file resolving Windows computer names to IP addresses. If you have a small or infrequently changing network you can distribute an LMHOSTS file to each computer in the network Each time a host changes you will have to manually change the LMHOSTS files.

Using Domain Names with DNS Servers

You can maintain a DNS server and Internet-assigned TCP/IP domain names as used on the Internet. If you plan to connect your network to the Internet, your IP addresses and DNS server routing configuration must be valid for the Internet

Using Domain Names and HOSTS

A HOSTS file is a simple text file resolving DNS domain names to IP addresses. If you have a small or infrequently changing network, you can distribute a HOSTS file to each computer. Each time a host changes you will have to manually change the HOSTS files.

Using DHCP in Your Intranet

You can take advantage of DHCP server automatic IP address administration.

A DHCP server is a Windows NT Server–based computer running Microsoft TCP/IP and the DHCP server software.

If you use DHCP servers, you must use WINS servers for clients to have automatic IP address name resolution in a Wide Area Network (WAN) environment. DHCP is defined in Requests for Comments (RFCs) 1533, 1534, 1541, and 1542. See Tcpip.hlp in Windows NT Server for more information about DHCP servers

Refer to Windows NT Server documentation for more information.

Using URLs and Creating HTML Links for Intranets

When you connect to a server or create HTML files and links on an intranet, you must name computers in accordance with the name resolution system implemented on your network. For example, if you use WINS servers on your network, your links will use Windows computer names, such as http://sales1/homepage.htm, where sales1 is the name of the computer running Internet Information Server

---

SNMP Monitoring

If you monitor your network by using Simple Network Management Protocol (SNMP), you can use the SNMP Management Information Bases (MIBs) provided by Microsoft Internet Information Server to monitor your Web server.

The MIB files included in the Sdk folder of the Microsoft Internet Information Server compact disc can be used by third-party SNMP monitors to enable SNMP monitoring of the WWW, gopher, and FTP services of Microsoft Internet Information Server

Internet Information Server supports SNMP monitoring only SNMP configuration is not supported

You will need to compile the MIB files using the MIB compiler that comes with your SNMP software before using them with the Windows NT SNMP service. You must start the services to be monitored before configuring and starting the SNMP service on your Internet Information Server–based computer Once the SNMP service has been started on both the remote and local computers, you can use SNMP tools to monitor the running services.

CHAPTER 5

Securing Your Site Against Intruders

Whether your Web server is handling millions of accesses directly over the Internet or maintaining departmental documents on your intranet, security is an important consideration. When you connect computers to an intranet or an Internet, you can communicate with people and computers worldwide. This broad flexibility imposes a degree of risk — not only can you communicate with people on other networks, users on other networks can initiate communication with your network. Although connecting to Web servers is generally done with good intentions, there are malicious individuals who attempt to infiltrate internal networks.

The Windows NT operating system was designed to help you secure your system against intruders. Internet Information Server builds on the Windows NT security model and provides additional monitoring and security features This chapter will help you effectively use Windows NT security and Internet Information Server security at your site. You should understand all of the information in this chapter before connecting your computer to a public network. If you do not understand the information, you should consult Windows NT documentation, an authorized Microsoft Solution Provider, or other qualified source before installing your site on the Internet.

This chapter explains

- How Internet Information Server security works.
- Controlling anonymous access to your Web site.
- Controlling access by user name or group name.
- Requiring a user name and password for authenticated access

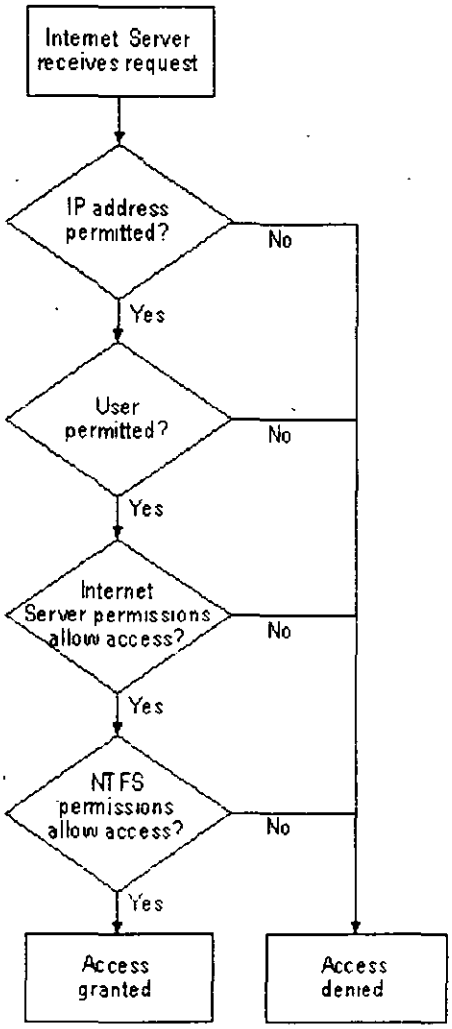
- Controlling access by setting folder and file permissions.
- Securing data transmissions with SSL.

How Internet Information Server Security Works

Internet Information Server is built on the Windows NT security model. Windows NT security helps you protect your computer and its resources by requiring assigned user accounts and passwords. You can control access to computer resources by limiting the user rights of these accounts. You can use the Windows NT File System (NTFS) to assign permissions to folders and files on your computer. You can control access to folders and files by preventing users from copying files to or from a folder, or by preventing users from executing files in certain folders.

In addition to the Windows NT security features, you can set Read-only or Execute-only virtual directories by using Internet Service Manager. Internet Information Server also provides a way to deny user access to computers with particular IP addresses. IIS supports the Secure Sockets Layer (SSL) protocol, which securely encrypts data transmissions between clients and servers.

When an IIS Web server receives a browser request for information, it determines whether the request is valid. A simple overview of the security process used on each request is presented in the following illustration



The following sections explain how to configure Windows NT and the Internet services to protect your system.

Controlling Anonymous Access

On many Web servers, almost all WWW, FTP, and gopher access is anonymous, that is, the client request does not contain a user name and password This occurs in the following cases.

- An FTP client logs on with the user name "anonymous."
- All gopher requests
- A Web browser request does not contain a user name and password in the HTTP header (this is the default on new Web connections with most browsers).

Even though the user is not logged on with an individual user name and password, you can

still control and monitor anonymous access. Each Internet service maintains a Windows NT user name and password that is used to process anonymous requests. When an anonymous request is received, the service "impersonates" the user configured as the "anonymous logon" user. The request succeeds if the anonymous logon user has permission to access the requested resource, as determined by the resource's Access Control List (ACL). If the anonymous logon user does not have permission, the request fails. You can configure the WWW service to respond to a failed anonymous request by requiring the user to provide a valid Windows NT user name and password, a process called authentication.

Configuring the Anonymous User Account

You can view and monitor the anonymous logon user account on the **Service** property sheets of Internet Service Manager (for the WWW, FTP, and gopher services). Each service running on the same computer can use either the same or different anonymous logon user accounts Including the anonymous logon user account in file or folder ACLs enables you to precisely control the resources available to anonymous clients.

The anonymous logon user account must be a valid Windows NT user account on the server providing the Web services, and the password must match the password for this user in that computer's user database. User accounts and passwords are configured in the Windows NT User Manager by setting **User Rights** in the **Policies** menu The anonymous logon user account must have the **Log on Locally** user right.

The IUSR_*computername* account is automatically created (with a randomly generated password) during Internet Information Server setup For example, if the computer name is marketing1, then the anonymous access account name is IUSR_marketing1.

By default, all Web client requests use this account. In other words, Web clients are logged on to the computer by using the IUSR_*computername* account The IUSR_*computername* account is permitted only to log on locally on the server providing the Web services.

Note The IUSR_*computername* account is also added to the group Guests. If you have changed the settings for the Guests group, those changes also apply to the IUSR_*computername* account You should review the settings for the Guests group to ensure that they are appropriate for the IUSR_*computername* account

For the WWW and FTP services, you can allow or prevent anonymous access (all gopher requests are anonymous) For each of the Web services (WWW, FTP, and gopher), you can change the user account used for anonymous requests and change the password for that account

To allow anonymous access

1. In Internet Service Manager, double-click the WWW service or the FTP service to display its property sheets, then click the **Service** tab.

2. For the WWW service, select the **Allow Anonymous** check box. For the FTP service, select the **Allow Anonymous Connections** check box.

3. Click **OK**.

To change the account or password used for anonymous access

1. In Internet Service Manager, double-click the service to display its property sheets, then click the **Service** tab.

2. In the **Anonymous Logon** user name box, type the new user name.

   The default user account is IUSR_*computername*, where *computername* is the name of your server. This account is created automatically when you set up Internet Information Server.

3. In the **Password** box, type the new password.

   A randomly generated password is automatically created for the IUSR_*computername* account.

   Note If you change the password for this account, you must also specify the new password for the account in User Manager.

4. Click **OK**

Using the Anonymous Account on Domain Controllers

When Internet Information Server is installed on a primary or secondary domain controller, the anonymous logon user account is created in the user account database of the domain When Internet Information Server is installed on a domain member-server, or a stand-alone server, the account is created on the local computer

If Internet Information Server is installed on multiple domain controllers of the same domain, a separate user account is created in the domain user database for each Internet server computer. This does not cause any conflicts because each user name is unique, containing the name of the associated computer However, you may find it more convenient to create a single anonymous logon user account in the domain to use for all Internet Information Server domain controllers in the domain This can simplify administration of ACLs. To do this, follow these steps

- In User Manager for Domains, create a new anonymous logon user account in the domain. Be sure that this account is made a member of appropriate groups, given a secure password, and is given the User Right (in the **Policies** menu) to log on locally.
- On the **Service** property sheet of Internet Service Manager, specify the new anonymous logon user name and password You must do this for each Internet Information Server

service running on all primary and secondary domain controllers in the domain.

- When later installing Internet Information Server on other domain controllers in the domain, be sure to use Internet Service Manager to modify the anonymous logon user name and password to match those created with User Manager for Domains Do this for each Internet Information Server service installed.

If you allow remote access only by the IUSR_*computername* account, remote users do not provide a user name and password, and have only the permissions assigned to that account. This prevents hackers from attempting to gain access to sensitive information with fraudulent or illegally obtained passwords. For some situations this provides the best security.

Controlling Access by User or Group

You can control access to your Web site by using the Windows NT User Manager to specify what certain users or groups of users are allowed to do on your server You can further control access by requiring Web client requests to provide a user name and password that Internet Information Server confirms before completing the request.

Setting Up User Accounts

Windows NT security helps you protect your computer and its resources by requiring assigned user accounts Every operation on a computer running Windows NT identifies who is doing the operation. For example, the user name and password that you use to log on to Windows NT identifies who you are and defines what you are authorized to do on that computer

What a user is authorized to do on a computer is configured in User Manager by setting user rights in the **Policies** menu User rights authorize a user to perform certain actions on the system, including the **Log on Locally** right, which is required for users to use Internet services if Basic authentication is being used.

If you are using Windows NT Challenge/Response Authentication, then the **Access this computer from network** right is required for users to use Internet services By default, everyone has this right

To increase security, follow these guidelines

- Do not give the IUSR_*computername* account, the Guests group, or the Everyone group any right other than the **Log on Locally** or **the Access the computer from this network** right
- Make sure that all user accounts on the system, especially those with administrative rights, have difficult-to-guess passwords In particular, select a good administrator

password.(a long, mixed-case, alphanumeric password is best) and set the appropriate account policies. Passwords can be set by using User Manager, or by typing at the system logon prompt.

- Make sure that you specify how quickly account passwords expire (which forces users to regularly change passwords), and set other policies such as how many bad logon attempts will be tolerated before locking a user out. Use these policies to prevent exhaustive or random password attacks, especially on accounts with administrative access. You can set these policies by using User Manager
- Limit the membership of the Administrator group to trusted individuals.
- If you use the predefined Windows NT user accounts INTERACTIVE and NETWORK for access control, make sure files in your Web site are accessible to these user accounts. In order for a file to be accessed by anonymous client requests or client requests using Basic authentication, the requested file must be accessible by the INTERACTIVE user. In order for a file to be accessible by a client request that uses Windows NT Challenge/Response authentication protocol, the file must be accessible by the NETWORK user.

Requiring a User Name and Password

You can restrict Web site access to only *authenticated* clients, that is, Web clients that supply a valid Windows NT user name and password When you use authentication, no access is permitted unless a valid user name and password are supplied. Password authentication is useful if you want only authorized individuals to access your Web site or specific portions controlled by NTFS. You can have both anonymous logon access and authenticated access enabled at the same time

The WWW service provides two forms of authentication: basic and Windows NT Challenge/Response (sometimes referred to as "NTLM")

Basic authentication does not encrypt transmissions between the client and server Because Basic authentication sends the client's Windows NT user name and password in essentially unencrypted over the networks, intruders could easily learn user names and passwords

Windows NT Challenge/Response authentication, currently supported only by Microsoft Internet Explorer version 2.0 or later, protects the password, providing for secure logon over the network In Windows NT Challenge/Response authentication, the user account obtained from the client is that with which the user is logged on to the client computer Because this account, including its Windows NT domain, must be a valid account on the Windows NT-based server running Internet Information Server, Windows NT Challenge/Response authentication is very useful in an intranet environment, where the client and server computers are in the same, or trusted, domains Because of the increased security, Microsoft recommends using the Windows NT Challenge/Response method of password authentication whenever possible

You have both Basic and Windows NT Challenge/Response authentication enabled by default. If the browser supports Windows NT Challenge/Response, it uses that authentication method. Otherwise, it uses Basic authentication. Windows NT Challenge/Response authentication is currently supported only by Internet Explorer 2 0 or later.

You can require client authentication for all FTP service requests or only for anonymous requests that fail. The FTP service supports only Basic authentication; therefore, your site is more secure if you allow anonymous connections. Your site is most secure if you allow only anonymous FTP connections.

To enable authentication for the WWW service

1. In Internet Service Manager, double-click the WWW service to display its property sheets, then click the **Service** tab.

2. Select **Basic (Clear Text)**, **Windows NT Challenge/Response**, or both.

3. Click **OK**.

To enable authentication for the FTP service

1. In Internet Service Manager, double-click the FTP service to display its property sheets, then click the **Service** tab.

2. To enable authentication for failed anonymous connections, clear (delete) the **Allow only anonymous connections** check box.

3. To require all client requests to be authenticated, clear the **Allow Anonymous Connections** check box.

Warning FTP and WWW Basic authentication send passwords across the network in clear text (that is, unencrypted), as does HTTP Basic authentication.

How Anonymous Logons and Client Authentication Interact

You can enable both anonymous connections and client authentication for the WWW service and for the FTP service This section explains how an IIS Web server responds to these access methods when both are enabled

Note that if client authentication is disallowed and anonymous connections are allowed, a client request that contains a user name and password is processed as an anonymous connection, and the server ignores the user name and password

WWW Service

When the WWW service receives a client request that contains credentials (a user name and password), the "anonymous logon" user account is not used in processing the request. Instead, the user name and password received by the client are used by the service. If the service is not granted permission to access the requested resource while using the specified user name and password, the request fails, and an error notification is returned to the client.

When an anonymous request fails because the "anonymous logon" user account does not have permission to access the desired resource, the response to the client indicates which authentication schemes the WWW service supports. If the response indicates to the client that the service is configured to support HTTP Basic authentication, most Web browsers will display a user name and password dialog box, and reissue the anonymous request as a request with credentials, including the user name and password entered by the user.

If a Web browser supports Windows NT Challenge/Response authentication protocol, and the WWW service is configured to support this protocol, an anonymous WWW request that fails due to inadequate permissions will result in automatic use of the Windows NT Challenge/Response authentication protocol. The browser will then send a user name and encrypted password from the client to the service. The client request is reprocessed, using the client's user information.

If the WWW service is configured to support both Basic and Windows NT Challenge/Response, the Web server returns both authentication methods in a header to the Web browser. The Web browser then chooses which authentication method to use. Because the Windows NT Challenge/Response protocol is listed first in the header, a browser that supports the Windows NT Challenge/Response protocol will use it A browser that does not support the Windows NT Challenge/Response protocol will use Basic authentication Currently, Windows NT Challenge/Response authentication is supported only by Internet Explorer 2.0 or later

FTP Service

When the FTP service receives a client request that contains credentials (a user name and password), the "anonymous logon" user account is not used in processing the request Instead, the user name and password received by the client are used by the service. If the service is not granted permission to access the requested resource while using the specified user name and password, the request fails, and an error notification is returned to the client.

When an anonymous request fails because the "anonymous logon" user account does not have permission to access the desired resource, the server responds with an error message Most Web browsers will display a user name and password dialog box, and reissue the anonymous request as a request with credentials, including the user name and password entered by the user

Warning Because the FTP service (and WWW Basic authentication) sends user names and passwords unencrypted over the network, intruders could use protocol analyzers to read the user names and passwords.

Creating Customized Authentication Schemes

If you need a WWW request authentication scheme not supported by the service directly, obtain a copy of the Win32 Software Development Kit (SDK), and read the ISAPI Filters specification on how to develop user-written ISAPI Filter dynamic-link libraries (DLLs) that handle request authentication. The Win32 SDK is available through the Microsoft Developer Network. For more information, visit the Microsoft home page (http://www.microsoft.com).

Setting Folder and File Permissions

Every access to a resource, such as a file, an HTML page, or an Internet Server API (ISAPI) application, is done by the services on behalf of a Windows NT user. The service uses that user's user name and password in the attempt to read or execute the resource for the client. You can control access to files and folders in two ways:

- By setting access permissions in the Windows NT File System (NTFS)
- By setting access permissions in the Internet Service Manager

Note File Allocation Table (FAT) file system partitions do not support access control. However, an FAT partition may be converted to NTFS by using the **convert** utility. Refer to Windows NT documentation for more information on using this utility.

Setting NTFS Permissions

You should place your data files on an NTFS partition. NTFS provides security and access control for your data files. You can limit access to portions of your file system for specific users and services by using NTFS. In particular, it is a good idea to apply Access Control Lists (ACLs) to your data files for any Internet publishing service.

ACLs grant or deny access to the associated file or folder by specific Windows NT user accounts, or groups of users. When an Internet service attempts to read or execute a file on behalf of a client request, the user account offered by the service must have permission, as determined by the ACL associated with the file, to read or execute the file, as appropriate. If the user account does not have permission to access the file, the request fails, and a response is returned, informing the client that access has been denied.

File and folder ACLs are configured by using the Windows NT Explorer. The NTFS file system gives you very fine control on files by specifying users and groups that are permitted

access and what type of access they may have for specific files and directories. For example, some users may have Read-only access, while others may have Read, Change, and Write access. You should ensure that the IUSR_*computername* or authenticated accounts are granted or denied appropriate access to specific resources.

You should note that the group "Everyone" contains all users and groups, including the IUSR_*computername* account and the Guests group. By default the group Everyone has full control of all files created on an NTFS drive.

If there are conflicts between your NTFS settings and Microsoft Internet Information Server settings, the strictest settings will be used.

You should review the security settings for all folders in your Web site and adjust them appropriately. Generally you should use the settings in the following table:

Directory Type	Suggested NTFS Access
content	Read access
programs	Read and Execute access
databases	Read and Write access

To secure your files on an NTFS drive

1. Put your files on your NTFS drive and add them to your Web site by using the **Directories** property sheet in Internet Service Manager.

2. In Windows NT Explorer, right-click the folder (directory) you want to secure (select your site root to secure the entire site), and choose **Properties**

3. In the **Properties** dialog box, choose the **Security** tab.

4. In the **Security** dialog box, choose **Permissions**

5. In the **Directory Permissions** dialog box, click **Add** to add users and groups.

6. In the **Add Users and Groups** dialog box, add the users that should have access

7. Click **OK**.

8. In the **Directory Permissions** dialog box, select the users and groups that should have permissions.

9. From the **Type of Access** list box, choose the permission level you want for the selected user or group

10. Click **OK**

Auditing File Access

To determine whether anyone has gained unauthorized access to sensitive files, you can audit the access of NTFS files and folders. For example, you can check for attempts by members of a specific user group to read files. You should review the audit records periodically to check for unauthorized access. To set auditing on a file or folder, use User Manager for Domains to enable auditing of File and Object Access, and then use Windows NT Explorer to specify which files to audit and which types of file access events to audit. To review audit entries, use Event Viewer.

For more information on setting the audit policy for files and folders, see the Windows NT documentation.

▵Setting WWW Directory Access

When creating a Web publishing directory (folder) in Internet Service Manager, you can set access permissions for the defined home directory or virtual directory, and all of the folders in it These permissions are those provided by the WWW service and are in addition to any provided by the NTFS file system. The permissions are:

Read Read permission enables Web clients to read or download files stored in a home directory or a virtual directory. If a client sends a request for a file that is in a directory without Read permission, the Web server returns an error. Generally, you should give directories containing information to publish (HTML files, for example) Read permission You should disable Read permission for directories containing Common Gateway Interface (CGI) applications and Internet Server Application Program Interface (ISAPI) DLLs to prevent clients from downloading the application files

Execute Execute permission enables a Web client to run programs and scripts stored in a home directory or a virtual directory. If a client sends a request to run a program or a script in a folder that does not have Execute permission, the Web server returns an error For security purposes, do not give content folders Execute permission.

A client request can invoke a CGI application or an Internet Server Application Program Interface (ISAPI) application in one of two ways.

- The file name of the CGI executable or the ISAPI DLL can be specified in the request (URL) An example URL would be

  http://inetsrvr.microsoft com/scripts/httpodbc dll/scripts/pubs.idc?lname=Smith

  For this request to be valid, the file Httpodbc dll must be stored somewhere in the Web "publishing tree" (the directory structure that contains your content files, in this example, in the Scripts folder), and the folder it is stored in must have the Execute permission selected This way the administrator can permit applications (CGI or ISAPI) to be run from a small number of carefully monitored directories

- The other way to configure CGI and ISAPI applications is to use the Web File Extension Mapping feature, which allows your executables and DLLs to be stored somewhere other than the Web publishing tree. An example URL would be:

  http://inetsrvr.microsoft.com/scripts/pubs.idc?lname=Smith

In this example, the script file (Pubs.idc) is stored in a folder of the Web publishing tree that has the Execute permission enabled. The service, upon receiving the request, will use the file-name extension mappings to determine where to find the application, which can be stored anywhere. This technique prevents users from invoking CGI and ISAPI applications directly by adding parameters in the URL. This is therefore a more secure mechanism, and useful for all Web applications and scripts. See "Associating Interpreters with Applications (Script Mapping)" in Chapter 10, "Configuring Registry Entries," for more information.

To set access permissions for a directory

1. In Internet Service Manager, double-click the WWW service to display its property sheets, then click the **Directories** tab
2. Select the folder for which you want to set permissions.
3. Click **Edit Properties**.
4. To allow Web clients to read and download the contents of a folder, select the **Read** check box.
5. To allow Web clients to run programs and scripts in a folder, select the **Execute** check box.
6. Click **OK**, then click **OK** again

Note We recommend you set either Execute access or Read access on a folder, but not both Executable scripts and programs should be kept in a virtual root separate from static Web content.

Controlling Access by IP Address

Microsoft Internet Information Server can be configured to grant or deny access to specific IP addresses. For example, you can exclude a harassing individual by denying access to your server from a particular IP address, or prevent entire networks from accessing your server Conversely, you can choose to allow only specific sites to have access to your service IP address security is probably most useful on the Internet to exclude everyone except known users.

The source IP address of every packet received is checked against the Internet Information Server settings in the **Advanced** property sheet. If Internet Information Server is configured to allow access by all computers except those listed as exceptions to that rule, access is denied to any computer with an IP address included in that list. Conversely, if Internet Information Server is configured to deny all IP addresses, access is denied to all remote users except those whose IP addresses have been specifically granted access.

To deny access to a specific computer or group of computers

1. In the **Advanced** property sheet of Internet Service Manager, choose the **Granted Access** button.

2. Click **Add**.

3. In the **IP Address** box, type the IP address of the computer to be denied access to your site or click the button next to the **IP Address** box to use a DNS name, such as www.company.com.

   To deny access to a group of computers, select **Group of Computers**. In the **IP Address** and **Subnet Mask** boxes, type the IP address and the subnet mask for a group to be denied access.

4. Click **OK**.

   Access will be granted to all computers except the ones in the window with an Access status of Denied

5. In the **Advanced** property sheet, click **OK**

To grant access to only a specific computer or group of computers

1. In the **Advanced** property sheet of the Internet Service Manager, choose the **Denied Access** button

   This step denies access to all computers except those you specifically grant access to

2. Click **Add**

3. In the **IP Address** box, type the IP address of the computer to be granted access, or click the button next to the **IP Address** box to use a DNS name, such as www.company com.

   To grant access to a specific group of computers, select **Group of Computers** In the **IP Address** and **Subnet Mask** boxes, type the IP address and the subnet mask for the group to be granted access

4. Click **OK**

Access will be denied to all computers except those in the window with an Access status of Granted.

5. In the **Advanced** property sheet, click **OK**.

Running Other Network Services

You should review all of the network services that you are using on any computer connected to the Internet.

Run Only the Services that You Need

The fewer services you are running on your system, the less likely a mistake will be made in administration that could be exploited Use the Services application in Control Panel to disable any services not absolutely necessary on your Internet server.

Unbind Unnecessary Services from Your Internet Adapter Cards

Use the Bindings feature in the Network application in Control Panel to unbind any unnecessary services from any network adapter cards connected to the Internet. For example, you might use the Server service to copy new images and documents from computers in your internal network, but you might not want remote users to have direct access to the Server service from the Internet

If you need to use the Server service on your private network, disable the Server service binding to any network adapter cards connected to the Internet. You can use the Windows NT Server service over the Internet, however, you should fully understand the security implications and comply with Windows NT Server Licensing requirements issues.

When you are using the Windows NT Server service you are using Microsoft networking (the server message block [SMB] protocol rather than the HTTP protocol) and all Windows NT Server Licensing requirements still apply HTTP connections do not apply to Windows NT Server licensing requirements

Check Permissions on Network Shares

If you *are* running the Server service on your Internet adapter cards, be sure to double-check the permissions set on the shares you have created on the system You should also double-check the permissions set on the files contained in the shares' folders to ensure that you have set them correctly

Do Not Enable Directory Browsing

Unless it is part of your strategy, you should not enable directory browsing on the **Directories** property sheet. Directory browsing potentially exposes the entire Web publishing file structure; if it is not configured correctly, you run the risk of exposing program files or other files to unauthorized access. If a default page (Default.htm) is not present and directory browsing is enabled, the WWW service will return a Web page containing a listing of files in the specified directory. It is always advisable to have a Default.htm page in any directory that you do not want to be browsed.

▵ Securing Data Transmissions with Secure Sockets Layer (SSL)

Previous sections of this chapter have dealt with securing your server from unauthorized access. This section discusses protocols that use cryptography to secure data transmissions to and from your server .

Microsoft Internet Information Server offers a protocol for providing data security layered between its service protocols (HTTP) and TCP/IP. This security protocol, called Secure Sockets Layer (SSL), provides data encryption, server authentication, and message integrity for a TCP/IP connection.

SSL is a protocol submitted to the W3C working group on security for consideration as a standard security approach for Web browsers and servers on the Internet. SSL provides a security "handshake" that is used to initiate the TCP/IP connection. This handshake results in the client and server agreeing on the level of security that they will use and fulfills any authentication requirements for the connection Thereafter, SSL's only role is to encrypt and decrypt the byte stream of the application protocol being used (for example, HTTP). This means that all the information in both the HTTP request and the HTTP response are fully encrypted, including the URL the client is requesting, any submitted form contents (such as credit card numbers), any HTTP access authorization information (user names and passwords), and all the data returned from the server to the client

An SSL-enabled server can send and receive private communication across the Internet to SSL-enabled clients (browsers), such as Microsoft Internet Explorer version 2 0 or later

SSL-encrypted transmissions are slower than unencrypted transmissions. To avoid reducing performance for your entire site, consider using SSL only for virtual folders that deal with highly sensitive information such as a form submission containing credit card information.

Enabling SSL security on a Web server requires the following steps.

1. Generate a key pair file and a request file
2. Request a certificate from a certification authority

3. Install the certificate on your server.

4. Activate SSL security on a WWW service folder.

Important Keep in mind the following points when enabling SSL security:

- You can enable SSL security on the root of your Web site (\InetPub\Wwwroot by default) or on one or more virtual folders.
- Once enabled and properly configured, only SSL-enabled clients will be able to communicate with the SSL-enabled WWW folders.
- URLs that point to documents on a SSL-enabled WWW folder must use "https://" instead of "http://" in the URL. Any links using "http://" in the URL will not work on a secure folder.

Generating a Key Pair

As part of the process of enabling Secure Sockets Layer (SSL) security on your Web server, you need to generate a key pair and then acquire an SSL certificate. The new Key Manager application (installed with the product and located in the Internet Server program group) simplifies this procedure.

To generate a key pair

1. In the **Microsoft Internet Server** submenu, click **Key Manager**, or click the Key Manager icon on the Internet Service Manager toolbar.

2. From the **Key** menu, click **Create New Key**.

3. In the **Create New Key and Certificate Request** dialog box, fill in the requested information, as follows

Key Name

Assign a name to the key you are creating.

Password

Specify a password to encrypt the private key

Bits

By default, Key Manager generates a key pair 1024 bits long. To specify a key that is 512 or 768 bits long, make the proper selection in this box. The more bits you specify, the greater your security. In international versions, the size of each key you

create is 512 bits

Organization

Preferably International Organization for Standardization (ISO)-registered, top-level organization or company name.

Organizational Unit

Your department within your company, such as Marketing.

Common Name

The domain name of the server, for example, www. *mycompany*.com.

Country

Two-letter ISO Country designation, for example, US, FR, AU, UK, and so on.

State/Province

For example, Washington, Alberta, California, and so on.

Locality

The city where your company is located, such as Redmond or Toronto.

Request File

Type the name of the request file that will be created.

4. After filling out the form, click **OK**
5. When prompted, retype the password you typed in the form, and click **OK**.

   An icon appears as the key is being created When the key has been created, a screen appears giving you information about new keys and how to obtain a certificate.
6. After reading the **New Key Information** screen, click **OK**.
7. To save the new key, from the **Servers** menu choose **Commit Changes Now**.
8. When asked if you want to commit all changes now, click **OK**.

Your key will appear in the Key Manager window under the name of the computer for which you created the key By default, a key is generated on your local computer.

Note Do not use commas in any field Commas are interpreted as the end of that field and will generate an invalid request without warning.

Generating a Key Pair on Another Server

You can set up a key pair on another server and install the certificate there. From the **Servers** menu, click **Connect to Server**, and follow the previous procedure under "Generating a Key Pair."

Once you have generated a key pair, you must get a certificate and then install that certificate with the key pair. For information about getting a certificate, see "Acquiring a Certificate" and "Installing a Certificate with a Key Pair."

Acquiring a Certificate

The key generated by Key Manager is not valid for use on the Internet until you obtain a valid certificate for it from a Certificate Authority, such as VeriSign. Send the certificate request file to the Certificate Authority to obtain a valid certificate Until you do so, the key will exist on its host computer, but cannot be used For instructions on acquiring a VeriSign certificate refer to VeriSign's Web site at http.//www.verisign.com/microsoft/.

Installing a Certificate with a Key Pair

After you complete your certificate request, you will receive a signed certificate from the Certificate Authority (consult your Certificate Authority for complete details). The key manager program will create a file similar to the following example:

```
-----BEGIN CERTIFICATE-----

JIEBSDSCEXoCHQEwLQMJSoZILvoNVQECSQAwcSETMRkOAMUTBhMuVrM
mIoAnBdNVBAoTF1JTQSBEYXPhIFN1Y3VyaXR5LCBJbmMuMRwwGgYDVQ
QLExNQZXJzb25hIEN1cnRpZmljYXR1MSQwIgYDVQQDExtPcGVuIE1hc
mt1dCBUZXN0IFN1cnZ1c1AxMTAwHhcNOTUwNzE5MjAyNzMwWhcNOTYw
NTE0MjAyOTEwWjBzMQswCQYDVQQGEwJVUzEgMB4GA1UEChMXU1NBIER
hdGEgU2VjdXJpdHksIEluYy4xHDAaBgNVBAsTE1BlcnNvbmEgQ2VydG
1maWNhdGUxJDA1BgNVBAMTG09wZW4gTWFya2V0IFR1c3QgU2VydmVyI
DExMDBcMA0GCSqGSIb3DQEBAQUAA0sAMEgCQQDU/71rgR6vkVNX40BA
qlpoGdSmGkD11N3sEPfSTGxNJXY58XH3JoZ4nrF7mIfvpghN11taY1m
vhbBPNqYe4yLPAgMBAAEwDQYJKoZIhvcNAQECBQADQQBqyCpws9EaAj
KKAefuNP+z+8NY8khckgyHNCLLpfnV+1P6m+bF66HNDU1Fz8ZrVOu3W
QapgLPV90kIskNKXX3a

------END CERTIFICATE-----
```

To install a certificate

1. In the Internet Server program group, click **Key Manager**
2. In the **Key Manager** window, select the key pair that matches your signed certificate.

   If you had backed up the key pair file, you have to load it first For instructions, see "Loading a Key Pair File" earlier in this chapter

3. From the **Key** menu, choose **Install Key Certificate**.

4. Select the Certificate file from the list (Certif.txt, for example), and click **Open**.

5. When prompted, type the password that you used in creating the key pair.

   The key and certificate are combined and stored in the registry of the server.

6. From the **Servers** menu, choose **Commit Changes Now**.

7. When asked if you want to commit all changes now, click **OK**.

You can back up a key and certificate combination by following the procedure under "Backing Up Keys" earlier in this chapter.

Note If you do not specify an IP address while installing your certificate, the same certificate will be applied to all virtual servers created on the system. If you are hosting multiple sites on a single server, you can specify that the certificate be used only for a particular server IP address by adding the IP address, for example:

```
10.191.28.45
```

Configuring a Directory to Require SSL

Once you have applied the certificate, you must enable the SSL feature from Internet Service Manager. SSL can be required on any virtual folder available in your Web site and is configured on the **Directories** property sheet.

To require SSL

1. In Internet Service Manager, double-click the WWW service to display its property sheets, then click the **Directories** tab.

2. Select the folder that requires SSL security, then click **Edit Properties**.

3. Select the **Require secure SSL channel** option, and then click **OK**.

Moving a Key Pair to Another Server

After creating a key pair, you can use Key Manager to move the key pair to another server.

To move a key pair to another server

1. From the **Servers** menu, click **Connect to Server**, type the name of the server you want to move the key pair to, and click **OK**.

   The server name appears in the list of servers (the left column).

2. Select the key you want to move.

3. From the **Edit** menu, click **Cut**.

4. Select the server you want to move the key pair to

5. From the **Edit** menu, click **Paste**.

You can copy a key pair to another server with the same procedure by substituting the **Copy** command for **Cut**.

Backing Up Keys

With Key Manager you download key information from the registry into a file on your hard disk and then copy this file or move it to a floppy disk or tape for safekeeping You can back up a private key pair file or a key with an installed certificate.

To back up a key or a private key pair file

1. From the **Key** menu in Key Manager, choose **Export Key** and then **Backup File**

2. After reading the warning about downloading sensitive information to your hard disk, click **OK**.

3. Type the key name in the **File Name** box, and click **Save**.

   The file is given a req file-name extension and is saved to your hard disk drive You can then copy it or move it to a floppy disk or magnetic tape

Loading Backed Up Keys

You can load backed-up keys or private key pair files into Key Manager with the **Import** command.

To load a backed-up key

1. From the **Key** menu in Key Manager, choose **Import Key** and then **Backup File**.

2. Select the file name from the list, and click **Open**

Loading a Key Created with Keygen.exe and Setkey.exe

If you have generated a key pair from the command line with the Keygen exe command and installed a certificate with Setkey exe, you can load them into Key Manager with the Import command.

To load a key

1. From the **Key** menu in Key Manager, choose **Import Key** and then **KeySet**.

2. In the **Private Key Pair File** box, type the file name for the key pair or click **Browse** and select the file.

3. In the **Certificate File** box, type the file name for the certificate or click **Browse** and select the file.

4. Click **OK**.

5. Type the password for the private key in the **Private Key Password** box, and click **OK**.

Suggestions for SSL Configuration and Operation

Microsoft recommends that you use separate content directories for secure and public content (for example, C:\InetPub\Wwwroot\Secure-Content and C:\InetPub\Wwwroot\Public-Content).

Save your key file in a safe place in case you need it in the future. It is a good idea to store your key file on a floppy disk and remove it from the local system after completing all setup steps. Do not forget the password you assigned to the key file.

Contents | Index | ◁ | △ | ▷

CHAPTER 6

Planning Your Content Directories and Virtual Servers

On small Web sites, Web content files are usually contained under one directory tree Larger Web sites often store HTML content files, Web applications, and databases in multiple directories on the same computer or on several computers in the network. To make the contents of directories that reside on other computers appear in your computer's Web site, you create virtual directories.

With Internet Information Server, you can also create virtual servers, which enable a single server to appear as several servers You can associate each content directory with a specific virtual server.

This chapter explains how to.

- Set up a single content directory.
- Set up default documents and enable directory browsing
- Create virtual servers
- Set up home directories
- Create virtual directories

See Chapter 5, "Securing Your Site Against Intruders," for more information about security and about using the Windows NT File System (NTFS) with your directories

Configuring a Single Content Directory

If your Hypertext Markup Language (HTML) content files are contained under one directory

tree, all you need to do is copy them to the default World Wide Web (WWW) home directory (\InetPub\Wwwroot) or change the home directory to refer to the location containing your files. However, if your files reside in multiple directories, or even multiple computers on your network, you will need to create virtual directories to make those files available from your Web site.

▵Setting the Default Document and Directory Browsing

If a remote user sends a request without a specific file name (for example, http://www microsoft.com/), the WWW service will return the specified default document, if it exists in that directory. You can place a file with the specified default document file name in each directory

If no default document is available, the WWW service will return an error, unless directory browsing is enabled. If directory browsing is enabled, a directory listing containing links to the files and folders in that directory will appear.

A default document can be included in all WWW directories. In the **Directories** property sheet for the WWW service, change the **Default Document** entry to the default file name you will use on your system Often the default document is set to be an index file (Index.htm) for the contents of that directory (or of the entire Web site). The default file name used is Default.htm.

If the user does not specify a file for a particular directory, a hypertext file and directory listing will be returned.

Directory browsing on the WWW service is very similar to browsing in File Transfer Protocol (FTP). Directory browsing is useful if you have a lot of files that you want to share quickly without converting them to Hypertext Markup Language (HTML) format.

Note Virtual directories will not appear in directory listings (also called "directory browsing" for the WWW service). To access a virtual directory, users must know the virtual directory's alias, and type the URL in the browser For the WWW service, you can also create links in HTML pages. For the gopher service, you can create explicit links in tag files so that users can access virtual directories For the FTP service, you can list virtual directories by using directory annotations

---

▵Creating Virtual Servers

By convention each domain name, such as www.company com, represents an individual computer However, it is possible to use a single computer and make it appear to be not only

a primary server (for example, named www.company.com), but also servers for different departments of your company (for example, marketing.company.com, sales.company.com, and so on). You can create *virtual servers* for these departments with Microsoft Internet Information Server. You do not need a different computer for each domain name.

To do this, you must obtain Internet Protocol (IP) addresses from your Internet Service Provider (ISP) for the primary server and for each virtual server you want to create. For example, you assign the first IP address (10 212.56.184) in the Domain Name System (DNS) as www.company.com (your primary server), and assign C:\Wwwroot as its content home directory. You register the second IP address (10.212.56 185) in the DNS as marketing.company.com, and assign a different drive or directory as its content home directory. Thus, it appears to users on the Internet that there are two computers when in fact it is the same computer running one copy of the WWW service. If you create a home directory without specifying an IP address, that home directory will be used for all requests containing server IP addresses not specified in other home directories.

These multiple IP addresses can be assigned to multiple network adapter cards, or to a single card. You use the Network application in the Windows NT Control Panel to bind the additional IP addresses to your network adapter card.

After the IP address is assigned to the network adapter card, you must assign a home content directory to that IP address In the **Directories** property sheet, select the **Virtual Server** box and enter its IP address Virtual directories (directories that are not home directories) can also be restricted to one virtual server by assigning an IP address to them.

Setting Up a Virtual Server

You set up a virtual server by using the **Directories** property sheet in Internet Service Manager.

1. To display property sheets in Internet Service Manager, double-click the WWW Service or the computer name

2. Click the **Directories** tab

3. Click the **Add** button

4. In the **Directory** box of the **Directory Properties** dialog box, select a directory by clicking the **Browse** button

5. Click **Home Directory**

6. Select the **Virtual Server** check box

7. Type the IP address for the virtual server

This address, which is typically supplied by your Internet service provider, must be

configured by using the **Microsoft TCP/IP Properties** dialog box (found in the Network application in the Windows NT Control Panel; click the **Protocols** tab, select **TCP/IP Protocol**, and click the **Properties** button).

8. Click **OK**

Specifying Directories with Virtual Servers

If you have assigned more than one IP address to your server, when you create a virtual directory you must specify which IP address has access to that directory. If no IP address is specified, that directory will be visible to all virtual servers.

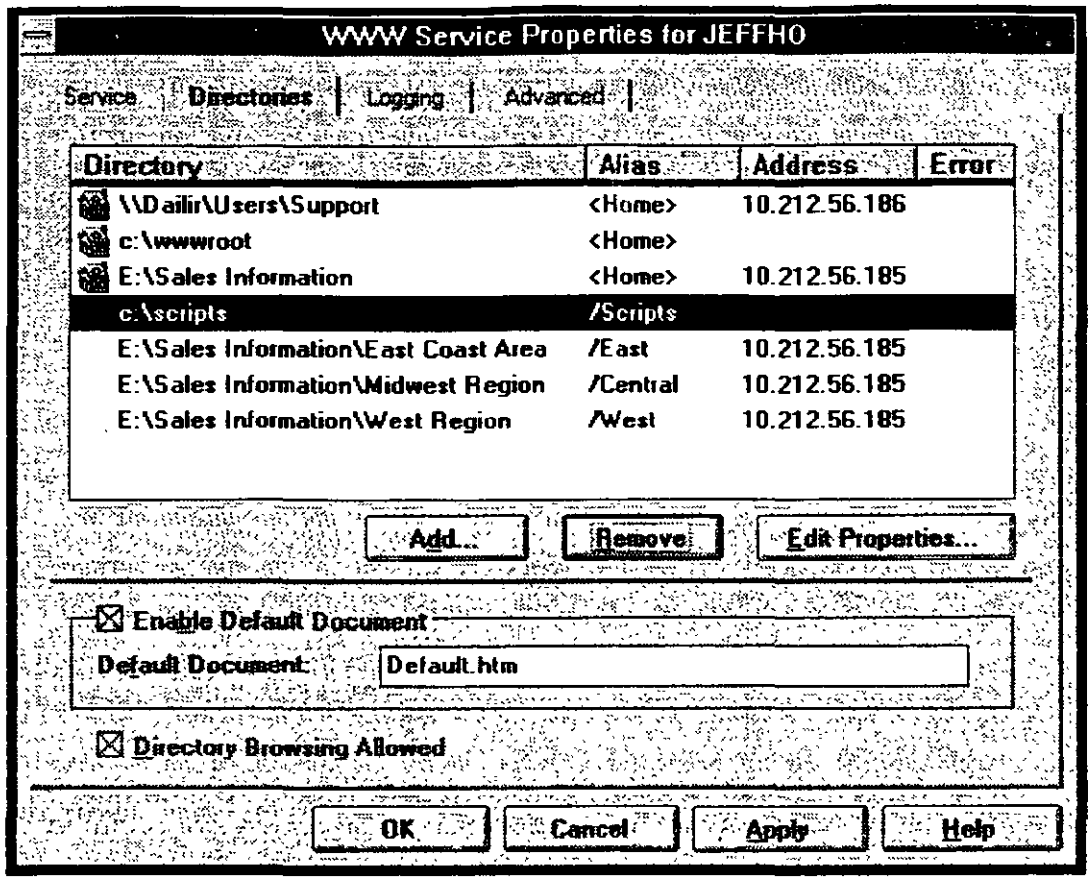
Important The default directories created during setup do not specify an IP address You may need to specify IP addresses for the default directories when you add virtual servers.

Directory

To specify the fully qualified path for the directory to use for the selected virtual server, choose the **Add** button and type the path in the **Directory** box of the **Directory Properties** dialog box, or use the **Browse** button to pick the directory to use.

Configuring Content Directories

If your site is complex, you can configure WWW service to publish from multiple directories by using Internet Service Manager. The **Directories** property sheet lists the content directories used by the WWW service



Directory lists the physical location of the directory.
Alias is the path for information service users
Address lists the IP address of virtual servers assigned to that directory
Error indicates any error status.

To configure individual WWW service directories, in the **Directories** property sheet click the **Add** button or the **Edit Properties** button

Home Directory

Each of the Internet services publishes information stored in one or more directories. The administrator specifies these publishing directories on the **Directories** property sheet of Internet Service Manager Adding a directory on this property sheet allows the respective service to make available to clients information stored in the specified directory, and all of its subdirectories Directories not listed on this property sheet are not available to clients.

Every service must have a home directory The home directory is the "root" directory for that service A root directory does not have a name By default, the home directory and all folders in it are available to users

To change your home directory

1. In Internet Service Manager, double-click the service for which you want to change the home directory to display its property sheets.

2. Click the **Directories** tab.

3. In the **Directory** list, select the directory with the <home> alias.

4. Click **Edit Properties**.

5. In the **Directory** box, type the name of the new directory, or select a new directory by using the **Browse** button.

6. In the **Access** box, select the access that you want to give users who connect to that directory.

7. Click **OK**.

8. Click **Apply** and then click **OK**.

To add a directory

1. In Internet Service Manager, double-click the service for which you want to add a directory to display its property sheets

2. Click the **Directories** tab.

3. Click **Add**

4. In the **Directory** box, type the name of the new directory or select a new directory by using the **Browse** button

5. In the **Access** box (if applicable), select the access you want to give users who connect to that directory.

6. Click **OK**.

7. Click **Apply** and then click **OK**

To delete a directory

1. In Internet Service Manager, double-click the service for which you want to delete a directory to display its property sheets

2. Click the **Directories** tab.

3. In the **Directory** list, select the directory you want to delete.

4. Click **Remove**.

5. Click **Apply** and then click **OK**.

Note Deleting a virtual directory does not delete the directory or files to which the virtual directory points

One (or more, if multiple virtual directories are active) of the directories listed on the **Directories** property sheet is marked as a home directory (sometimes referred to as a *root* directory). The path used in a client request to refer to the home directory is a forward slash (/). When a client request contains a path of /, or does not specify the path to a resource, the Web server looks in the defined home directory for the resource. For example, all of the following URLs refer to the Web server's home directory.

http://inetsrvr.microsoft.com

http //inetsrvr.microsoft com/

http://inetsrvr.microsoft.com/content.htm

The action taken by the Web server for the first two URLs shown above depends on the settings of the **Default Document** and **Directory Browsing** options, specified on the **Service** property sheet of Internet Service Manager. For the third example, the HTML file Content.htm, located in the home directory, is sent to the client If a file by that name does not exist in the home directory, the server returns an error to the client. Other directories are not searched for such a file.

When a client logs on to the FTP service, the service looks for a subdirectory under the specified home directory with the name of the user logging on. For anonymous FTP logons, the service looks for a directory called "anonymous" under the home directory. If such a directory exists, the user will start the session with it as the current directory If such a directory is not found, the current directory will be the home directory

Subdirectories of the home directory are accessible to clients. For example, if a WWW service is configured with a home directory of C \Wwwroot, then the following URL:

http //inetsrvr microsoft com/data/content htm

causes the Web server to look for a file by the name content.htm in the directory C:\Wwwroot\Data If the Data subdirectory does not exist, or the file is not found in that directory, the server will return an error The FTP service allows changing the current directory to subdirectories of the home directory (by using the **cd** command), and gopher selectors can refer to objects in subdirectories of the home directory

Virtual Directory

Each of the Internet services can publish from multiple directories. Each directory can be located on a local drive, or across the network, by specifying the directory with a Universal

Naming Convention (UNC) name, and a user name and password to use for access permission. A virtual server can have one home directory and any number of other publishing directories. These other publishing directories are referred to as *virtual directories*.

To simplify client URL addresses, the services present the entire set of publishing directories to clients as a single directory tree. The home directory is the root of this "virtual" directory tree, and each virtual directory is addressed as if it were a subdirectory of the home directory. Actual subdirectories of the virtual directories are available to clients as well. The WWW service alone supports virtual servers; thus, the FTP and gopher services can have only one home directory.

Note Virtual directories will not appear in directory listings (also called "directory browsing" for the WWW service). To access a virtual directory users must know the virtual directory's alias, and type the URL in the browser For the WWW service, you can also create links in HTML pages. For the gopher service, you can create explicit links in tag files so that users can access virtual directories For the FTP service, you can list virtual directories by using directory annotations.

When a virtual directory is defined in Internet Service Manager, an *alias* is associated with the virtual directory. The alias is the subdirectory name that will be used by clients to access information in the virtual directory. If alias names for virtual directories are not specified by the administrator, an alias name is generated automatically by Internet Service Manager

For example, suppose an administrator defines two directories for the WWW service as follows

C:\Wwwroot <home directory>

D:\Webdata Alias = data

If C:\Wwwroot contains the subdirectory C:\Wwwroot\Scripts\, and D:\Webdata contains the subdirectory D:\Webdata\Images\, the following URLs can be requested by a Web client

http://inetsrvr.microsoft com/schedule.htm

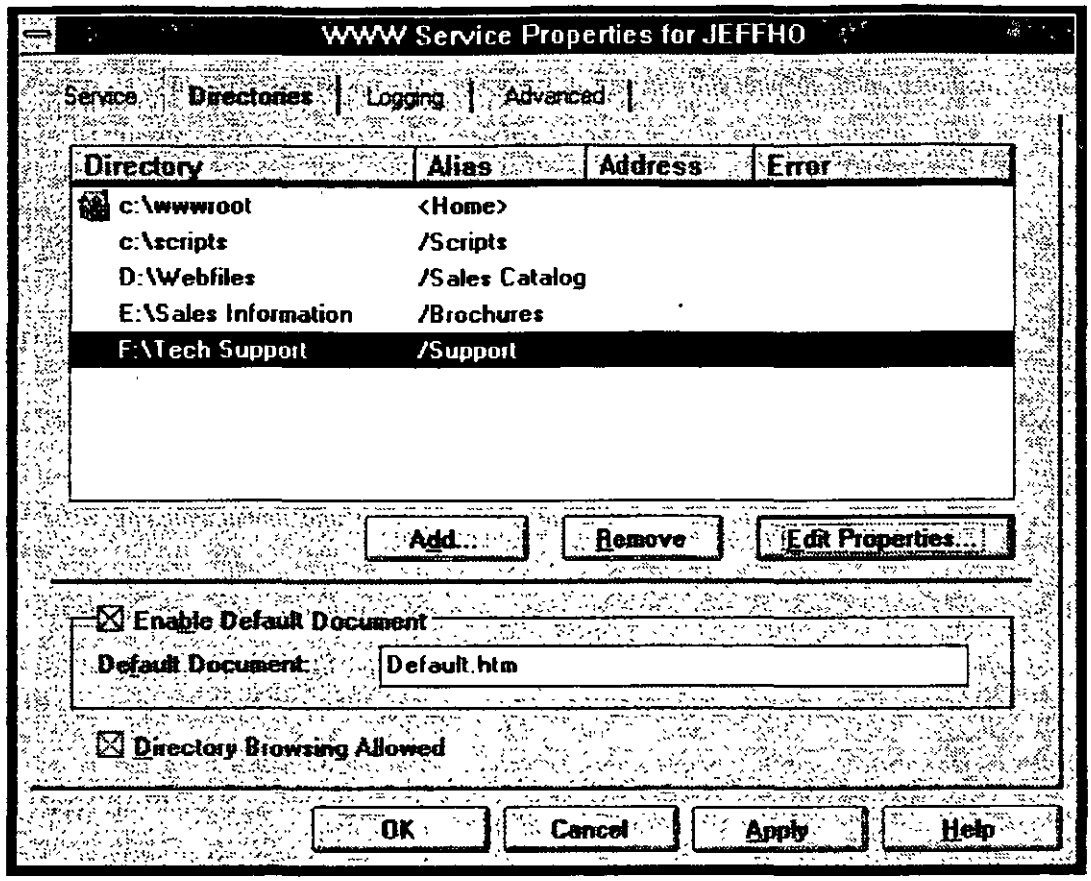
http://inetsrvr.microsoft com/scripts/query1 htm

http://inetsrvr.microsoft.com/data/stocks.htm

http://inetsrvr microsoft.com/data/images/graph1 htm

For another example, if you want to provide three different product catalogs, each catalog could be stored on a separate hard drive on the server www.company.com.

Virtual directories can be used to present three separate drives as three subdirectories



To browsers, virtual directories appear as subdirectories of the "root" home directory. You must provide the name (alias) that browsers will use to specify that directory.

Note To browse virtual directories, the URL for the virtual directory must be specified. This can be done either by clicking a hypertext link containing the URL, or by typing the URL in the browser.

Creating Virtual Directories

You can create an almost unlimited number of virtual directories for your service, although performance may suffer if you create too many of them.

To create a virtual directory

1. In Internet Service Manager, double-click the service for which you want to add a virtual directory to display its property sheets.
2. Click the **Directories** tab.
3. Click **Add**.
4. Click **Browse** to select a directory in the **Directory** box.

5. Click **Virtual Directory**, then type the name of the virtual directory in the **Alias** box.

6. Set the Access permissions.

7. Click **OK**.

8. Click **Apply** and then click **OK**.

Note Virtual directories will not appear in directory listings (also called "directory browsing" for the WWW service) To access a virtual directory, users must know the virtual directory's alias and type the URL in the browser. For the WWW service, you can also create links in HTML pages. For the gopher service, you can create explicit links in tag files so that users can access virtual directories.

Specifying Directories with Virtual Servers

If you have assigned more than one IP address to your server, when you create a directory, you must specify which IP address has access to that directory. If no IP address is specified, that directory will be visible to all virtual servers.

Important The default directories created during setup do not specify an IP address. You may need to specify IP addresses for the default directories when you add virtual servers

---

Account Information

This entry applies only if the physical directory is listed by using a Universal Naming Convention (UNC) path, such as \\Research4\Public\Wwwfiles Enter a user name and password with permission to use the network directory share

Access Check Boxes

Read must be selected for content directories

For the FTP Service, **Write** must be selected for directories that will accept data from users Assign Write access cautiously to prevent unauthorized users from placing malicious files on, or deleting information from, your computer

For the WWW service, **Execute** must be selected for directories containing programs, scripts, and Internet Server API (ISAPI) applications Also, ensure that any directory marked Execute is not also marked Read, this will prevent users from seeing your interactive content executable files.

For the WWW service, **Require secure SSL channel** must be selected to require encrypted communication for a directory For more information on Secure Sockets Layer (SSL), see Chapter 5, "Securing Your Site Against Intruders"

CHAPTER 7

Logging Server Activity

Each of the services contained in Microsoft Internet Information Server can be configured to log information about who accessed the server and what information they accessed. This data can help you fine-tune your site, plan for the number of users that regularly gain access to your site, assess content, and audit security.

The logging feature in Internet Information Server has been designed for flexibility in the following areas:

- Choice of data stores:

  File system or Microsoft® SQL Server.

- Various log-file formats.

  Standard format, European Microsoft Windows NT Academic Centre (EMWAC) format, or National Center for Supercomputing (NCSA) Common Log File format.

- Location of log files within the system

- Creation of new log files:

  In logging to file, new log files can be created whenever the files achieve a particular size, or whenever the day, week, or month changes

This chapter explains how to.

- Configure logging
- Read file logs.
- View logs in databases
- Convert log files to other formats

Configuring Logging

When you set up Internet Information Server, you can enable logging to see who has been using the server and how many times your online information was accessed.

To configure logging:

- Determine in which folder the logs will be stored.
- Specify how often logs are to be rotated (every day, every week, every month, and so on).
- Select the log tools you want to use to analyze the logs your server collects.

In Internet Service Manager, double-click the service to display its property sheets. The **Logging** property sheet sets logging for the selected information service.

Log to File

To start logging, select the **Enable Logging** check box on the **Logging** property sheet. To stop logging, clear the **Enable Logging** check box Choose **Log to File** to log activity information for the selected information service to a text file

Log Format

Use the **Log Format** box to select the logging format you want Click the arrow and choose either Standard format or NCSA format, National Center for Supercomputing Applications (NCSA) Common Log File format

Automatically open new log

This option generates new logs using the specified frequency If not selected, the same log file will grow indefinitely.

Log file folder

This option sets the folder (directory) containing the log file

Filename

This field shows the file name used for logging If multiple services are configured to log to the same folder, they will use the same file

To log to a file

1. In Internet Service Manager, double-click a service to display its property sheets, then click the **Logging** tab.

2. Select the **Enable Logging** check box.

3. Select **Log to File**.

4. In the **Log Format** box, select the logging format you want, either Standard or NCSA.

5. To create a new log file when certain conditions are met, select the **Automatically open new log** check box.

   The service will close the log file and create a new one with a different name in the same folder when the appropriate interval or file size is reached. Log file names are as follows:

   - Inetsv1.log if **Automatically open new log** is not selected.
   - Inetsv*nnn*.log (where *nnn* is a sequentially increasing number) if **When file size reaches** is selected
   - In*mmddyy*.log (where *mmddyy* is the month, day, and year when the log file is created) if one of the **Daily**, **Weekly**, or **Monthly** options is enabled.

For the **Daily**, **Weekly**, or **Monthly** options, the log file is closed the first time a log record is generated after midnight on the last day of the current log file. The new log file name will include the date of the first day in the log file.

For the **When file size reaches** option, every time the log file is closed and a new one is created, the sequential number in the file name is incremented.

When logging to a file, the maximum total log line is 1200 bytes Each field is limited to 150 bytes.

Log to SQL/ODBC Database

When you install Microsoft Internet Information Server, logging to a file is the default method of logging. If you prefer to collect logs in a database, you must install ODBC version 2.5 or later To access the pages, make sure that the WWW service is running, and then in the Internet Explorer **Address** box, type the local computer name. Alternatively, you can follow the manual procedure described later in this section

For best results, log to a Microsoft SQL Server version 6 5 database If you do not want to log to a database or use the Internet Database Connector on a Web server, do not install any ODBC drivers.

Choose **Log to SQL/ODBC Database** to log activity information to any Open Database Connectivity (ODBC)-compliant data source. Set **the ODBC Data Source Name (DSN)**, **Table**, and specify the **user name** and **password** to use when logging to the database.

When using ODBC for logging, each field is limited to 255 bytes.

Note Logging to a database increases the amount of time and resources needed to service WWW (HTTP), FTP, and gopher requests. Therefore, if your site has heavy traffic, you should log to the file system to maximize performance.

To manually prepare for logging to a database

1. Create a table that conforms to the sizes of the fields for your database programs, such as Microsoft SQL Server

   In Microsoft SQL Server, the sizes of the fields for a table are as follows:

   ClientHost varchar(255), username varchar(255), LogTime datetime, service varchar(255), machine varchar(255), serverip varchar(50), processingtime int, bytesrecvd int, bytessent int, servicestatus int, win32status int, operation varchar(255), target varchar(255), parameters varchar(255)

   You can find these values in the Logtemp.sql file in the Inetsrv folder

2. Set up a database on your server and create a system Data Source Name (DSN)

Note For Microsoft® Access, the system DSN is the file name of your database

To log to a database

1. In Internet Service Manager, double-click the service for which you want to set up the database.

2. Click the **Logging** tab

3. Select the **Enable Logging** check box

4. Select **Log to SQL/ODBC database**

5. In the **ODBC Data Source Name (DSN)** box, type the system DSN that you added in step 2 of the previous procedure

6. In the **Table** field, type the name of the table (not the file name of the table)

7. In the **User Name** and **Password** fields, type a user name and password that is valid for the computer on which the database resides

8. Click **Apply** and then click **OK**

How to Read Log Files

Following are three entries from a log from a server running the WWW, gopher, and FTP services; the entries are in two tables only because of page-width limitations.

Client's IP address	Client's username	Date	Time	Service	Computer name	IP address of server
10.75.176.21	—	12/11/95	7:55:20	W3SVC	TREY1	10.107.1.121
10.16.7.165	anonymous	12/11/95	23:58:11	MSFTPSVC	TREY1	10.107.1.121
10.55.82.244	—	12/11/95	0:00:34	GopherSvc	TREY1	10.107.1.121

Elapsed time	Bytes received	Bytes sent	Service status code	Windows NT status code	Name of the operation	Target of the operation
4502	163	3223	200	0	GET	small.gif
60	275	0	0	0	[376] PASS	intro
6139	273	62184	0	0	file	form1.bmp

Parameters for the operation, if applicable, will be listed in the final fields.

Note All fields are terminated with a comma (,). A hyphen acts as a placeholder if there is no valid value for a certain field

As a sample interpretation of logging data, the first entry in the table says that an anonymous client with the IP address of 10.75.176.21 downloaded (issued a GET command for) the file Small.gif at 7:55 AM on December 11, 1995, from a server named TREY1 at IP address 10.107.1.121. The 163-byte HTTP request had an elapsed processing time of 4502 milliseconds (almost half a second) to complete (without error) and returned 3223 bytes of data to the anonymous client

The following example shows a log file in NCSA format.

157.55.85.138 - REDMOND\doug [07/Jun/1996:17:39:04 -0800] "POST /iisadmin/default.htm?-, HTTP/1.0" 200 3401

Remote host name	Client's username	Date	Time
157.55.85.138	REDMOND\doug	07/Jun/1996	17:39:10 -0800

Request	Service Status code	Bytes received
GET /scripts/iisadmin/ism.dll?http/serv. HTTP/1.0	200	5125

Viewing Logs in Databases

You can use any ODBC-supported database to log server activity By logging to a database, you can direct the logging of all Internet Information Server services to a single source.

You can use any ODBC-compliant application to view the log data in your database.

In addition, you can use the Internet Database Connector to view log data in a Web browser

---

Converting Log File Formats

Internet Service Manager provides a choice between two log formats.

- Standard format (Microsoft Professional Internet Services format)
- NCSA Common Log File format

In the **Log Format** box on the **Logging** property sheet, click the arrow and select the format you want.

if you have created Microsoft Internet Information Server log files in Standard format and want to convert them to either the EMWAC log file format or NCSA Common Log File format, use the Microsoft Internet Log Converter (Convlog.exe). At the command prompt, type **convlog** without parameters to see syntax and examples

To convert logs to other formats

1. Add Convlog exe (in the \Inetsrv folder, by default) to your path

2. In a command-prompt window, type the **convlog** command. See the syntax and examples below.

Syntax

convlog -s[f|g|w] -t [emwac | ncsa[:*GMTOffset*] | none]

-o [*output directory*] -f [*temp file directory*] -h *LogFilename*

-d<m:[*cachesize*]>

Parameters

-s[f|g|w]

Specifies the service for which to convert log entries

f = Process FTP log entries

g = Process gopher log entries

w = Process WWW log entries

The default for the **-s** switch is to convert logs for all services.

-t [emwac | ncsa[:*GMTOffset*] | none]

Specifies the destination conversion format. The default is to create output files in EMWAC format.

-o [*output directory*]

Specifies the directory for the converted files. The default is the current directory.

-f [*temp file directory*]

Specifies a temporary directory to hold temporary files created by **convlog** The default is C:\Temp or the directory specified by the "tmp" environment variable.

-n[m:[*cachesize*]|i]

Specifies whether to convert IP addresses to computer or domain names. The default is to not convert IP addresses.

m[*cachesize*] = Specifies to convert IP addresses to computer names The default *cachesize* is 5000 bytes

i = Specifies to not convert IP addresses to computer names

-h

Displays Help

LogFilename

Specifies the name of the log to be converted **Convlog** will display the file name for the converted file

-dm:[*cachesize*]

Converts IP addresses in NCSA log format to computer names or domain names. The default is to not convert IP addresses. The default *cachesize* is 5000 bytes.

Examples

convlog -sf -t ncsa -o c:\logs in*.log

convlog -t ncsa:-0300 in*.log

convlog -o \\stats\logs c:\logs\in*.log

convlog -sfg in*.log

convlog -nm *.log

convlog -t none -nm:20000 *.log

Contents | Index | ◁ | △ | ▷

CHAPTER 8

Publishing Information and Applications

Internet Information Server can publish both information and applications. This means that your Web site can contain anything from static pages of information to interactive applications. You can also find and extract information from, and insert information into, databases.

This chapter explains how to:

- Prepare your computer and your information for publishing.
- Install and use interactive applications on your computer.
- Publish by using an Open Database Connectivity (ODBC)–compliant data source.

Preparing Information for Publishing

Most Web pages are formatted in Hypertext Markup Language (HTML). HTML files are simple ASCII text files with codes embedded to indicate formatting and hypertext links HTML specifications are changing constantly You should probably review the HTML specifications (available on the Internet) to fully plan your HTML pages.

Authoring HTML Files

You can use any text editor, such as Notepad or Write, to create and edit your HTML files; but you will probably find an HTML editor, such as Microsoft® FrontPage™ or Internet Assistant for Microsoft® Word, easier to use

You use the HTML editor or other system to create HTML files, which can include hyperlinks to other files on your system If you want to include images or sounds, you will also need appropriate software to create and edit those files

Publishing HTML and Other File Formats

Your files can include images and sound. You can even create links to Microsoft® Office files or to almost any other file format Remote users must have the correct viewing application to view non-HTML files. For example, if you know that all remote users will have Microsoft Word, you can include links to Microsoft Word .doc files. The user can click the link and the document will appear in Word on the user's computer.

Once you have created your information in HTML or other formats, you can either copy the information to the default directory InetPub\Wwwroot, or you can change the default home directory to the directory containing your information.

MIME Type Configuration

If your Web site includes files that are in multiple formats, your computer must have a Multipurpose Internet Mail Extension (MIME) mapping for each file type. If MIME mapping on the server is not set up for a specific file type, browsers may not be able to retrieve the file. See the Windows NT registry for the default MIME mappings.

To configure additional MIME mappings, start the Registry Editor (Regedt32.exe) and open

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\InetInfo\Parameters\MimeM

Add a REG_SZ value for the MIME mapping required for your computer with the following syntax:

<mime type>,<filename extension> , <mime type>, <mime type>

For example

text/html,htm,
image/jpeg,jpeg,

The string associated with the value (that is, the value content) should be blank The default entry with the file-name extension specified as an asterisk (*) is the default MIME type used when a MIME mapping does not exist For example, to handle a request for the file Current vgr when the the file-name extension vgr is not mapped to a MIME type, your computer will use the MIME type specified for the asterisk extension, which is the type used for binary data.Usually, this will cause browsers to save the file to disk

Including Other Files with the Include Statement

You can add common information into HTML files just before sending the files to users. This feature is handy for including the same text on each HTML page, such as copyright information or a link to the home page

The format of the include statement is

The value can contain a relative path or the full path, from the home directory of your WWW service.

For example, to include a link to your home page in each HTML document:

1. Create the file Linkhome.htm, which contains the HTML codes you want to repeat; for example, a button to your home page. The file would contain HTML code that looks similar to this:

```
<A HREF="/homepage.htm"><IMG SRC="/images/button_h.gif"></A>
```

2. Use the file-name extension .stm when you create your Web pages (rather than .htm or .html).

Notes The .stm extension tells Internet Information Server that there is an include statement in the file If you name the file with an .htm or .html extension, the include statement will be ignored.

Using .stm files may affect performance Therefore, use this extension only when necessary.

However, in the Windows NT registry, you can change the default stm extension to any extension you want, except for .htm or html For details, see the ServerSideIncludesExtension registry key in Chapter 10, "Configuring Registry Entries."

3. In each .stm file, use an **include file** statement where you want the repeated information to appear. For example

```
<!-- #include file="/header.htm" -->
```

Note that all paths are relative to the WWW home directory and can include virtual directories

Publishing Dynamic Applications

One of the most exciting features you get when you use Microsoft Internet Information Server is the ability to develop applications or scripts that remote users start by clicking HTML links or by filling in and sending an HTML form Using programming languages such as C or Perl, you can create applications or scripts that communicate with the user in dynamic HTML pages

Creating the Applications or Scripts

Interactive applications or scripts can be written in almost any 32-bit programming language, such as C or Perl, or as Windows NT batch files (which have the .bat or .cmd file-name extension). When you write your applications or script you can use one of two supported interfaces, Microsoft Internet Server Application Programming Interface (ISAPI) or Common Gateway Interface (CGI). Documentation for ISAPI is available from Microsoft by subscription to the Microsoft Developer Network (MSDN). You can find an introduction to CGI later in this chapter; CGI information readily accessible by way of the Internet Batch files can issue any command valid at the command prompt.

Applications that use ISAPI are compiled as dynamic-link libraries (DLLs) that are loaded by the WWW service at startup. Because the programs are resident in memory, ISAPI programs are significantly faster than applications written to the CGI specification.

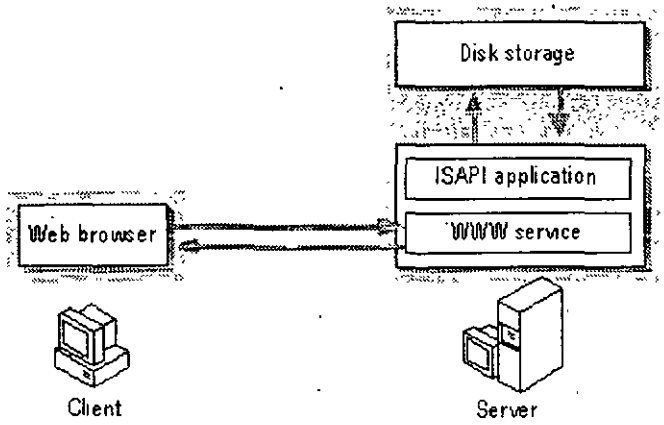
ISAPI Perl Available for Download

Hip, Inc., the independent software vendor that develops Perl for Win32 platforms, has developed a version of Perl that runs as an ISAPI application. This means that Perl server scripts can run much faster than before by taking advantage of the in-process model of ISAPI. An unsupported release of ISAPI Perl is now available for download at http://www perl hip.com/. More information is available on that WWW site. Please use the perlis@mail.hip.com e-mail alias to ask questions or send feedback, especially if you have existing Perl scripts.

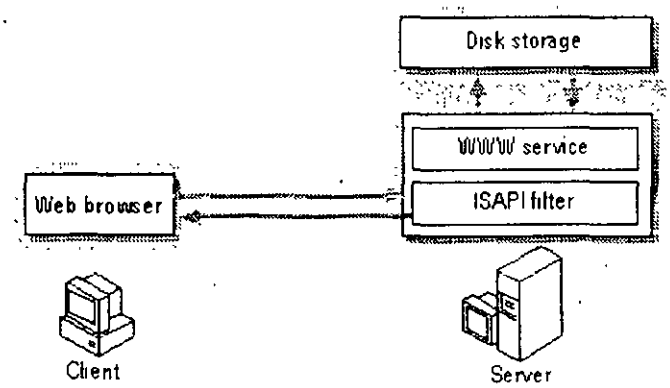
Internet Server API

ISAPI for Windows NT can be used to write applications that Web users can activate by filling out an HTML form or clicking a link in an HTML page on your Web site. The remote application can then take the user-supplied information and do almost anything with it that can be programmed, and then return the results in an HTML page or post the information in a database.

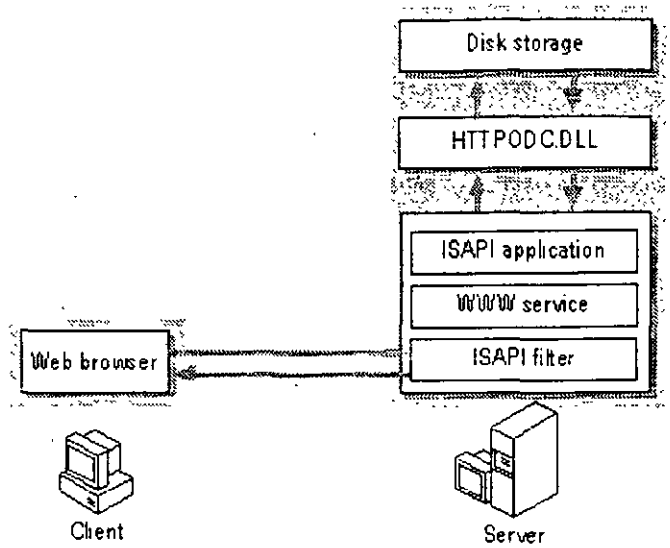
ISAPI can be used to create applications that run as DLLs on your Web server If you have used Common Gateway Interface (CGI) scripts before, you will find that the ISAPI applications have much better performance because your applications are loaded into memory at server run-time. They require less overhead because each request does not start a separate process.



Another feature of ISAPI allows pre-processing of requests and post-processing of responses, permitting site-specific handling of Hypertext Transfer Protocol (HTTP) requests and responses. ISAPI filters can be used for applications such as customized authentication, access, or logging.



You can create very complex sites by using both ISAPI filters and applications ISAPI extensions can also be combined with the Internet Database Connector to create highly interactive sites.



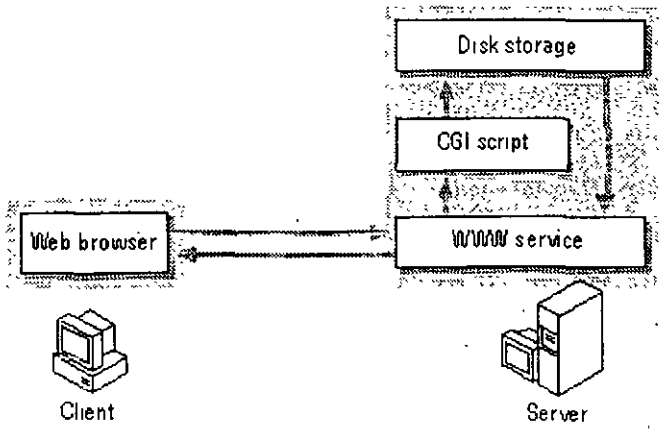
For complete information about programming with ISAPI, see the Microsoft Win32 BackOffice Software Development Kit (SDK), available from MSDN. See the introductory chapter of this guide, "Before You Begin," for further information about obtaining the ISAPI SDK.

Common Gateway Interface

Common Gateway Interface (CGI) is a set of specifications for passing information between a client Web browser, a Web server, and a CGI application A client Web browser can start a CGI application by filling out an HTML form or clicking a link in an HTML page on your Web server. As with ISAPI, the CGI application can take the information the client Web browser supplies and do almost anything that can be programmed, then return the results of the application in an HTML page, or post the information to a database. Because simple CGI applications are often written using scripting languages such as Perl, CGI applications are sometimes referred to as "scripts "

Microsoft Internet Information Server can use most 32-bit applications that run on Windows NT and conform to the CGI specifications

The following figure illustrates how a browser, a server, and a CGI application exchange information by using CGI The rest of this section discusses this five-part process



Client Sends Request

A client browser can make a CGI request to a server by either of two methods:

GET

The client appends data to the URL it passes to the server.

POST

The client sends data to the server by way of the HTTP message data field, thereby overcoming size limitations inherent to the GET method.

The client initiates a CGI process by clicking any of the following on an HTML page

- A hypertext link that runs the script directly
- The "Submit" button in an HTML form.
- An inline object retrieved with the GET method.
- A search object (that is, one that uses the HTML tag ISINDEX).

Server Receives Request

The URL that the client browser sends to the server contains the name of the CGI script or application to be run. The server compares the file name's extension to the server's Script Mapping registry key to determine which executable to launch. The server has Script Map entries for cmd and .bat files, which launch Cmd.exe, and for idc files, which launch the Internet Database Connector. To enable the server to launch a type of CGI application without an extension mapping, add an entry for that application type to the registry key. For example, to enable Perl scripts to run, add an entry like the following.

Where

- \Reskit\Perl\Bin\ is the directory containing the executable.
- Perl.exe is the command executed.
- the first **%s** is the translated path of the PERL script (the URL translated to a local path).
- The second **%s** is the query string (information in the URL) and is passed as a command line parameter only if the query string does not contain an equals (=) sign.

Server Passes Request to Application

The server passes information to the CGI application by means of environment variables, then launches the application. Some of these variables are server-related; the majority come from the client browser and relate either to the client browser or to the request it is sending. See the table of variables at the end of this chapter for a partial list of environment variables.

CGI Application Returns Data to Server

The application performs its processing. If it is appropriate, the application then writes data in a format the client can receive to the standard output stream (STDOUT). The application must follow a specific format in returning data

1. The first line or lines contain server directives, and must contain the MIME content-type. Other server directives are Location (which redirects the client to, or returns, another document) and Status.
2. A blank line must follow server directives
3. The data the application returns to the client follows the blank line.

Server Returns Data to Client

The server takes the data it receives from STDOUT and adds standard HTTP headers It then passes the HTTP message back to the client

For more information about CGI, refer to the CGI specifications at http://hoohoo.ncsa.uiuc.edu/cgi/

CGI and Internet Information Server

The WWW service supports the standard Common Gateway Interface (CGI) specification. However, you should be aware of the following, unique to the implementation of CGI on Internet Information Server

- For this release, only 32-bit CGI applications work with the WWW service

- The REMOTE_USER environment variable is not present when the user is logged in as the anonymous user (that is, when the Web server is accessed anonymously).
- All of the variables defined for ISAPI applications are passed to the CGI application as environment variables.

Note that CGI applications are typically stand-alone executables. This is in contrast to ISAPI applications, which are typically loaded as DLLs and are therefore server extensions. Thus, ISAPI applications offer enhanced performance when compared to CGI applications and scripts.

Security Considerations for Executables

Common Gateway Interface (CGI) executables must be used with extreme caution to prevent potential security risk to the server As a rule, give only Execute permission to virtual directories that contain CGI or Internet Server API (ISAPI) applications

It is highly recommended that you configure script mapping. Script mapping ensures that the correct interpreter (Cmd.exe, for example) starts when a client requests an executable file.

World Wide Web content directories should be assigned Read permission only. Any executable files intended for downloading from Windows NT File System (NTFS) drives should have only Read access enabled

You can run batch files as CGI executable files, but you must do so with extreme caution to prevent potential security risk to the server

Note CGI executable files can also have the file-name extension .exe or .cgi.

Execute Permission for ISAPI Applications

Internet Information Server opens ISAPI applications in the security context of the calling user. An access check is performed against that calling user. To restrict execution to selected users, NTFS permissions can be used with ISAPI applications such as the Internet Database Connector (IDC).

For example, to secure the IDC without putting permissions on the .idc file, you can grant NTFS Execute permission for Inetsrv\Httpodbc.dll to the appropriate users. Httpodbc dll is the name of the ISAPI application DLL that implements the IDC Then, whenever a user tries to execute the IDC, the server will check the permissions. Access will be allowed only if Execute permission has been granted for that user

Note Once an ISAPI application has been loaded, it remains loaded until the WWW service is stopped Internet Information Server does not track security descriptor changes after the ISAPI application has been loaded If you change permissions for an ISAPI application after it has been loaded, you must stop and restart the WWW service before the change will take

effect.

Take care in setting Access Control Lists (ACLs) on the Winnt directory and its subdirectories. Some ISAPI applications and databases require access to files and DLLs in these directories.

Note ISAPI application DLLs can have the file-name extension .dll or .isa.

Installing Your Application on Internet Information Server

Once you have written your application or script, place it in the Scripts directory, a virtual directory for applications. This virtual directory has Execute access.

You must also ensure that every process started by your application is running by using an account with adequate permissions. If your application interacts with other files, the account you assign to your program must have the appropriate permissions to use those files By default, applications run using the IUSR_*computername* account, which must have adminstrator and execute permissions for these application files.

Running Your Application

If your application does not require data from the user, you will typically create a link to your application in a simple HTML file. If your application does require data from the user, you will probably use an HTML form. In other instances you can just send a Uniform Resource Locator (URL), usually containing data parameters, to invoke a program.

An HTML link to an application that does not require input from the user might look like the following example

where Scripts is the virtual directory for interactive applications

If you are creating an application that requires input from the user, you will need to understand both HTML forms and how to use the forms with ISAPI or CGI. This information is widely available on the Internet or from other sources

Associating Interpreters with Applications

Because you have the flexibility to create applications in almost any programming language, Internet Information Server uses the file-name extension to determine which interpreter to invoke for each application The default interpreter associations are listed below You can use the Registry Editor to create additional associations

Extension	Default Interpreter
.bat, .cmd	Cmd.exe
.idc	Httpodbc.dll
.exe, .com	System

Security Implications

When you allow remote users to run applications on your computer, you run the risk of hackers attempting to break into your system. Microsoft Internet Information Server is configured by default to reduce the risk of malicious intrusion by applications in two important ways.

First, the virtual directory Scripts contains your applications. Only an administrator can add programs to a directory marked as an execute-only directory. Thus, unauthorized users cannot copy a malicious application and then run it on your computer without first gaining administrator access.

It is recommended that you grant read and execute permission for the IUSR_*computername* account on the directory associated with the virtual folder, and full control only to the administrator Perl scripts (.pl file-name extension) and IDC files (.idc and .htx file-name extensions) need both read and execute permission However, to prevent someone from installing an unsafe file on your server, do not grant write permission.

Second, if you have configured the WWW service to allow only anonymous logons, all requests from remote users will use the IUSR_*computername* account. By default, the IUSR_*computername* account is unable to delete or change files by using the Windows NT File System (NTFS) unless specifically granted access by an administrator. Thus, even if a malicious program were copied to your computer, it would be unable to cause much damage to your content because it will only have IUSR_*computername* access to your computer and files.

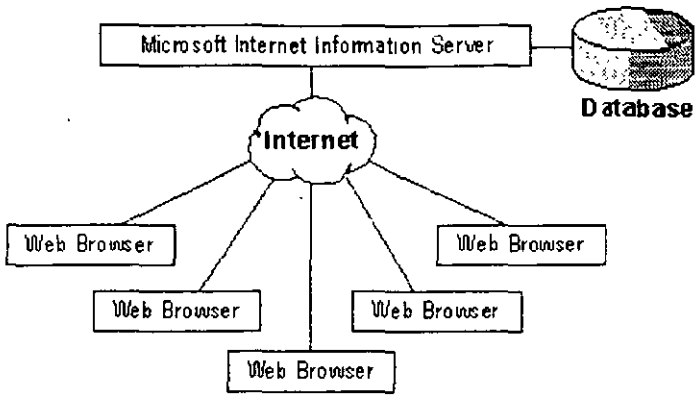
Publishing Information and Using a Database

With the WWW service and the Open Database Connectivity (ODBC) drivers provided with Internet Information Server, you can

- Create Web pages with information contained in a database
- Insert, update, and delete information in the database based on user input from a Web page
- Perform other Structured Query Language (SQL) commands.

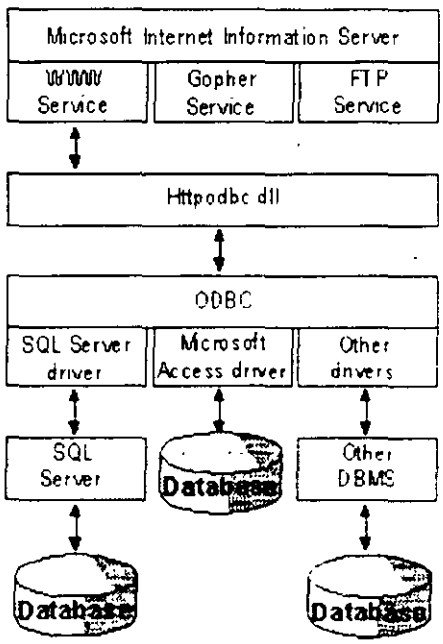
How the Internet Database Connector Works

Conceptually, database access is performed by Internet Information Server as shown in the following diagram.



Web browsers (such as Internet Explorer, or browsers from other companies such as Netscape) submit requests to the Internet server by using HTTP. The Internet server responds with a document formatted in HTML. Access to databases is accomplished through a component of Internet Information Server called the Internet Database Connector (IDC) The Internet Database Connector, Httpodbc.dll, is an ISAPI DLL that uses ODBC to gain access to databases

The following illustration shows the components for connecting to databases from Internet Information Server.



The IDC uses two types of files to control how the database is accessed and how the output

Web page is constructed. These files are Internet Database Connector (.idc) files and HTML extension (.htx) files.

The Internet Database Connector files contain the necessary information to connect to the appropriate ODBC data source and execute the SQL statement. An Internet Database Connector file also contains the name and location of the HTML extension file.

The HTML extension file is the template for the actual HTML document that will be returned to the Web browser after the database information has been merged into it by the IDC.

Installing ODBC and Creating System Data Sources

When the ODBC option is selected during setup, ODBC version 2.5 components are installed. This version of ODBC supports System DSNs (Data Source Names) and is required for using ODBC with Microsoft Internet Information Server.

System DSNs were introduced in ODBC version 2.5 to allow Windows NT services to use ODBC.

To install the ODBC drivers

1. If you did not install the ODBC Drivers and Administration option, run Setup again by clicking the Internet Information Server Setup icon in the Microsoft Internet Server program group You will need the Windows NT Server compact disc, or a network installation directory containing the complete contents of the compact disc

2. Click the **OK** button

3. Click the **Add/Remove** button

4. Click the **OK** button

5. Select the **ODBC Drivers and Administration** option.

6. Click the **OK** button.

7. The **Install Drivers** dialog box appears.

8. To install the SQL Server driver, select the SQL Server driver from the **Available ODBC Drivers** list box, and click the **OK** button

   Setup completes copying files

To create the system data sources

1. Double-click the Control Panel icon in the Main program group of Program Manager.

2. Double-click the ODBC icon.

The **ODBC Data Sources** dialog box appears.

You may see other data sources in the list if you previously installed other ODBC drivers.

3. Click the **System DSN** button

Important Be sure to click the **System DSN** button The Internet Database Connector will work only with System DSNs.

The **System Data Sources** dialog box appears.

4. Click the **Add** button.

The **Add Data Source** dialog box appears.

5. Select an ODBC driver in the list box and click **OK** A dialog box specific to your driver will appear.

6. Enter the name of the data source

The data source name is a logical name used by ODBC to refer to the driver and any other information required to access the data, such as the actual server name or location of the database. The data source name is used in Internet Database Connector files to tell Internet Information Server where to access the data

For Microsoft SQL Server, the server name, network address, and network library displayed in the Setup dialog box are specific to your installation If you do not know what to enter in these controls, accept the defaults To find out the details, click the **Help** button and find the section that describes your network.

7. Click the **OK** button

The **System Data Sources** dialog box will be displayed again, but now will have the name of the data source displayed

8. Click the **Close** button to close the **System Data Sources** dialog box

9. Click the **Close** button to close the **Data Sources** dialog box.

10. Click the **OK** button to complete the ODBC and DSN setup

32-Bit ODBC Drivers

The Internet Database Connector requires 32-bit ODBC drivers. Refer to the Internet Information Server Help files or the Windows NT ODBC Help file for information about the ODBC option.

Microsoft Access ODBC Drivers

The Internet Database Connector requires the 32-bit ODBC drivers shipped with Microsoft® Office 95 and Microsoft® Access 95. The ODBC driver for Microsoft Access 2.0 will not work with Internet Information Server.

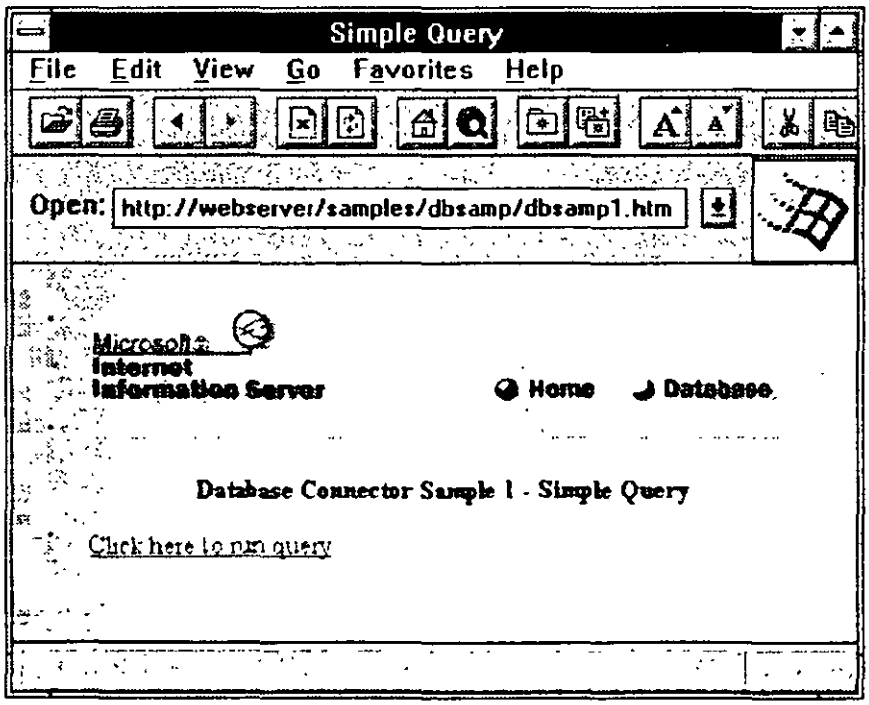
Authoring Web Pages with Database Access

In order to provide access to a SQL database from your Web page, you will need to create an Internet Database Connector file (.idc file-name extension) and an HTML extension file (htx file-name extension).

Walking through a Sample Database Query

This example starts with a simple Web page called Sample.htm. The sample Web page will contain one hyperlink that will result in a query being executed using the ODBC driver for Microsoft SQL Server, with the results returned as another Web page.

The following graphic shows Dbsamp1.htm as it is displayed by Microsoft Internet Explorer (assuming that Internet Information Server has been installed on a computer called "webserver")

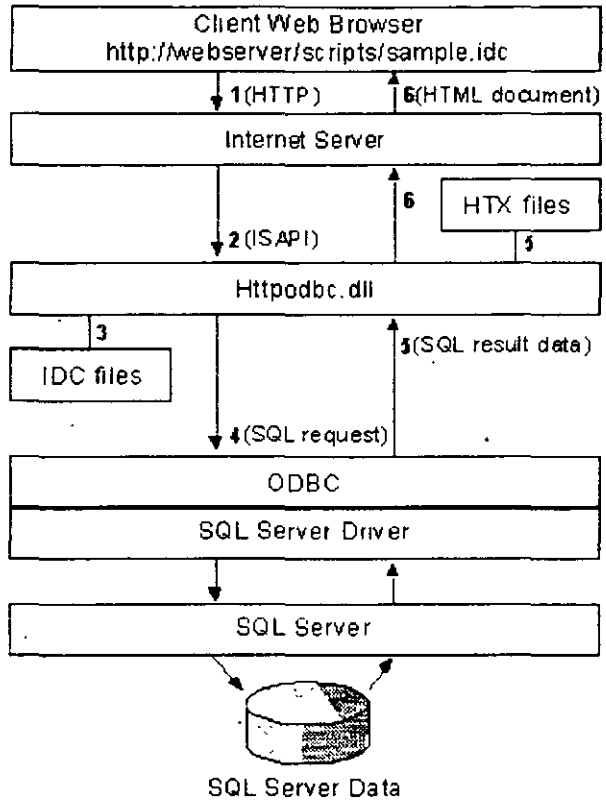


When the hyperlink "Click here to run query" is clicked, another Uniform Resource Locator (URL) is sent to the server. The URL precedes the hyperlink text (it is formatted as hidden text).

```
<A HREF="http://webserver/samples/dbsamp/dbsamp1.idc">Click here to run query</A>
```

The Internet Database Connector file for the IDC to use (Dbsamp1.idc) is referenced in the URL. Extension file mapping precludes the need to reference Httpodbc.dll in the URL.

On Internet Information Server, the entire process of using the Internet Database Connector for this example is performed in six steps, as shown in the following diagram.



1. The URL is received by Internet Information Server.

The URL is sent by the Web browser

2. Internet Information Server loads Httpodbc.dll and provides it with the remaining information in the URL.

Idc files are mapped to Httpodbc dll Httpodbc dll loads and obtains the name of the Internet Database Connector file (and other items) from the URL passed to Internet Information Server

3. Httpodbc.dll reads the Internet Database Connector file.

The Internet Database Connector file contains several entries in the format

In the Sample.idc file, the ODBC data source is specified by:

```
Datasource: Web SQL
```

And the HTML extension file is specified by:

```
Template: sample.htx
```

Here are the entire contents of the file Sample.idc referenced in the preceding URL:

```
Datasource: Web SQL
Username: sa
Template: sample.htx
SQLStatement:
-SELECT au_lname, ytd_sales
- from pubs.dbo.titleview
- where ytd_sales>5000
```

In the sample idc file the data source name is "Web SQL" The ODBC installation notes tell how to create a data source called Web SQL.

The other items contained in the sample .idc file include:

- User name, which must be a valid logon to the ODBC datasource; in this example, the logon is to the "sa" account on a Microsoft SQL Server
- Template, which specifies the file to use to merge the results.
- SQL Statement, which contains the SQL statement to execute.

See "Learning the Features of the Internet Database Connector," later in this chapter, for definitions for all the fields that can be specified in Internet Database Connector files

The SQLStatement in Sample idc returns all the author last names and year-to-date sales in units from the "pubs" sample database in SQL Server for authors whose books have year-to-date sales of more than 5000 dollars

4. The IDC connects to the ODBC data source, and executes the SQL statement contained within the Internet Database Connector file.

The connection is made to the ODBC data source by the IDC, which in this example loads the ODBC driver for SQL Server and connects to the server specified in the definition of the data source Once the connection is made, the SQLStatement in the Internet Database Connector file is sent to the SQL Server ODBC driver, which in turn

sends it to SQL Server.

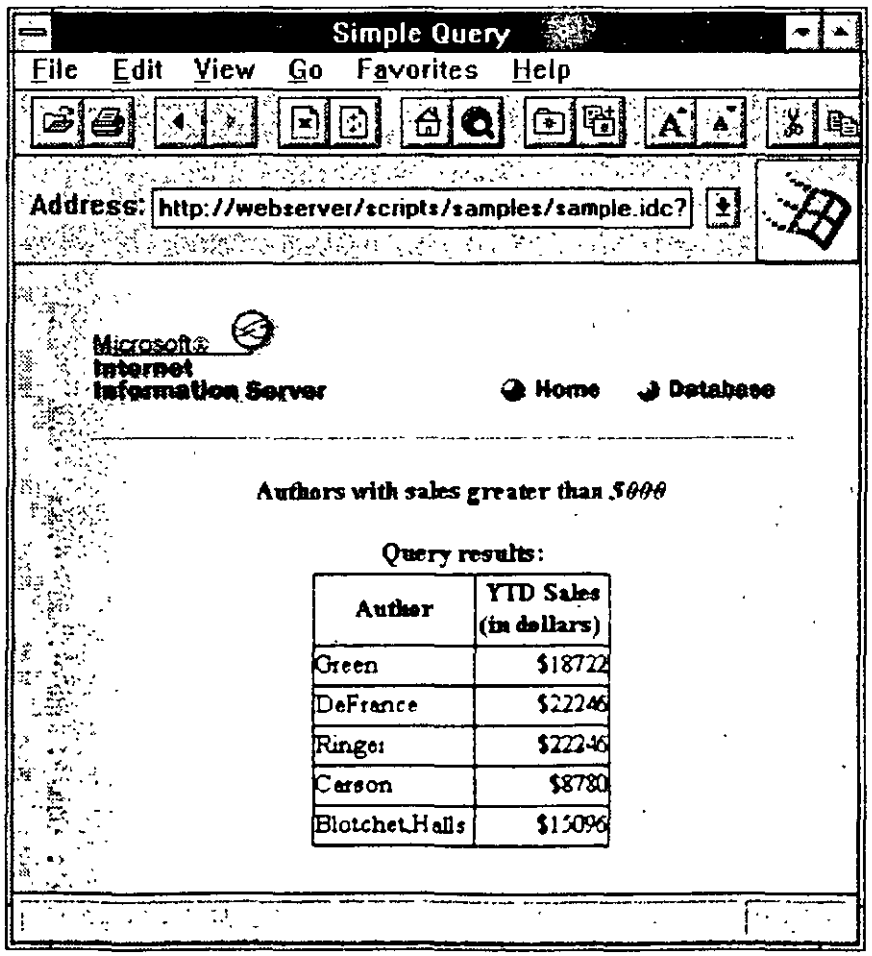
5. The IDC fetches the data from the database, and merges it into the HTML extension file.

After the SQL statement has been executed, IDC reads the HTML extension file specified in Sample.idc (Sample.htx). HTML extension (.htx) files contains special HTML tags which IDC uses to control where and how the data returned from the SQL statement is merged

6. The IDC sends the merged document back to Internet Information Server, which returns it to the client.

After all the data has been merged into Sample.htx, the complete HTML document is sent back to the client

The resulting Web page is displayed in the Microsoft Internet Explorer as shown following.



Understanding the Sample.htx File

To return data to the WWW client, the .idc file merges the HTML extension .htx file and the ODBC data. This combined data is attached to standard HTTP headers (200 OK status, Content-Type, and so on) and passed to the WWW service and returned to the client.

The .htx file is an HTML document with some additional tags enclosed by <%%> or <!--%%-->, which the .idc file uses to add dynamic data to the document. The HTML formatting in the .htx file typically formats the data being returned: There are six keywords (begindetail, enddetail, if, else, endif, and "%z") that control how the data from the database is merged with the HTML format in the .htx file. Database column names specify what data is returned in the HTML document. For example, the following line in an .htx file merges data from the Emailname column for every record processed:

```
<%begindetail%><%Emailname%><%enddetail%>
```

The Sample.htx file is an HTML document that contains Internet Database Connector tags for data returned from the database (the tags are shown in bold for clarity). Some HTML formatting has been removed to highlight the IDC tags.

Most of the HTML formatting has been removed for clarity.

```
<HTML>
<BODY>
<HEAD><TITLE>Authors and YTD Sales</TITLE></HEAD>
<%if idc.sales eq ""%>

<H2>Authors with sales greater than <I>5000</I></H2>
<%else%>

<H2>Authors with sales greater than <I><%idc.sales%></I></H2>
<%endif%>

<P>
<%begindetail%>
<%if CurrentRecord EQ 0 %>

Query results
<B>Author YTD Sales<BR></B>
<%endif%>
<%au_lname%><%ytd_sales%>
<%enddetail%>
<P>
<%if CurrentRecord EQ 0 %>
<I><B>Sorry, no authors had YTD sales greater than </I><%idc.sales%>.</B>
```

<P>
<%else%>

<HR>
<I>
The Web page you see here was created by merging the results of the SQL query with the template file Sample.htx.
<P>
The merge was done by the Microsoft Internet Database Connector and the results were returned to this Web browser by the Microsoft Internet Information Server.
</I>
<%endif%>

</BODY>
</HTML>

The <%begindetail%> and <%enddetail%> sections delimit where rows returned from the database will appear in the document. Columns returned from the query are surrounded by <%%>, such as <%au_lname%> and <%ytd_sales%> in this example.

Learning the Features of the Internet Database Connector

The Internet Database Connector has several features that help create Web pages containing data from a database.

Internet Database Connector Files

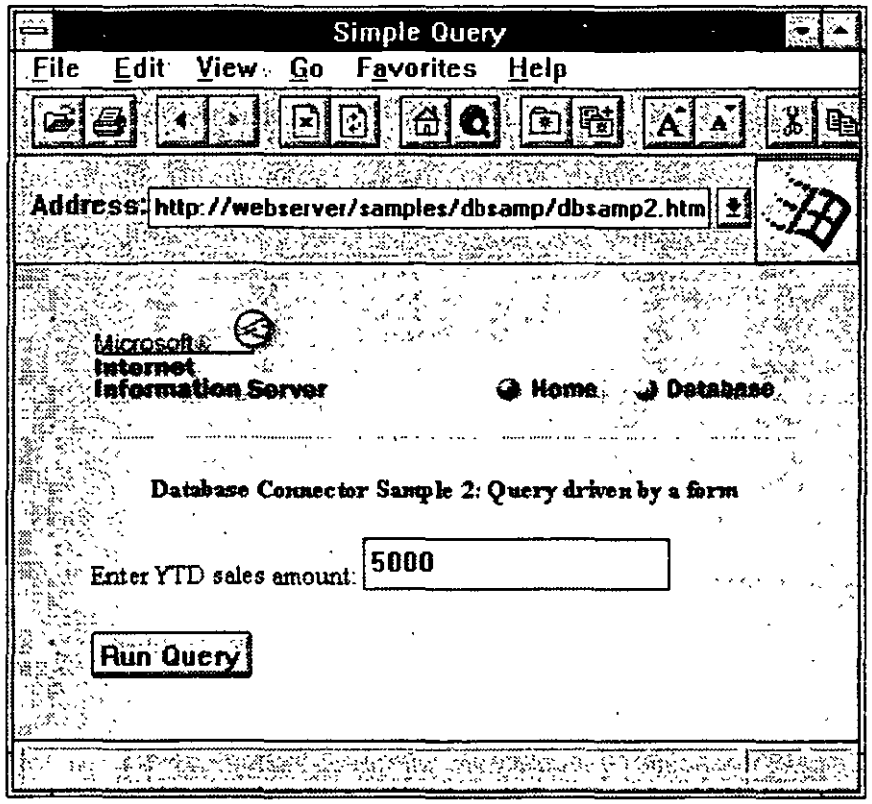
Internet Database Connector files contain the information used to access the database The following section describes the features of Internet Database Connector files

Parameters

The example in the preceding section shows only the simplest kind of query, a query that was defined completely in the Internet Database Connector file Although this type of query is useful, even more powerful Web pages can be constructed through the use of parameters Parameters are the names and values of HTML-form controls, such as "<INPUT >", and names specified directly in URLs These names and values are sent by Web browsers and can be used in SQL statements on the server

For example, in the last section the query in Sample idc returned only the authors whose year-to-date sales exceeded 5000 By using a parameter, you could build a Web page that asks the user to decide what number to use instead of 5000

The Web page must prompt the user for the year-to-date sales figure and then name the associated variable to "sales " Dbsamp2 htm shows a form with an input field used to obtain the number:



The HTML syntax for the input field and button in Sample2 htm is

```
<FORM METHOD="POST" ACTION="/scripts/samples/sample2.idc">
<P>
Enter YTD sales amount: <INPUT NAME "sales" VALUE="5000" >
<P>
<INPUT TYPE="SUBMIT" VALUE="Run Query"
</FORM>
```

In the Internet Database Connector file Sample2 idc, you use the parameter shown in bold in place of the number 5000

```
sales
```

Here the parameter name must be "sales" so that it corresponds to the <INPUT NAME= "sales" ...> on the Web page Parameters must be enclosed with percent characters (%) to distinguish them from a normal identifier in SQL. When the Internet Database Connector encounters the parameter in the idc file, the Internet Database Connector substitutes the value sent by the Web browser and then sends the SQL statement to the ODBC driver.

The percent character (%) is also a wildcard character in SQL. You can use wildcards in an SQL query to search for an element in a table that contains certain characters To insert a

single "%" for a SQL wildcard, use "%%." This prevents the IDC from trying to use the % as a parameter marker For example:

```
SQLStatement:
+SELECT au_lname, ytd_sales, title
+ from pubs.dbo.titleview
+ where title like '%%%title%%%'
```

For a percent sign to be recognized as an SQL wildcard you must double it and then add the percent characters around the parameter to distinguish the string as a parameter. In the example, the query searches for all entries in the title column with the word *title* in them. This query returns the following:

```
title
title and deed
main title page
author and title
```

To return all entries with the word *title* as the first five letters, you would format the query as follows

```
SQLStatement:
+SELECT au_lname, ytd_sales, title
+ from pubs.dbo.titleview
+ where title like 'title%%%'
```

In this example, the following results are returned:

```
title
title and deed
```

To return all entries with the word *title* as the last five letters, you format the query as follows

```
SQLStatement:
+SELECT au_lname, ytd_sales, title
+ from pubs.dbo.titleview
+ where title like '%%%title'
```

In this example, the following results are returned

```
title
                : title
```

You can build powerful collections of Web pages by using the output of one query to provide links to other queries For example, to show the titles for an individual author, instead of returning the author name as plain text, you can format it as a link and then use the link to do another query

Another example included Internet Information Server shows how to do this type of linkage Dbsamp3.htm is used to run the query in Sample3 idc, which uses Sample3.htx for the output template. Sample3.htx will return author last names as links, which, when clicked, will display the titles for each author by using Sample3a idc and Sample3a.htx

Fields in Internet Database Connector (.idc) Files

The following tables list the fields that can be specified in an Internet Database Connector file. Note that parameters or server variables may appear anywhere in an .idc file.

Required Fields in an Internet Database Connector (.idc) File

Field	Description
Datasource	The name that corresponds to the ODBC system Data Source Name (DSN) you created earlier by using the ODBC Administrator or the tool provided with the samples.
Template	The name of the HTML extension file that formats the data returned from this query. By convention these files use the file-name extension .htx.
SQLStatement	The SQL statement to execute. The SQL statement can contain parameter values, which must be enclosed with percent characters (%) from the client. The SQLStatement can occupy multiple lines in the Internet Database Connector file. Following the SQLStatement field, each subsequent line beginning with a plus sign (+) is considered part of the SQLStatement field. Multiple SQLStatements can appear in the same file.

Optional Fields in an Internet Database Connector (.idc) File

Field	Description
DefaultParameters = *param=value* [, *param=value*] [...]	The parameter values, if any, that will be used in the Internet Database Connector file if a parameter is not specified by the client.
Expires	The number of seconds to wait before refreshing a cached output page. If a subsequent request is identical, the cached page will be returned without ever accessing the database. The Expires field is useful when you want to force a requery of the database after a certain period of time. The IDC does not cache output pages by default. It caches them only when the Expires field is used.
MaxFieldSize	The maximum buffer space allocated by the IDC per field. Any characters beyond this will be truncated. The parameter applies only to fields returned from the database that exceed 8192 bytes. The default value is 8192 bytes.
MaxRecords	The maximum number of records that the IDC will return from any one query. The MaxRecords value is not set by default, meaning that a query can return up to 4 billion records. Set this value to limit the records returned
ODBCConnection	Insert this field with the value of *pool* to add the connection to the connection pool, which keeps the connection to the database open for future requests The IDC then sends data through a pooled connection for subsequent execution of an idc file that contains the same values for Datasource, Username, and Password. Set this option to improve performance using the Internet Database Connector. Also, there is a *nonpool* option, which specifies that the connection for the .idc file in which this option is set should not be taken from the connection pool Set the value of this field to **nopool** to manage the cache of connections more precisely. Also, if there is a limit on the number of current connections, you do not want the connection pool to monopolize all the connections; otherwise, no one else could connect to the SQL Server. **Note** To set the default to connection pooling, you must set the PoolIDCConnections registry entry to 1. For details, see Chapter 10, "Configuring Registry Entries"
Password	The password that corresponds to the user name. If the password is null, this field can be left out
RequiredParameters	The parameter names, if any, that Httpodbc.dll will ensure are passed from the client, otherwise, it will return an error Parameter names are separated with a comma
Translationfile	The path to the file that maps non-English characters (such as à, ô, or é) so that browsers can display them properly in HTML format If the translation file is not in the same directory as the idc file, you must type the full path to the translation file Syntax: Translationfile C:*directoryname**filename* Use the Translationfile field if you are publishing a database in a language other than English. A translation file is a text file with each special character mapped in the following format *value=string*<CR> where *value* is an international character and *string* is the HTML translation code
Username	A valid user name for the data source name supplied in the Datasource field **Note** If you use Microsoft SQL Server with the integrated security

	option, the username and password fields in the .idc file are ignored. The logon to SQL Server is performed using the credentials of the Web user. If the request is made as the anonymous user, the username and password are determined by the settings for the anonymous user (IUSR_*computername* by default) in the Internet Service Manager. If the client request contained logon credentials, the username and password supplied by the end user are used to log on to SQL Server.
Content-Type	Any valid MIME type describing what will be returned to the client. Almost always this will be "text/html" if the .htx file contains HTML.

ODBC Advanced Optional Fields

ODBC advanced options allow debugging and fine-tuning of the ODBC driver used by the Internet Database Connector. For more details about these options, consult your ODBC driver documentation or the ODBC Software Development Kit (SDK). The format in the IDC file is:

```
ODBCOptions: Option Name=Value[,Option Name=Value...]
```

For example, to stop the SQL statement from running for more than 10 seconds and enabling tracing of ODBC function calls, in the IDC file you would specify:

```
ODBCOptions: SQL_QUERY_TIMEOUT=10, SQL_OPT_TRACE=1, SQL_OPT_TRACEFILE=C:\Sql.log
```

All options are described in the following table

Option Name	Value	Purpose
SQL_ACCESS_MODE	0 = Read/Write 1 = Read Only.	An indicator for the ODBC driver or data source that the connection is not required to support SQL statements that cause updates to occur. This mode can be used to optimize locking strategies, transaction management, or other areas as appropriate to the driver or data source. The driver is not required to prevent such statements from being submitted to the data source. The behavior of the driver and data source when asked to process SQL statements that are not read-only during a read-only connection is implementation-defined. SQL_ACCESS_MODE set to 0 is the default, which allows reading and writing.
SQL_LOGIN_TIMEOUT	Integer	The number of seconds to wait for a logon request to complete before disconnecting. The default is driver-dependent and must be nonzero. If the value is 0, the timeout is disabled and a connection attempt will wait indefinitely. If the specified timeout exceeds the maximum log on timeout in the data source, the driver substitutes that value.
SQL_OPT_TRACE	0 = Trace off 1 = Trace on	When tracing is on, each ODBC function call made by Httpodbc.dll is written to the trace file. You can specify a trace file with the SQL_OPT_TRACEFILE option. If the file already exists, the ODBC appends to the file. Otherwise, it creates the file. If tracing is on and no trace file has been specified, ODBC writes to the file Sql.log.
SQL_OPT_TRACEFILE	File name	The name of the trace file to use when SQL_OPT_TRACE=1. The default is SQL.LOG
SQL_PACKET_SIZE	Integer	The network packet size, in bytes, to be used to exchange information between the database management system (DBMS) and the Web Server **Note** Many data sources either do not support this option or can return only the network packet size. If the specified size exceeds the maximum packet size or is smaller than the minimum packet size, the driver substitutes that value.
SQL_TRANSLATE_DLL	File name	The name of a DLL containing the functions SQLDriverToDataSource and SQLDataSourceToDriver that the driver loads and uses to perform tasks such as character-set translation
SQL_TRANSLATE_OPTION	Integer	Value controlling translation functionality, which is specific to the translation DLL being used. Consult the documentation for the driver and translation DLL for details.

SQL_TXN_ISOLATION	Integer 1=Read Uncommited 2=Read Committed 4=Repeatable Read 8=Serializable 16=Versioning	Sets the transaction isolation level. The Internet Database Connector does not support transactions than span more than the request in the .idc file. However, for some DBMSs, setting the SQL_TXN_ISOLATION option to 1 (Read Uncommited) will result in higher concurrency and therefore better performance. However, with this setting, data that has not been committed to the database by other transactions may be retrieved .
SQL_MAX_LENGTH	Integer	The maximum amount of data that the driver returns from a character or binary column. This option is intended to reduce network traffic and should only be used when the data source (as opposed to the driver) in a multiple-tier driver can implement it.
SQL_MAX_ROWS	Integer	The maximum number of rows to return for a SELECT statement. If the value equals 0 (the default), then the driver returns all rows. This option is intended to reduce network traffic when the data source itself can limit the return rows, as opposed to the MaxRecords built-in variable in the Internet Database Connector, which limits the rows fetched.
SQL_NOSCAN	0=Scan for and convert escape clauses 1=Do not scan for and convert escape clauses	Specifies whether the driver does not scan SQL strings for escape clauses. If set to 0 (the default), the driver scans SQL strings for escape clauses. If set to 1, the driver does not scan SQL strings for escape clauses; instead, the driver sends the statement directly to the data source. If your SQL statement does not contain any ODBC escape clauses, a special syntax enclosed by curly braces ({ }), then setting this option to 1 will provide a small performance gain by directing the driver to not scan the SQL string
SQL_QUERY_TIMEOUT	Integer 0=No timeout	The number of seconds to wait for a SQL statement to execute before canceling the query When set to 0 (the default) there is no timeout. If the specified timeout exceeds the maximum timeout in the data source, or is smaller than the minimum timeout, the driver substitutes that value.
Integer	Driver Specific	Driver-specific option values can be specified in the form *number=value*. For example, 4322=1, 234=String

Using Select Multiple List Boxes in HTML Forms

When an HTML form containing a <SELECT MULTIPLE...> tag is used, the Internet Database Connector converts the items selected into a comma-separated list; the list can be used in the .idc file just like other parameters. However, because the parameter is actually a list, it will typically only be used for SQLSelect statements with an IN clause, as in the following examples.

If the parameter name in the .idc file is enclosed in single quotation marks, each element of the list will be enclosed in single quotation marks also. You should enclose the parameter name in single quotation marks whenever the column in the IN clause is a character column or other type in which literals are quoted (dates and times, for example). If there are no single quotation marks around the parameter name, no quotation marks will be placed around each element of the list. You should not enclose the parameter name in single quotation marks when the column in the IN clause is a numeric type or any other type in which literals are not enclosed in single quotation marks

For example, if an HTML form contained the multiple-choice list box shown below.

```
<SELECT MULTIPLE NAME="region">
<OPTION VALUE="Westerr">
<OPTION VALUE="Easterr">
<OPTION VALUE="Northern">
<OPTION VALUE="Southern">
</SELECT>
```

You can construct an .idc file with an SQL statement

```
SQLStatement:+ SELECT * FROM Pubs WHERE region IN ('%region%')
```

If the user selected "Northern," "Western," and "Eastern" from the HTML form, the SQL statement would be converted to.

```
SELECT * FROM Pubs WHERE region IN ('Northern', 'Western', 'Eastern')
```

Another example of an HTML form is shown below, but this time uses numeric data, and therefore no quotation marks enclose the parameter in the idc file.

```
<SELECT MULTIPLE NAME="
<OPTION VALUE="1994">
<OPTION VALUE="1995">
</SELECT>
```

You can construct an idc file with an SQLStatement

```
SQLStatement: SELECT * FROM Pubs WHERE year IN (%year%)
```

If the user selected "1994" and "1995" from the HTML form, the SQL statement would be converted to

```
SELECT product, sales_year FROM sales WHERE sales_year IN (1994, 1995)
```

Using Batch Queries and Multiple Queries

In an .idc file, you can group SQL queries in two ways, as batch queries or as multiple queries.

Batch Queries

If you are querying databases that can simultaneously process several queries in a SQL statement (such as SQL Server database), you should format your statements in batch query syntax to optimize performance For example:

```
SQLStatement:
+insert into perf(testtime, tag) values (getdate(), '%tag%')
+SELECT au_lname, ytd_sales from pubs.dbo.titleview where ytd_sales>5000
+SELECT count(*) as nrecs from pubs.dbo.titleview where ytd_sales>5000
```

Multiple Queries

If you are querying databases that cannot process a series of SQL queries simultaneously, then formulate your queries as multiple queries For example:

```
SQLStatement:
+insert into perf(testtime, tag) values (getdate(), '%tag%')
SQLStatement:
+SELECT au_lname, ytd_sales from pubs.dbo.titleview where ytd_sales>5000
SQLStatement:
+SELECT count(*) as nrecs from pubs.dbo.titleview where ytd_sales>5000
```

Batch queries are processed together at once, whereas multiple queries are processed one at a time. Therefore, you will get better performance by formatting your queries as a batch if your database can handle batch queries

HTML Extension (.htx) Files

HTML extension files contain a number of keywords that control how the output HTML document is constructed. These keywords are explained in the following sections.

<%begindetail%>, <%enddetail%>

The <%begindetail%>, <%enddetail%> keywords surround a section of the HTML extension file in which the data output from the database will be merged. Within the section, the column names delimited with <% and %> or <!--%%-->are used to mark the position of the returned data from the query. For example

```
<%begindetail%>
<%au_lname%> <%ytd_sales%>
<%enddetail%>
```

will list the columns au_lname and ytd_sales. Any column can be referred to in this way. Column names can also be referred to elsewhere in the HTML extension file.

Note If there are no records returned from the query, the <%begindetail%> section will be skipped. For each SQL statement that generates a result set (for example, SELECT), there should be a corresponding <%begindetail%> <%enddetail%> section in the .htx file.

<%if%>, <%else%>, <%endif%>

HTML extension files can contain conditional logic with an if-then-else statement to control how the Web page is constructed. For example, one common usage is to insert a condition to display the results from the query on the first row within a <%begindetail%> section; but if there are no records returned by the query, to display the text "Sorry, no authors had YTD sales greater than" **%idc.sales%** By using the <%if%> statement and a built-in variable called "CurrentRecord" you can tailor the output so that the error message is printed when no records are returned Here is an example showing the use of the <%if%> statement.

```
<%begindetail%><%if CurrentRecord EQ 0 %>

Query results

<B>Author YTD Sales<B>
<%endif%>
<%au_lname%><%ytd_sales%>
<%enddetail%>
<P>
<%if CurrentRecord EQ 0 %>
<I><B>Sorry, no authors had YTD sales greater than <%idc.sales%>.</B>
<P>
<%else%>
<H5>
<I>
The Web page you see here was created by the results of the SQL query with the
template file Sample.htx.
<P>
The merge was done by the Microsoft Internet Database Connector and the results were returned
to this Web browser.
</I>
<%endif%>

</BODY>
</HTML>
```

The general syntax is.

```
<%if condition%>
HTML text
<%else%>
HTML text
<%endif%>
```

Where *condition* is of the form

value1 operator value2

and *operator* can be one of the following

EQ	if *value1* equals *value2*
LT	if *value1* is less than *value2*
GT	if *value1* is greater than *value2*
CONTAINS	if any part of *value1* contains the string *value2*

The operands *value1* and *value2* can be column names, one of the built-in variables (CurrentRecord or MaxRecords, see below), an HTTP variable name (see following), or a constant. When used in an <%if%> statement, values are not delimited with <% and %> For example, to do special processing on author name "Green," use the condition:

```
<%begindetail%>
<%if au_lname EQ "Green"%>
this guy is green!
<%endif%>
<%enddetail%>
```

The <%if%> statement can also be used to do special processing based on information from HTTP variables For example, to format a page differently based on the type of client Web browser you could include the following in the HTML extension file

```
<%if HTTP_USER_AGENT contains "Mozilla"%>
client supports advanced HTML features.
<%else%>
client is <%HTTP_USER_AGENT%>
<%endif%>
```

CurrentRecord, MaxRecords

The CurrentRecord built-in variable contains the number of times the <%begindetail%> section has been processed The first time through the <%begindetail%> section, the value is zero Subsequently, the value of CurrentRecord changes every time another record is fetched from the database.

The MaxRecords built-in variable contains the value of the MaxRecords field in the Internet Database Connector file MaxRecords and CurrentRecord can only be used in <%if%> statements

Parameters from Internet Database Connector files

Parameters from Internet Database Connector files can be accessed in the HTML extension file by prefixing the name of the parameter with "idc" and a period In Sample3.htx shown earlier, you could show the value of the parameter %sales% by including the line

HTTP variables

Several variables in HTML extension files can give a lot of information about the environment and Web client connected to the server In addition all headers sent by the client are available To access them by using the Internet Database Connector you must convert them

1. Add HTTP_ to the beginning.
2. Convert all dashes to underscores.
3. Convert all letters to uppercase.

The following table gives a listing of default variables. These are environment variables for CGI applications and HTTP variables for IDC applications.

Internet Information Server Variables

Variable	Meaning
ALL_HTTP	All HTTP headers that were not already parsed into one of the listed variables. These variables are of the form HTTP_<*header field name*>, for example: HTTP_ACCEPT */*, q=0.300, audio/x-aiff, audio/basic, image/jpeg, image/gif, text/plain, text/html HTTP_USER_AGENT: Microsoft Internet Explorer/0 1 (Win32) HTTP_REFERER: http://webserver/samples/dbsamp/dbsamp3.htm HTTP_CONTENT_TYPE application/x-www-form-urlencoded HTTP_CONTENT_LENGTH 10
AUTH_TYPE	The type of authorization in use. If the user name has been authenticated by the server, this will contain Basic. Otherwise, it will not be present.
CONTENT_LENGTH	The number of bytes that the script can expect to receive from the client.
CONTENT_TYPE	The content type of the information supplied in the body of a POST request.
GATEWAY_INTERFACE	The revision of the CGI (Common Gateway Interface) specification with which this server complies
HTTP_ACCEPT	Special-case HTTP header. Values of the Accept: fields are concatenated, separated by a comma (,); for example, if the following lines are part of the HTTP header: accept */*, q=0.1 accept: text/html accept image/jpeg then the HTTP_ACCEPT variable will have a value of: */*, q=0 1, text/html, image/jpeg
LOGON_USER	The user's Windows NT account
PATH_INFO	Additional path information, as given by the client. This comprises the trailing part of the URL after the script name but before the query string (if any).
PATH_TRANSLATED	The value of PATH_INFO, but with any virtual path name expanded into a directory specification.
QUERY_STRING	The information that follows the question mark (?) in the URL that referenced this script.
REMOTE_ADDR	The IP address of the client.
REMOTE_HOST	The hostname of the client.
REMOTE_USER	The user name supplied by the client and authenticated by the server.
REQUEST_METHOD	The HTTP request method
SCRIPT_NAME	The name of the script program being executed.
SERVER_NAME	The server's hostname (or IP address) as it should appear in self-referencing URLs.
SERVER_PORT	The TCP/IP port on which the request was received.
SERVER_PORT_SECURE	The value of 0 or 1 The value 1 indicates the request is on the encrypted port.
SERVER_PROTOCOL	The name and version of the information-retrieval protocol relating to this request, usually HTTP/1.0.
SERVER_SOFTWARE	The name and version of the Web server under which the Internet Server Extension is running
URL	The URL of the request

Contents | Index | ◁ | △ | ▷

CHAPTER 9

Using the FTP and Gopher Services

In addition to the WWW service, Microsoft Internet Information Server provides two additional services: File Transfer Protocol (FTP) and gopher. These services are "legacy" services on the Internet, meaning that they are older protocols. However, far from being outdated, these services' simplicity is often a compelling reason to consider using them in your Web site.

This chapter explains:

- The FTP and gopher services and how they work.
- When to use the FTP and gopher services
- How to configure the services.

What is the FTP Service?

FTP was one of the earliest protocols used on TCP/IP networks and the Internet. FTP is used to transfer files from one computer on a network to another computer on the same network. FTP was especially useful for transferring files between different computers, such as transferring files from a UNIX® computer to a computer running MS-DOS® or Windows 3.1

Early FTP client software was character based, and was similar to using the Windows NT command prompt to list and copy files. A character-based program was used to log on to the remote computer, browse directories, and to then transfer files.

Internet Explorer simplifies this process by automatically logging you onto the FTP server if anonymous connections are permitted. Directory listings are automatically displayed as hypertext links, permitting point-and-click simplicity in traversing directories and copying files from a server to a client. (Note that you cannot copy files from a client to a server by using Internet Explorer.)

When Should I Use the FTP Service?

The protocol used for the World Wide Web (WWW), Hypertext Transfer Protocol (HTTP), has replaced most functions of FTP. However, of the three Internet services only FTP can be used to copy files from a client computer to a server computer. If your remote users need to do this, they must use FTP.

Also, if you have existing files that you want to make available to remote users, FTP is an extremely easy service to install and maintain. After installation, point the FTP service to your files; no additional configuration is necessary

Files made available through FTP can be in any format, such as document files, multimedia files, or application files. If your remote clients are using Internet Explorer, the clients can specify whether to copy the file or to start a helper application to immediately display or play the file.

How Does the FTP Service Work?

The FTP service requires that users log on to use the service. Once logged on, users can navigate the directories made available to the FTP service. Dedicated FTP clients allow remote users to copy files to the FTP site and issue other FTP commands, including logging off.

Configuring Session Activity

You can configure the number of simultaneous connections allowed, and the amount of time allowed for connections

Because users are logged on until they log off or break the connection, you can use the **Connected Users** button in the **Service** property sheet to keep track of which users are currently connected.

Viewing Current Sessions

To see users currently connected to your FTP site

1. In Internet Service Manager, double-click the FTP service to display its property sheets
2. Click the **Service** tab
3. Click **Current Sessions**
4. If you want to disconnect a user, select the user and then click **Disconnect**. To disconnect all connections, click **Disconnect All**
5. Click **Close** and then click **OK**

Configuring FTP Logon

You use Internet Service Manager to configure logon requirements for the FTP service.

If the FTP service is configured for anonymous logon, clients can log on with the user name "anonymous." Traditionally, anonymous FTP users log on using their e-mail addresses as passwords. Note that Internet Explorer and other Web browsers automatically log on anonymously to all FTP sites that permit anonymous logon.

FTP clients are also permitted to log on with a Windows NT user name and password permitted to use that computer. On Windows NT File System (NTFS) drives, you can control every user's access permissions and file access. To use this mechanism to log on with a Web browser, type **ftp://***user:password@computername/* or **ftp://***username@computername/*

In Internet Service Manager **FTP Service Properties**, select the **Allow only anonymous connections** check box to prevent users from using user names With this check box enabled, any account other than "anonymous" cannot log on. This is useful for security because only one account, that assigned for anonymous logon, is permitted access; intruders cannot attempt to gain access with the administrator account.

Controlling Anonymous Connections

To set user name and password security

1. In Internet Service Manager, double-click the FTP service and then click the Service tab to display that property sheet

2. In the **Allow Anonymous Connections** box, type the user name and password that you want the FTP service to use when accessing resources on behalf of a client

   This account must be a valid account set up in the Windows NT User Manager. Permissions assigned to this account apply to all anonymous logons.

3. Select the **Allow only anonymous connections** check box if you want to deny access to any non-anonymous logons

   This option is handy if you do not want users to log in with their own user names and passwords because FTP passwords are unencrypted However, all users will have the same access privilege, as defined by the anonymous account. By default, this option is not enabled. Select this option if users should not connect by using their Windows NT user accounts

4. Click **OK**

Customizing Messages

To customize Welcome, Exit, and Maximum connections messages

1. In Internet Service Manager, double-click the FTP service to display its property sheets.

2. Click the **Messages** tab.

3. In the **Welcome message** box, type the welcome message you want to display when users connect.

4. In the **Exit message** box, type the message you want to display when users disconnect.

5. In the **Maximum connections message** box, type the message you want to display when a user tries to connect but cannot because the maximum number of users are already connected.

6. Click **Apply** and then click **OK**.

Configuring FTP Directories

This section describes how to configure your FTP directories.

Setting the Home Directory

By default, all subdirectories are available in the home directory You should place all your FTP files in the home directory For information about setting and changing your home directory, see Chapter 6, "Planning Your Content Directories and Virtual Servers "

You can also add virtual directories, just as with the WWW service; however, because of FTP's technical limitations as an older protocol, virtual directories are not visible to users Users can browse a virtual directory only if they know the alias of the virtual directory

Setting Listing Style

Some browsers require that the FTP listing be styled in UNIX format. You should set the FTP listing style to UNIX format for maximum compatibility with browsers

To determine how directory listings are displayed

1. In Internet Service Manager, click the **Directories** tab

2. In the **Directory Listing Style** box, select

   UNIX to display directories in UNIX format

   MS-DOS to display directories in MS-DOS format

Setting Read and Write Permission

Read permission is set for all FTP virtual root directories by default Setting Write permission allows users to place files on your computer

Remove Read permission and set Write permission to create a dedicated folder (directory) to which users can copy files but cannot see any files left by others. Such a directory is sometimes referred to as a "drop-box" directory.

You must set Read and Write permission by using Internet Service Manager. On NTFS drives you may also set additional permissions and restrictions using Windows NT Explorer.

Read

In order for an FTP client to be allowed to see a directory in a directory listing and Get (download) files from that directory, the Read permission must be set for that directory.

Read permission is set for all FTP virtual root directories by default Remove Read permission and set Write permission to create a dedicated directory to which users can copy files, but cannot see any files left by others

Write

In order for an FTP client to be able to Put (upload) files into a directory, the Write permission must be set for that directory. If a directory has the Write permission enabled and the Read permission disabled, the directory will not appear in directory listings — but an FTP client can change to the directory, assuming that the user knows the name of the directory. Files can then be uploaded into the directory.

Setting Write permission will allow users to place files on your computer.

Note On NTFS drives, it remains necessary to grant the users you want to use the "drop-box" directory Read access by way of **Directory Permissions** in Windows NT Explorer so that these users are able to change into the "drop-box" directory (using the FTP **cd** command, for example). Thus, these users must have both NTFS Read and Write permissions in Windows NT Explorer, but they should have only Write permissions in Internet Service Manager.

Creating Annotation Files

Each directory can contain an annotation file, which can be used to summarize the information that the directory contains This summary appears automatically to remote browsers

You can add directory descriptions to show FTP users the contents of a particular directory on an FTP site. This is done by creating a file called ~ftpsvc~.ckm in that folder (directory). Usually you want to make this a hidden file so that directory listings do not display it

You can add directory descriptions to inform FTP users of the contents of directories on an FTP site.

To annotate files

1. Create a file called ~ftpsvc~.ckm in each directory where you want to annotate with the information to be displayed to the user

2. In the Windows NT Explorer, select the file and make it a hidden file so that directory listings do not display this file.

3. From an FTP client, type **Site ckm** at the command prompt, or use the Registry Editor to enable annotated directories by adding the following value:

```
HKEY_LOCAL_MACHINE\SYSTEM
 \CurrentControlSet
  \Services
   \MSFTPSVC
    \Parameters
```

AnnotateDirectories REG_DWORD
Range: 0 or 1 Default = 0 (false — that is, directory annotation is off).
The preceding value defines the default behavior of directory annotation for newly connected users. Directory descriptions are used to inform FTP users of the contents of a directory on an FTP site The directory description is saved in a file named ~ftpsvc~.ckm, which is usually a hidden file. When this value is 1, directory annotation is enabled. This registry entry does not appear by default in the registry, so you must add an entry if you want to change its default value.

Client Errors Browsing FTP, Directory Annotation Enabled

If directory annotation is enabled on your FTP service, Web browsers may display error messages when browsing your FTP directories. You can eliminate such errors by limiting each annotation file to one line or by disabling directory annotation.

Special Directories in the Home Directory

You can add special directories to the home directories to control the default directory displayed to FTP users These directories must be physical subdirectories; they cannot be specified by using virtual directories.

Note The preceding does not apply when gaining access to FTP by using a Web browser, Web browsers automatically change to the root directory when logging on However, this does not preclude the user from from changing to the special directory by using the **cd** command

Using User Name Directories

User name directories are directories in the home directory with names that match a user name If a user logs on with a user name that has a matching directory in the home directory, that directory is used as the root

You can use FTP user name directories to control the root directory presented to users. FTP user name directories are not created by default during setup.

Using the Anonymous Directory

The Anonymous directory is a directory in the home directory named "Anonymous." If a user logs on by using the user account Anonymous, the directory name Anonymous is used as the root directory.

Note You can restrict access to a directory to a specific user by using **Directory Permissions** for that directory in Windows NT Explorer Each user must also have access to the Ftproot home directory.

FTP Clients

You can use any FTP client to connect to the computer running the FTP service. Windows NT Workstation and Windows NT Server include a character-based FTP client (this client can be started only at the command prompt).

Microsoft Windows NT includes Internet Explorer, which you can use to browse FTP sites. You use a Uniform Resource Locator (URL) to connect to an FTP site; for example, ftp://ftp.microsoft.com/.

What is the Gopher Service?

Although the gopher service is similar to FTP because it allows you to easily publish existing archives of files, the gopher service overcomes some limitations of the FTP service. With the gopher service, you can create links to other computers or services, annotate your files and directories, and create custom menus

The Microsoft Internet Information Server gopher service supports all gopher features. In addition, the gopher service supports Gopher Plus selector strings, which allows the server to return additional information to the client, such as administrator name, modification date, and MIME type.

To set up a gopher site, copy your files to the gopher home directory (\Inetpub\Gophroot). Clients can then browse the gopher directories as easily as using Windows NT Explorer. To enhance your site you can create tag files that provide links to other computers or services, to annotate your files and directories, and to create custom menus See "Tag Files," later in this chapter, for more information.

Configuring the Gopher Service

This section gives you an overview of configuring the gopher service To configure your

service you should configure the following:

- The directory or directories from which documents will be published. See Chapter 6, "Planning Your Content Directories and Virtual Servers" for information about setting up directories.
- Items that the gopher service will make available under a specified directory tree.
- Tags and how they are to be stored.
- Indexes to speed up searches
- Activity-log records. For information about logging see Chapter 7, "Logging Server Activity"
- Number of simultaneous connections allowed and the amount of time allowed each connection.

Controlling Security by User Name and Password

To set user name and password security

1. In Internet Service Manager, double-click the gopher service to display its property sheets and then click the **Service** tab.
2. In the **Anonymous Logon** box, type the user name and password that you want the gopher service to use when accessing resources on behalf of a gopher client

   By default IUSR_*computername* is used for anonymous logons. You can also use any valid Windows NT account set up in the Windows NT User Manager
3. Click **OK**

Setting up WAIS Index Queries

Wide Area Information Search (WAIS) index searching is not enabled by default in Internet Information Server To enable WAIS, you must change the following entry in the Windows NT registry from 0 (disabled) to 1 (enabled)

Tag Files

Tag files can be used to supplement the standard gopher display returned to clients with additional information and to provide links to other computers

All information about a file that is sent to a client comes from tag files. This information includes the name of a file displayed for the client. Typical tag files contain:

- Display name
- Host name
- Port number

If you are running Gopher Plus client, you can add more information to each tag file, such as the server administrator's name and e-mail name, the file's date of creation, and date of last modification.

You must first create the file and then store it on the gopher server, which is the computer running the gopher service.

You create tags for your gopher site with the **gdsset** utility. To see the complete syntax of the **gdsset** command, type **gdsset** at the command line with no parameters.

Tag files are hidden files. Use Windows NT Explorer to set the hidden attribute for tag files

On drives formatted using the file allocation table (FAT) file system, the tag file name is the same as the file it describes, with .gtg appended to the file name. For example, if the content file name is Catalog.txt then the tag file name would be Catalog.txt.gtg.

On drives formatted using NTFS, the tag file name is the same as the file it describes with :gtg appended to the file name NTFS tag files are stored in an alternate data stream. For example, if the content file name is Catalog.txt then the tag file name would be Catalog.txt.gtg Note that a colon rather than a period is used to start the extension.

Tag files stored on FAT volumes can be edited by using most ASCII-based text editors, such as Notepad. The file may need to be unhidden to edit it. Tag files stored on NTFS volumes cannot be edited by most text editors because the file is stored in an alternate data stream.

Note that if your computer is configured for FAT, you must move the tag file manually when you move the corresponding data files To move the tag file, first make it visible, because tag files are hidden files Then move the file, and make hidden it again (You can use Windows NT Explorer to make files hidden or visible, to show all files, including hidden files, in the **View** menu, click **Options**, click the **View** tab, then select **Show all files**)

Note If disk space is critical, make sure that you include the hidden tag files when you calculate how much space your files will take up

Creating Tag Files

To create a tag file

- Type the following syntax on the command line:

  gdsset -c -g*n* -f "*description of file*" -a "*administrator's name*" -e *e-mail filename*

  where

  - -c Use this flag to edit or create a new file.
  - -g*n* The value for *n* can be any single-digit code from 0 to 9 If you omit this flag, the code for the file type will default to 9, binary.
  - -a "*administrator's name*" The value between the quotation marks is the administrator's name. If you omit this flag, the value defaults to the service administrator's name in the Service dialog box of the Microsoft Internet Service Manager.
  - -e *-e-mail* The value is the administrator's e-mail address. If you omit this flag, the value defaults to the service administrator's e-mail name in the Service dialog box of the Microsoft Internet Service Manager
  - *filename* The value is the name of the tag file you're creating or editing

This command line automatically hides the tag files you create

To create a batch command to tag a series of files that have the same type, such as a series of text files, use the following syntax.

[illegible]

To create a link from your local gopher site to a directory on another computer

- Run the **gdsset** command with the following syntax

  gdsset -c -g*n* -f "*file description*" -a "*administrator's name*" -e *e-mail* -h *hostname filename*

  where

  - -c Edits or creates a new file
  - -g*n* The value for *n* can be any single-digit code from 0 to 9 If you omit this flag, the code for the file type will default to 9, binary For a list of type codes, see "Interpreting Item Types"
  - -f "*file description*"

    A synopsis of the contents of the file

- -a "*administrator's name*"

  The value between the quotation marks is the administrator's name. If you omit this flag, the value defaults to the service administrator's name in the Service dialog box of the Microsoft Internet Service Manager.

- -e *e-mail*

  The value is the administrator's e-mail address. If you omit this flag, the value defaults to the service administrator's e-mail address in the Service dialog box of the Microsoft Internet Service Manager.

- -h *hostname* The value specifies the name of the computer to link to.

- *filename*

  The value is the name of the file for which you want to create a tag file.

Gdsset automatically hides the tag files you create.

The following command displays information stored in a tag file

gdsset -r *filename*

To create a batch command to tag a series of files that have the same type, such as a series of text files, use the following syntax

for %i in (* txt) do <echo %i && gdsset -c -g0 -f %i %i

Interpreting Item Types

The following list shows all possible gopher item type codes and what they mean The first character is the type code

0	A file, usually a flat text file.
1	A gopher directory.
2	A CSO phone-book server.
3	An error.
4	A Macintosh® file in Binhex format.
5	An MS-DOS binary archive.
6	A UNIX Uuencoded file.
7	An index-search server.
8	A Telnet session.
9	A binary file.
c	A calendar or calendar of events.
g	A graphic interchange file (GIF) graphic.
h	An HTML World Wide Web hypertext page.
i	An in-line text that is not an item.
I	Another kind of image file.
m	A BSD format mbox file.
P	A PDF document.
T	A TN3270 mainframe session
:	A bitmap Image (use Gopher Plus information for type of image).

Contents Index

CHAPTER 10

Configuring Registry Entries

The configuration registry stores values that define the working environment for the Windows NT operating system and any services installed on the computer running Windows NT. Usually, to change these values, you use graphical tools, such as Control Panel, Windows NT Setup, or Internet Service Manager. Windows NT also includes a utility, the Registry Editor (Regedt32.exe), which you can use to inspect and modify the configuration registry directly

You can configure the Internet services by using Internet Service Manager. The services also use several additional configuration parameters in the registry not configured by using Internet Service Manager. Parameters are either specific to a service or are global to Internet Information Server and all services

Wherever possible, you should use Internet Service Manager to make changes to your Internet server settings For a registry change to take effect, you must restart the service affected by the change. For global entries you must restart all services .

See the following sections for entries in this chapter They show the values used by Internet Information Server.

- Global Entries
- Service-Specific Entries with Common Names
- WWW Service Entries
- FTP Entries

- Gopher Entries
- Setup Entries

The following sections help you configure the registry for your specific needs:

- Server Multipurpose Internet Mail Extensions (MIME) Mapping
- Associating Interpreters with Applications (Script Mapping)
- Adding Virtual Directories

Before you modify the registry, it is strongly recommended that you read Part IV of the *Windows NT Resource Guide* (found in the Microsoft Windows NT Resource Kit). This part of the book describes in detail how to use and change parameters in the registry.

Caution Using the Registry Editor incorrectly can cause serious problems, including corruption that may make it necessary to reinstall Windows NT or Microsoft Internet Information Server. Using the Registry Editor to edit entries in the registry is equivalent to editing raw sectors on a hard disk. If you make mistakes, your computer's configuration could be damaged. You should edit registry entries only for settings that you cannot adjust through the user interface, and be very careful whenever you edit the registry directly

---

Creating Registry Entries

This chapter documents registry keys installed by default as well as those you can create When you install Internet Information Server, the following registry keys are installed by default You must create any keys that do not appear in this list.

Registry Keys Installed by Default

AdminEmail	ExitMessage	LogNonAnonymous
AdminName	GreetingMessage	LogSqlDataSource
AllowAnonymous	InstallPath	LogSqlPassword
AllowGuestAccess	LogAnonymous	LogSqlTableName
AnonymousOnly	LogFileDirectory	LogSqlUserName
AnonymousUserName	LogFileFormat	LogType
ConnectionTimeOut	LogFilePeriod	MaxClientsMessage
EnablePortAttack	LogFileTruncateSize	MaxConnections

Global Registry Entries

These parameters are used for global control of the Internet services.

Registry Path:

```
HKEY_LOCAL_MACHINE\SYSTEM
 \CurrentControlSet
  \Services
   \InetInfo
    \Parameters
```

BandwidthLevel REG_DWORD

Range: 0 - 0xFFFFFFFF
Default: 0xFFFFFFFF

Specifies the maximum network bandwidth used for Internet Information Server. This helps to prevent overloading the network with Internet Information Server activity. For example, for administrators of small corporate servers, where a single server is used for multiple sites, this will help to reduce network usage for Internet Information Server servers. It is recommended that this parameter be set from Internet Service Manager. Otherwise, the server must be stopped and restarted for this value to take effect. The value 0xFFFFFFFF means "Do not restrict bandwidth."

CacheSecurityDescriptor REG_DWORD

Range: 0 - 1
Default: 0

Specifies whether security descriptors are cached for file objects. If enabled (with the value of 1), Internet Information Server retrieves security permissions when caching a file object and will not need to gain access to the file object to check access rights for new users. This feature is useful only if you have more than one user account (not using anonymous only). By default Internet Information Server does not cache security descriptors, but checks the access rights against the file object for new user accounts

DisableMemoryCache REG_DWORD

Range: 0 -1
Default: 0

Disables server caching This key cannot be configured through the Internet Service Manager If you change this setting, stop the server and restart it for the change to take effect.

ListenBackLog REG_DWORD

Range: 1-unlimited
Default: 15

Specifies the maximum number of active connections to hold in the queue waiting for server attention. Enhanced Internet Information Server functionality generally makes it unnecessary to use or modify this entry, although extremely heavy use might benefit by increasing this value up to 50.

LogFileBatchSize REG_DWORD

Range: 0 - 0xFFFFFFFF
Default: 64*1024 (64 KB)

Specifies the batch size for writing a log file. The server caches the last LogFileBatchSize bytes of data in memory buffers before it dumps the current buffer to disk. Such batch processing reduces the amount of disk traffic created by log files. In some instances, you may need to reduce the time between writing the buffer to disk. To change the default setting you must add this value to the key using the new setting.

MaxConcurrency REG_DWORD

Range: 0 - 0xFFFFFFFF
Default: 0

Specifies the amount of concurrency that a system should provide. We use completion ports for handling input-output (I/O) In general it is not good to have more than one thread running and conflicting on shared memory or locks. This key specifies how many threads per processor should be allowed to run simultaneously if there is a pending I/O operation. The specific value of 0 allows system to make intelligent choice of the number of threads to use. Any nonzero value specifies that the system should allow that many threads per processor to run simultaneously.

MaxPoolThreads REG_DWORD

Range: 0 - 0xFFFFFFFF
Default: 10

Specifies the number of pool threads to create per processor. Each pool thread watches for the network request and processes it. Generally, it is not good to create more than 20 threads per processor.

MemoryCacheSize REG_DWORD

Range: : 0 - 0xFFFFFFFF
Default: : 3072000 (3MB)

Internet Information Server caches system handles, directory listings, and other values of frequently used data to improve performance of the system This parameter specifies the amount of memory in bytes to allocate for that cache When this value is changed, the server must be stopped and restarted for this to take effect. A value of 0 means "Do not do any caching." The performance may be low when caching is off. Sites with heavy traffic can increase this size, provided there is sufficient RAM on the computer.

MinFileKbSec REG_DWORD

Range: 1 - 8192
Default: 1000

When a Web server sends a file to the client, a timeout is established for how long the server will allow the transfer to continue before ending it The timeout chosen is the maximum of the Connection Timeout specified in the Internet Service Manager plus the size of the file divided by the value specified as MinFileKbSecs For example, a file size of 100 kilobytes is given a timeout of 100 seconds, or the Connection Timeout if the latter is greater Note that the registry name is misleading, because the value is in *bytes*, not kilobytes as the name might imply

ObjectCacheTTL REG_DWORD
Range: 0 - 0x7FFFFFFF, 0xFFFFFFFF (seconds) Default: 30 seconds
This registry entry controls the Time To Live (TTL) setting, which defines the length of time that objects are held in cached memory. If an object in the memory cache has not been referenced for the defined period, that object will be phased out of the cache. If system memory is limited or the server's contents are dynamic, you can use a lower TTL to prevent system memory from being used to cache a large number of volatile objects. Setting the value to 0xFFFFFFFF disables the object-cache scavenger and allows cached objects to remain in the cache until they are overwritten. Disabling the cache is useful if your server has ample system memory and your data is relatively static.

PoolThreadLimit REG_DWORD
Range: 0 - 0xFFFFFFFF Default: 2 * # MB
Specifies the maximum number of pool threads that can be created in the system. Each pool thread watches for the network request and processes it.

ThreadTimeout REG_DWORD
Range: 0 - 0xFFFFFFFF Default: 24*60*60 (24 hours)
Specifies the amount of time an input-output processing thread should be maintained even if there is no I/O activity on the system. In general when there is no I/O activity and no requests outstanding the server is idle and does not consume memory. But if that situation prolongs and exceeds the ThreadTimeout interval, then the thread is stopped. Units are in seconds.

UserTokenTTL REG_DWORD
Range: 0 - 0x7FFFFFFF Default: 15 * 60 (10 Minutes)
When a request is made to the server, the security credentials for the request (or the configured anonymous user) are used to create a user token on the server which the server impersonates when accessing files or other system resources. The token is cached so that the Windows NT logon only takes place the first time the user accesses the system or after the user's token has fallen out of the cache. Windows NT Challenge/Response authentication tokens are *not* cached. Units are in seconds

Service-Specific Registry Entries with Common Names

The following parameters are stored in the registry by service, for service-specific behavior, but have the same name for each service

Registry Path

```
\CurrentControlSet
 \Services
  \ServiceName
   \Parameters
```

where *ServiceName* is

MSFTPSVC	**FTP Service**
GOPHERSVC	gopher Service
W3SVC	WWW Service

AdminName REG_SZ
Range: String Default: Administrator
Specifies the user-friendly administrator name. The gopher service uses this name to send back responses for Gopher Plus queries. This parameter also serves as a way of identifying who administers a service.

AdminEmail REG_SZ
Range: String Default: Admin@corp.com
Specifies the e-mail address for the administrator of a particular service. The gopher service uses this name to send back responses for Gopher Plus queries.

ServerComment REG_SZ
Range: String Default: ""
Specifies a user-friendly comment for a service. This information is used to add a configurable comment in Internet Service Manager.

EnableSvcLoc REG_DWORD
Range: 0, 1 Default: 1
The Internet Information Server services register themselves with a service locator so that the service can be discovered by Internet Service Manager. This parameter controls such registration. If set to 0, the service will forgo registration. Set to 1, it registers the service for service location. To change the default setting, you must add this value to the key using the new setting.

AllowAnonymous REG_DWORD
Range: 0, 1 Default: 1
Specifies if an anonymous user should be allowed to connect and make a request to the server. By convention, most Internet services allow anonymous connections to gain access to files.

AnonymousUserName REG_SZ
Range: String Default: Guest
Specifies the name of the local user account to use for anonymous users. All server actions associate a user name and password with the action. This parameter should not be changed in the registry. You must change this parameter by using Internet Service Manager so that the appropriate password can also be set. The password is stored in protected area in the registry.

ConnectionTimeOut REG_DWORD
Range: 0-0xFFFFFFFF Default: 600 seconds
Specifies the time the server should maintain a connection when there is no activity.

DefaultLogonDomain REG_SZ
Range: string Default: *domainname*
Specifies the default logon domain that validates a clear-text logon when no domain is specified in the user name field. The default value is the domain name for servers that are domain controllers or the name of the local computer (if stand-alone).

LogonMethod REG_DWORD
Range: 0, 1, 2 Default: 0
Specifies the logon method for clear-text logons. A value of 0 means that users must have the right to log on locally to be given access to the server. A value of 1 means that users must have the right to log on as a batch job A value of 2 means that users will be logged on as network, which means they must have the user right to access the local computer from a network, which you can set in the Windows NT User Manager for Domains. If you are running SQL Server through an ODBC connector with "SQL Integrated Security" enabled, you need to set this value to either 0 or 1. If this key is not in the registry, the default value is 0.

LogFileDirectory REG_EXPAND_SZ
Range: String Default: %systemroot%\system32\logfiles
Specifies the directory in which log files are to be stored. Each service generates a log record for each request processed

LogFileFormat REG_DWORD
Range: 0, 3 Default: 0
Specifies the format for in which entries are recorded in a text file. The value 0 (the default) indicates Standard format. The value 3 indicates National Center for Supercomputing Applications (NCSA) Common Log File format.

LogFilePeriod REG_DWORD

Range: 0,1,2,3
Default: 1

Specifies the type of log files to be produced where

0 = No period. Each log file is limited by size specified in LogFileTruncateSize.
1 = Open a new log file every day
2 = Open a new log file every week
3 = Open a new log file every month

LogFileTruncateSize REG_DWORD

Range: 0-0xFFFFFFFF
Default: 4,000,000,000 bytes

Specifies the maximum size of each log file generated. Once the specified size is reached, the logging module automatically opens a new log file. A value of 0 means "Do not truncate."

LogSqlDataSources REG_SZ

Range: String
Default: ""

This string specifies the name of the ODBC data source to use for sending the request logs for the service to a SQL-compatible database system. This data source should be a system DSN in the ODBC installation on the server.

LogSqlTableName REG_SZ

Range: String
Default: ""

Specifies the name of the ODBC table name used for sending the request logs for the service to a SQL-compatible database system The table should be created by the administrator as per the specification provided with the services The user should also have proper access permissions to insert data into the table.

LogSqlUserName REG_SZ

Range: String
Default: ""

Specifies the user name to use when accessing the ODBC data source specified for ODBC-based logging. This user must be a valid user on the server to which the LogSqlDataSource registry parameter is pointing

LogSqlPassword REG_SZ

Range: String
Default: ""

Specifies the password for establishing an ODBC connection for a particular user account on the ODBC data source The password is stored as a clear text.

LogType REG_DWORD
Range: 0, 1, 2 Default: 1
Specifies the type of logging. The type specifies the destination of log files where 0 = No logging 1 = Log to files 2 = Log to ODBC data source

MaxConnections REG_DWORD
Range: 0 - 0xFFFFFFFF. Default: unlimited
Specifies the maximum number of simultaneous connections that the server allows at any given time. When the number of current connections exceeds this value, the service rejects the request. A friendly message can be sent to the client that was refused access.

WWW Service Registry Entries

In addition to the parameters listed in "Service-Specific Registry Entries with Common Names," the WWW service maintains the following parameters

Registry Path:

```
HKEY_LOCAL_MACHINE\SYSTEM
 \CurrentControlSet
  \Services
   \W3SVC
    \Parameters
```

AcceptByteRanges REG_DWORD
Range: 0, 1 Default: 1, enabled
The value determines whether the HTTP server will process the "Range" header for type "bytes:". If enabled, the server will signal that it is accepting range requests by sending the "Accept-Range: bytes" header field, and will process an incoming request specifying a "Range: bytes=" header field according to the Internet draft "Byte range extension to HTTP."

AccessDeniedMessage REG_SZ
Range: string Default: " "
The message to send back to clients when they have been denied access to the server. Often this message will be a short HTML document, explaining how to gain access.

AllowGuestAccess REG_DWORD

Range: 0, 1
Default: 1, enabled

This flag specifies whether Guest logons are allowed for the WWW service. When a new user logs on, the server checks to see if the user is logged on as aWindows NT guest user. For a Guest connection, based on the value of this flag, the WWW service either rejects or accepts the new connection. Allowing Guest access has been known to cause problems in a poorly managed site.

Under the default installation of Windows NT systems, the Guest account is granted permissions for all types of access on the system. Because this default could easily compromise security, you should turn this switch off by changing the value to 0.

AllowSpecialCharsInShell REG_DWORD

Range: 0, 1
Default: 0, disabled

This value controls whether the Cmd.exe special characters (such as &) are allowed on the command line when running batch files (.bat and .cmd files). These special characters can pose a serious security risk. If the value of this entry is set to 1, malicious users can execute random commands on the server. Therefore, it is highly recommended to leave this setting as 0, the default.

CacheExtensions REG_DWORD

Range: 0-1
Default: 0x1

Specifies whether Internet Server API (ISAPI) extensions are cached in memory. If set to 0, ISAPI extensions are not cached. See the ISAPI documentation for more information. Use this registry entry for debugging only

CheckForWAISDB REG_DWORD

Range: 0, 1
Default: 0

The WWW service uses the Wide Area Information Server (WAIS) Toolkit to support Web-based searches Microsoft does not provide the WAIS Toolkit This flag is used to specify if search is supported and if the service should check for WAIS Toolkit. If set to 0, the service does not support searches and does not look for WAIS Toolkit. If set to 1, then the service supports searches if Waislook.exe is installed in the system.

CreateProcessAsUser REG_DWORD

Range: 0-1
Default. 1

For CGI scripts, by default the server runs the script in the context of the user making the request by using the Win32 CreateProcessAsUser API If you set this flag to 0, CGI scripts will be started with the CreateProcess API and the scripts will run in the system context. This has serious security implications because CGI scripts will have much greater access to the system than they normally would have

CreateProcessWithNewConsole REG_DWORD

Range: 0, 1
Default: 0, disabled

By default, CGI scripts are run in a detached process. If you want to run CGI scripts in a process with a new console, for example, when input/output redirection is in the script, change this setting to 1. The process will then be created using the CREATE_NEW_CONSOLE flag.

Note Creating a new console for each CGI script has serious performance implications and should not be done unless slower performance is acceptable.

DefaultLoadFile REG_SZ

Range: String
Default: Default.htm

Specifies the file to return to a client if no file is included in a client's request.

DirBrowseControl REG_DWORD

Range: see the explanation paragraph
Default: 0x4000001e

Specifies both the display attributes of directory browsing and whether the **DefaultLoadFile** is used. The value used here is arrived at by adding the hexidecimal values of the attributes listed below. The first four digits of the specified value control whether directory browsing is enabled and whether the default file is enabled. For example, the default setting 0x4000001e has directory browsing disabled but the default file is loaded. To enable directory browsing, you would add the value 0x80000000 to the default setting 0x4000001e, resulting in the value 0xc000001e To control browsing attributes, you would modify the last four digits. For example, to show only the date of files you could use the value 0xc0000002.

Behavior	Value
Load Default File	0x40000000
Directory Browsing Enabled	0x80000000
Browsing Attributes	
Show Date	0x00000002
Show Time	0x00000004
Show Size	0x00000008
Show Extension	0x00000010
Display Long Date	0x00000020

DefaultLogonDomain REG_SZ

Range: String
Default: [blank]

Specifies the default domain for logon. Leaving this value blank (the default) has the following effect: If the computer is a domain controller, the default domain is the domain name; if the computer is not a domain controller, the default domain is the computer name.

FilterDLLs REG_SZ
Range: String Default: sspifilt.dll
Comma-separated list of ISAPI filter DLLs.

GlobalExpire REG_DWORD
Range: 0x0-unlimited (seconds) Default: 0xffffffff
Specifies the time in seconds that files will be considered valid. This value is used by the server in the expires header (using Greenwich Mean Time [GMT] time) to indicate to clients how long a static file is valid. This is typically set to 0x0, to prevent the files on the server from being cached by proxies or clients

LogSuccessfulRequests REG_DWORD
Range: 0, 1 Default: 1
Determines whether or not to record successful activities in the log file. The value 1 logs successful activities, and 0 turns it off.

LogErrorRequests REG_DWORD
Range: 0, 1 Default. 1
Determines whether or not to record errors in the log file. The value 1 turns error logging on, and 0 turns it off.

NTAuthenticationProviders REG_SZ
Range: String Default: NTLM
Lists possible Windows NT authentication schemes returned to clients. Internet Information Server provides the default Windows NT Challenge/Response (NTLM) scheme enabled in the WWW Service property sheet. Third parties may provide alternate Windows NT authentication schemes in the future.

PoolIDCConnections REG_DWORD
Range: 0, 1 Default: 0
When running a series of Internet Database Connector (.idc) files, you will improve performance if you open a connection to the SQL server and keep it open, rather than opening and closing a connection each time the database is queried. To pool connections by default, set this registry entry to 1. Resetting this value to 1 will add the connection referenced in all .idc files to the connection pool. Alternatively, you can selectively choose which .idc files should have their connections pooled by using the ODBCConnection: field in the .idc file. For details, see Chapter 8, "Publishing Information and Applications." The .idc file determines whether it can use a connection from the connection pool based on data source, user name, password, and the logged-on user account specified in the .idc file. If there is an exact match between these fields in the current .idc file and the .idc file specified in the URL, a connection from the connection pool will be used.

PoolIDCConnectionsTimeOut REG_DWORD
Range. [in seconds] Default: 30
Controls how long the IDC will keep an ODBC connection in the pool before closing the connection. When the IDC pools a connection, it is potentially taking a license slot for every pooled connection. The value set for this key lets the administrator determine when license slots are released and when server resources are returned to the database server.

ReturnURLUsingHostName REG_DWORD
Range: 0, 1 Default: 0
With the default setting (0), the server returns its Internet Protocol (IP) address to a client when doing redirects if the host header field is not present. To return a host name or the computer name of the server, change this registry setting to 1. If a host name has been added in the Host Name box of the DNS dialog box, the server will then return that name; otherwise, it will return the server's computer name, which appears in the Host Name box by default. To fill in a host name, open the TCP/IP property sheet in the Network application of the Windows NT Control Panel. Click the DNS tab, and type a name in the Host Name box

ScriptMap REG_SZ

See "Associating Interpreters with Applications (Script Mapping)," later in this chapter.

ScriptTimeout REG_DWORD
Range: 0x1-0x80000000 Default: 0x384
Specifies the maximum time the WWW service will wait for a response from CGI scripts

SecurePort REG_DWORD
Range: 0x0-0xfa00 Default: 0x1bb
Specifies the TCP port to use for SSL.

ServerSideIncludesEnabled REG_DWORD
Range: 0x0-0x1 Default: 0x1
Set to 0x1, this value enables the use of Include files to permit including repetitive information in files.

ServerSideIncludesExtension REG_SZ
Range: String Default: .stm
Specifies the file extension for files that the server will scan for include statements

FTP Service Registry Entries

In addition to the parameters listed in "Service-Specific Registry Entries with Common Names," the FTP service maintains the following parameters.

Registry Path

```
HKEY_LOCAL_MACHINE\System
  \CurrentControlSet
    \Services
      \MSFTPSVC
        \Parameters
```

AccessCheck REG_DWORD
Range: <any> Default: <any>
Checks the access of incoming user connections. The server impersonates the logged-on user and attempts to open the registry key for read and write. If the key does not exist, read and write permissions are granted. If the key exists, read and write permissions are granted to the user based on the access permission on the registry key. This feature is specifically useful for servers that publish content on a FAT volume and therefore do not have the rich security features of NTFS. Because it is hard to manage and performance slows down, Microsoft does not recommend using this approach to provide security.

AllowKeepAlives REG_DWORD

Range: 0, 1
Default: 1

In some rare instances, you may want to turn off "Connection: keep-alive" negotiation with clients. Most clients support making multiple requests to the server on a TCP session, so this feature significantly decreases the workload on the server. Turning off keep-alive negotiation will have serious performance implications and should be used only when necessary.

AnonymousOnly REG_DWORD

Range: 0, 1
Default: 0

Specifies if only anonymous connections are permitted. If set to 1, only anonymous connections are permitted (especially true of FTP service). To change the default setting, you must add this value to the key using the new setting.

EnablePortAttack REG_DWORD

Range: 0, 1
Default: 0

This parameter is set by default to prevent a security problem in the FTP protocol specification. The FTP service specification allows passive connections to be established based on the port address given by client. This can allow hackers to execute destructive commands in the FTP service. The problem occurs when the FTP service connects using a port other than FTP Data port (20) and port number is less than IP_PORT_RESERVED (1024). **EnablePortAttack** controls if such an attack should be allowed By default, the service does not make any connections to port numbers lower than IP_PORT_RESERVED (other than 20). If you want to users to connect by using other ports as specified in the FTP RFC, this flag should be enabled.

ExitMessage REG_SZ

Range: String
Default: ""

The FTP service sends back an exit message when a client sends a **quit** command. This string specifies the exit message sent

GreetingMessage REG_MULTI_SZ

Range: String
Default: ""

When a new user connects to the FTP Server, the server can send a friendly welcome message detailing contents and administrative information This string (multiple lines) specifies the message to use for greeting the new client connections.

LogAnonymous REG_DWORD

Range: 0, 1
Default: 1

Controls whether a log record should be written for anonymous connections. If set to 0, no log records are written for anonymous connections

LogNonAnonymous REG_DWORD
Range: 0, 1 Default: 1
Controls whether a log record should be written for non-anonymous connections. If set to 0, no log records are written for non-anonymous connections. Only the FTP and WWW services have non-anonymous user support.

MaxClientsMessage REG_SZ
Range: String Default: ""
When the current connection exceeds the maximum connections (in the MaxConnections key) specified for the service, the service can send a friendly message to clients. This message is a single-line message.

AccessCheck REG_DWORD
Range: any Default: any
Used for access checks of incoming user connections. The server impersonates the logged-on user and attempts to open the registry key for read and write. If the key does not exist, then read and write permissions are granted. If the key exists, then based on the access permission on the registry key, read and write permissions are granted to the user. This feature is useful for servers that publish content on a FAT volume and hence do not have the rich security features of NTFS This is not a recommended approach to provide security because of poor manageability and performance. To enable this feature, you must add this value to the key using the appropriate access settings.

AllowGuestAccess REG_DWORD
Range: 0, 1 Default: 1
Specifies if guest logons are permitted for FTP service. When a new user logs on, the server checks to see if the user is logged on as Windows NT user with guest permissions. For a guest connection, based on the value of this entry, the FTP service either rejects or accepts the new connection. Permitting Guest access has been known to create problems in poorly managed sites. Under default installation of Windows NT systems, Guest is granted permissions for many types of access on the system It is recommended that administrators do not permit access by using the Guest account To change the default setting to "No access by using the Guest account," you must add this value to the key using the new setting

AnnotateDirectories REG_DWORD

Range: 0, 1
Default: 0 (FALSE)

FTP service supports annotating a directory with custom messages. The annotation text is stored in a special file named ~ftpsvc~.ckm in the directory to be annotated. If this file exists in the target directory of a Change Directory (CWD) FTP operation, then the service responds with the contents of this file for the operation. This provides a way for administrators to add custom messages for directories under consideration. By default the service is configured to not send annotation text. If you choose to add a custom message, the annotation file should be created as well as setting this value to 1. Also, it is recommended that you make the annotation file a hidden file so that the file does not appear on a directory listing.

MsdosDirOutput REG_DWORD

Range: 0, 1
Default: 1 (TRUE)

Specifies the style of directory output for a LIST operation from an FTP client. If the value is set to 1, the service generates a MS-DOS-style directory listing. If the value is set to 0, the service generates an UNIX-style listing. Some clients will not display MS-DOS-style listings. For this reason you should consider setting this value to 0. UNIX style listings consume more CPU time.

LowercaseFiles REG_DWORD

Range: 0, 1
Default: 0 (FALSE)

The FTP service uses the native case for file names (how the file names are stored in file system). However, in order for exact comparisons with case-sensitive file systems to work, it may be necessary to ensure that proper file names are used. Administrators can add this value to ensure that the service uses lowercase for such comparisons.

Realm REG_SZ

Range: *string*
Default: *Host Header or IP address*

Supplies the realm value when the server requests a client to authenticate because the client was denied access to a resource when using Basic (clear text) authentication. This value appears in the browser's user name-password prompt

UploadReadAhead REG_DWORD

Range: 0 - 0x80000000
Default: 48K

When the client posts data to the server, this is the default amount the server will read before passing control to the application. The application is then responsible for reading the rest of the data Increasing this size increases the amount of memory required on the server

UsePoolThreadForCGI REG_DWORD
Range: 0, 1 Default: 1
Internet Information Server by default uses a server pool thread to do CGI processing. This means CGI requests that take an extended period of time can consume a server pool thread. Adjusting **MaxPoolThreads** under ..\services\infocomm\parameters can make more pool threads available.

Gopher Service Registry Entries

In addition to the parameters listed in "Service-Specific Registry Entries with Common Names," the gopher service maintains the following parameters.

Registry Path

```
HKEY_LOCAL_MACHINE\SYSTEM
 \CurrentControlSet
  \Services
   \GOPHERSVC
     \Parameters
```

CheckForWAISDB REG_DWORD
Range: 0, 1 Default: 0
The gopher service uses the WAIS Toolkit to support gopher-based searches. Microsoft does not provide the WAIS Toolkit. This flag is used to specify if search is supported and if the service should check for WAIS Toolkit. If set to 0, the service does not support searches and does not look for WAIS Toolkit. If set to 1, then the service supports searches if Waislook.exe is installed in the system.

Setup Registry Entries

Internet Information Server creates the following parameters during setup These values are used by the Setup program after initial setup to determine the current configuration of Internet Information Server Note that multiple registry paths are included in this section

InstalledBy REG_SZ
Range. INetStp Default: INetStp
The presence of this entry indicates that Internet Information Server is installed.

```
INetMgr
 \Parameters
```

MajorVersion REG_DWORD
Range: 1 Default: 1
Indicates the major version number, for example, the 1 in version 1.0.

MinorVersion REG_DWORD
Range: 1-9 Default: 0
Indicates the minor version number, for example, the 0 in version 1.0.

```
HKEY_LOCAL_MACHINE\SOFTWARE
 \Microsoft
  INetMgr
   \Parameters
    \AddonServices
```

FTP REG_SZ
Range: string Default: fscfg.dll
Defines the configuration DLL used by the FTP service.

Gopher REG_SZ
Defines the configuration DLL used by the gopher service
Range: string Default: gscfg.dll

WWW REG_SZ
Range: string Default: w3scfg.dll
Defines the configuration DLL used by the WWW service.

AnonymousUser REG_SZ
Range String Default: IUSR_*computername*
Specifies the anonymous user account created during setup

InstallPath REG_SZ
Range: String Default: c:\winnt\system32\inetsrv
Specifies the installation location for Internet Information Server.

MajorVersion REG_DWORD
Range: 1 Default: 1
Indicates the major version number, for example, the 1 in version 1.0.

MinorVersion REG_DWORD
Range: 1-9 Default: 0
Indicates the minor version number, for example, the 0 in version 1.0.

```
HKEY_LOCAL_MACHINE\SOFTWARE
 \Microsoft
  InetStp
   Help
```

The presence of this entry indicates that Help is installed

```
HKEY_LOCAL_MACHINE\SOFTWARE
 \Microsoft
  \InetExplore
```

InstalledBy REG_SZ
Range: INetStp Default: INetStp
The presence of this entry indicates that Internet Explorer version 1.5 is installed.

Server MIME Mapping

If your server provides files that are in multiple formats, you must configure your server's Multiple Internet Mail Extensions (MIME) mapping to ensure your server maps the file type correctly when returning the file to remote browsers. If MIME mapping on the server is not set up for a specific file type, browsers may not be able to retrieve the file. More than 100 MIME mappings are installed by default.

To configure additional MIME mappings

1. Start the Registry Editor (Regedt32.exe) and open

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\InetInfo\Parameters\

   Note that each MIME type is a REG_SZ with the type of information as the *name* of the value with an empty value.

2. Add the value for the MIME mapping needed on your server by using the following syntax

Syntax:

```
<mime type>,<filename extension>,,<gopher type>
```

Note the double comma before the gopher type parameter.

Example:

```
text/html,htm,,1
image/gif,gif,,5
```

In this example, when clients ask the Web server for a file that ends in the extension .gif, the MIME type returned to the client would be image/gif.

The default entry with the file-name extension specified as an asterisk (*) is the default MIME type used when a MIME mapping does not exist. For example, to handle a request for the file Current vgr when the the file-name extension vgr is not mapped to a MIME type, the server will use the MIME type specified for the asterisk extension, which is the type used for binary data Usually, this will cause browsers to save the file to disk.

Associating Interpreters with Applications (Script Mapping)

With file-name extension mapping, you can map file-name extensions to the proper program to run files with those extensions The following file-name extensions are preinstalled

.bat or .cmd=C:\Winnt\System32\cmd.exe /c %s %s

.idc=C: \Winnt\System32\Inetsrv\Httpodbc.dll

For other file-name extensions, you must edit the information in the the Windows NT registry

In the .bat example above, the first %s is the mapped URL (that is, C:\InetPub\Scripts\Test.bat) The second %s represents the parameters to the URL (in other words, the query string, the second %s is used only if an equals sign is not found).

Thus, you can reference URLs such as

/scripts/test.bat?This+is+a+search

– Or –

/scripts/bugs idc?Assign=Johnl

To configure additional script mappings

1. Start Regedt**32**.exe and open

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\

2. From the **Edit** menu, choose **Add Value** The Data type is REG_SZ.

3. Type the file-name extension used for your scripts.

4. In the String editor, type the full path to the interpreter used with that script.

5. Restart the WWW service

Adding Virtual Directories by Using the Registry

You should use Internet Service Manager to manage your virtual directories. You can, however, add or modify virtual directories by using Regedt32 exe.

To add virtual directories by using the Registry Editor

1. Start Regedt**32**.exe and open

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\<*service*>\Parameter Roots

   where <*service*> is W3SVC, GOPHERSVC, or MSFTPSVC

2. From the **Edit** menu, choose **Add Value** The Data type is REG_SZ.

3. Type the alias name for your directory and click the **OK** button.

4. In the String editor, type the full path to the virtual directory

Each virtual root has the following form

Where

Root Name This is the name of the virtual directory as it would appear in an URL. For example "/scripts" or "/specs" A root name of just "/" is considered to be the home root that will be used if no other roots match

Host Address The Host address is an optional field that indicates the server IP address this virtual root is associated with By specifying a host IP address, multiple logical servers can be

setup on a single machine. If a host address is specified, then only clients making requests on this IP address will see this virtual root.

Physical Path The physical path the Root Name should point to. For example "C:\Wwwroot" or "\\Server\Share". In the latter case where a UNC share is specified, a valid username and password must be specified.

User Name Only used if **Physical path** is a UNC share; specifies the user context to connect and impersonate as when accessing files over this virtual root. Note that the password is kept in a protected part of the registry and must be set using the Internet Service Manager

Access Mask This item is a single hexadecimal character bitfield that specifies what operations are allowed on this root. The mask is not used by the gopher server because only Read operations are ever performed. Note that this mask has no influence on any NTFS ACLs that might be on the files File ACLs must grant the appropriate permissions in addition to setting the appropriate value on the virtual root. The values for the bitfield are.

0x00000001 - Read access is allowed (FTP and HTTP)

0x00000002 - Write access is allowed (FTP only)

0x00000004 - Execute access is allowed (HTTP only)

0x00000008 - SSL or PCT encryption required (HTTP only)

The servers always match the longest virtual root first, thus "/123/567/89" will match "/123/567" before it matches "/123". The home root ("/") always matches last Virtual roots with host IP addresses always match before roots without host addresses.

Note Virtual directories will not appear in directory listings (also called directory browsing for the WWW service). To access a virtual directory users must know the virtual directory's alias, and type the URL address in their browser For the WWW service, you can also create links in HTML pages For the gopher service, you can create explicit links in tag files so that users can access virtual directories For the FTP service, you can list virtual directories by using directory annotations

CHAPTER 11

Troubleshooting and Error Messages

This chapter tells how to troubleshoot an Internet Protocol (IP) network. It also lists and explains error messages. Consult with your network administrator for further information.

Troubleshooting an IP Network

Follow these guidelines while troubleshooting an IP network:

- Always begin at the network interface layer and work up to the application layer.
- Make sure protocols at each layer of the Internet protocol suite can communicate with the layer above and below it.

To troubleshoot an IP network

1. Ping successfully.

   If you can ping successfully, you have verified IP communications between the network interface layer and the internet layer. The **Ping** command uses the Address Resolution Protocol (ARP) to resolve the IP address to a hardware address for each echo request and echo reply.

2. Establish a session with a host

   If you can establish a session, you have verified TCP/IP session communications from the network interface layer through the application layer.

Note If you are unable to resolve a problem, you may need to use an IP analyzer (such as Microsoft Network Monitor) to view network activity at each layer.

The first goal in troubleshooting is to make sure you can successfully ping an IP address. Ping a host with its host name only after you can successfully ping the host with its IP address.

To troubleshoot the network interface and internet layers by using the Ping command

1. Ping the loopback address to verify that TCP/IP was installed and loaded correctly.

   If this step is unsuccessful, verify that the system was restarted after TCP/IP was installed and configured.

2. Ping your IP address to verify that it was configured correctly.

   If this step is unsuccessful, view the configuration by using the Network application in the Windows NT Control Panel to verify that the address was entered correctly, and verify that the IP address is valid and that it follows addressing guidelines.

3. Ping the IP address of the default gateway to verify that the gateway is functioning and configured correctly.

   If this step is unsuccessful, verify that you are using the correct IP address and subnet mask.

4. Ping the IP address of a remote host to verify the connection to the wide area network

   If this step is unsuccessful.

   - Make sure that IP routing is enabled.
   - Verify that the IP address of the default gateway is correct
   - Make sure that the remote host is functional.
   - Verify that the link between routers is operational.

After you can successfully ping the IP address, ping the host name to verify that the name is configured correctly in the HOSTS file

Verifying TCP/IP Session Communications

The next goal in troubleshooting is to successfully establish a session Use one of the following methods to verify communications between the network interface layer and the application layer

To establish a session with a Windows NT-based computer or other RFC-compliant NetBIOS-based host, make a connect with the **Net use** or **Net view** command If this step is unsuccessful.

- Verify that the destination (target) host is NetBIOS-based
- Confirm that the scope ID on the destination host matches that of the source host

- Verify that you used the correct NetBIOS name.
- If the destination host is on a remote network, check the LMHOSTS file for the correct entry.

To establish a session with a non-RFC-compliant NetBIOS-based host, use the Telnet or FTP utility to make a connection. If this step is unsuccessful.

- Verify that the destination host is configured with the Telnet daemon or FTP daemon.
- Confirm that you have the correct permissions on the destination host.
- Check the HOSTS file for a valid entry if you are connecting using a host name.

Error Messages

A home directory already exists for this service. Creating a new home directory will cause the existing directory to no longer be a home directory. An alias will be created for the existing home directory.

This message is a warning only It appears when the new home directory you are trying to add already exists The maximum number of home directories allowed is one per virtual root

Invalid Server Name

While trying to connect to a server, you typed an invalid server name. Try to connect again and make sure you type the name correctly.

More than 1 home directory was found. An automatic alias will be generated instead.

When getting the directory entries from the server, Internet Service Manager has determined that a duplicate exists This duplicate may have been added by using the Registry Editor or in some other way

No administerable services found.

While trying to connect to a server, you typed the name of a server that has no installed services that Internet Service Manager can administer That is, WWW, FTP, and gopher services have not been installed on the computer you connected to.

The alias you have given is invalid for a non-home directory.

You're trying to assign the alias '' to a non-home directory This alias automatically means *home*.

The connection attempt failed because there's a version conflict between the server and client software.

This message is an RPC error message The RPC interface does not match what is expected. This should happen only if you are running a beta admininstration tool or server. The official error is RPC_S_UNKNOWN_IF.

The service configuration DLL '*filename*' failed to load correctly.

The named service configuration DLL (for example, W3scfg dll) failed to load. The DLL or one if its dependencies could be missing or corrupted Generally this is a setup problem. Run the Setup program and select **Remove All**, then reinstall Microsoft Internet Information Server.

Unable to connect to target machine.

This message is an RPC error message that appears while executing an API. The computer could be offline. The system error was EPT_S_NOT_REGISTERED or RPC_S_SERVER_UNAVAILABLE

Unable to create directory.

The directory name or path you typed in in the **New Directory Name** box cannot be created. It could be an invalid path, or a file may already exist that has this name

Contents | Index | ◁ | △ | ▷

Contents | Index | ◁ | ▷

APPENDIX A

Glossary

This glossary documents terms found in the documentation for Internet Information Server and Internet Explorer. See the Windows NT online Help for additional information.

A B C D E F G H I L M N O P R S T U V W

A

annotation file
For the FTP service, a summary of the information in a given directory. This summary appears automatically to remote browsers

anonymous logons
This feature allows remote access only by the IUSR_*computername* account. Remote users can connect to that computer only without a user name and password, and they have only the permissions assigned to that account.

associating
See **file-name extension mapping**

authentication
Determining if a user has permission to access a resource or perform an operation

B

bandwidth control
Setting the maximum capacity that a service is allowed to use You can deliberately limit a server's Internet workload by not allowing it to receive requests at full capacity, to save resources for other programs such as e-mail

Basic clear-text authentication
An authentication protocol supported by Internet Explorer. There is no encryption with this protocol.

BIND
See **Domain Name System (DNS)**

bits per second (bps)
The measure of speed at which data is transferred over a network.

bps
See **bits per second**.

browser
A tool for navigating and accessing information on the Internet or an intranet.

C

cache
A store of files from a Web server copied locally for quicker access. To configure your cache on the Internet Explorer browser, from the **View** menu choose **Cache Settings**.

CGI
See **Common Gateway Interface (CGI)**.

challenge/response
A method of authentication in which a server uses Windows NT security to allow access to its resources.

client/server architecture
The structure of services that run on the Internet or an intranet The client computer accesses the Web server, which supplies the client with resources or information not found on the client's own host Also, CGI and ISAPI applications can do processing on the Web server and return results to the client

Common Gateway Interface (CGI)
An interface used by an application that runs on a Web server when a client requests it.

connected user
A user who is currently accessing one of the Microsoft Internet Information Server

cryptography
A method of securing data transmissions to and from your Web server

D

data integrity
A way of preventing data from being altered in transit

Data Source Name (DSN)
The name that allows a connection to an ODBC data source, such as a SQL Server

database. You set this name by using the ODBC application in the Control Panel.

DHCP
See **Dynamic Host Configuration Protocol (DHCP)**.

dial-up
A connection to a computer by telephone, through a modem

discovery mechanism
A way of finding other servers on the network. In Internet Server Manager, choose **Find All Servers** from the **Properties** menu.

DNS
See **Domain Name System (DNS)**.

DNS spoofing
Assuming the DNS name of another system by either corrupting a name-service cache, or by compromising a domain-name server for a valid domain

domain
For Windows NT Server, a collection of computers that share a common domain database and security policy. Each domain has a unique name

domain controller
For a Windows NT Server domain, the server that authenticates domain logons and maintains the security policy and the master database for a domain

Domain Name System (DNS)
A protocol and system used throughout the Internet to map Internet Protocol (IP) addresses to user-friendly names. DNS is sometimes referred to as the BIND service.

DSN
See **Data Source Name (DSN)**

Dynamic Host Configuration Protocol (DHCP)
An industry-standard protocol that assigns Internet Protocol (IP) configurations to computers.

E

encryption
A way of making data indecipherable while it is being sent from computer to computer.

F

file-name extension mapping
Connecting all files with a certain file-name extension to a program. For example, through the Windows NT Explorer, all .txt files are associated by default with Notepad. In Internet Explorer, you can associate file-name extensions with applications through the **Helpers** dialog box. To display this dialog box, from the **View** Menu, choose **Helpers**.

File Transfer Protocol (FTP)
An industry standard for sharing files between computers.

filter
A feature of ISAPI that allows pre-processing of requests and post-processing of responses, permitting site-specific handling of Hypertext Transfer Protocol (HTTP) requests and responses.

firewall
A system or combination of systems that enforces a boundary between two or more networks and keeps hackers out of private networks.

friendly name
A name that substitutes for an IP address, for example, www.microsoft.com instead of an IP address such as 157 45.60 81

FTP
See **File Transfer Protocol (FTP)**

G

gateway
A hardware or software device that directs network traffic.

gopher
A hierarchical system for finding and retrieving information from the Internet or an intranet

Gopher Plus
An enhanced version of gopher, including a way of getting more information about an item (such as file size, last date of modification, and the administrator's name), the ability to display a single file in multiple formats (such as regular text, rich text, and PostScript®), a way to add a short description of the item, and the ability to ask a user to fill out a form to obtain an item

gopherspace
All files available on a gopher server for display through the gopher protocol.

H

home directory
The root directory for a service, where the content files are stored. By default, the home directory and all its subdirectories are available to users.

HTML
See **Hypertext Markup Language (HTML)**.

HTTP
See **Hypertext Transfer Protocol (HTTP)**.

hyperlink
A way of jumping to another place on the Internet Hyperlinks usually appear in a different format from regular text You initiate the jump by clicking the link

hypertext
Documents with links to other documents Click a link to display the other document.

Hypertext Markup Language (HTML)
The formatting language used for documents on the World Wide Web.

Hypertext Transfer Protocol (HTTP)
The underlying protocol by which WWW clients and servers communicate.

I

Integrated Services Digital Network (ISDN)
A connection to the Internet installed by your Internet service provider (ISP). A dial-up ISDN line can offer speeds up to 128,000 bps

interactive applications
A program written in C, Perl, or as a Windows NT batch file The user initiates the program by clicking a hyperlink

Internet
The global network of computers that communicate through a common protocol, TCP/IP

Internet Log Converter
A program that turns Microsoft Internet Information Server log files into either European Microsoft Windows Academic Centre (EMWAC) log file format or the Common Log File format Convlog exe is in the Inetsrv directory

Internet Network Information Center (InterNIC)

The coordinator for DNS registration.

Internet Protocol (IP)
The part of TCP/IP that routes messages from one Internet location to another.

Internet Protocol (IP) address
A unique address that identifies a host on a network. It identifies a computer as a 32-bit address that is unique across a TCP/IP network. An IP address is usually represented in dotted-decimal notation, which depicts each octet (eight bits, or one byte) of an IP address as its decimal value and separates each octet with a period, for example: 102.54.94.97.

Internet Service Providers (ISPs)
Public providers of remote connections to the Internet.

InterNIC
See **Internet Network Information Center (InterNIC)**

intranet
A TCP/IP network that can be connected to the Internet but is usually protected by a firewall or other device (for example, a corporate network).

IP
See **Internet Protocol (IP)**.

IP address
See **Internet Protocol (IP) address**

ISDN
See **Integrated Services Digital Network (ISDN)**

ISPs
See **Internet Service Providers (ISPs)**

L

leased line
A high-capacity line (most often a telephone line) dedicated to network connections

link
See **hyperlink**

log file
The file in which logging records are stored. This file can be either a text file or a database file.

logging
Storing information about events that occurred on a firewall or network.

M

Management Information Databases (MIBs)
Software that describes manageable aspects of your network using the Simple Network Management Protocol (SMNP). The MIB files included in the Sdk directory of the Microsoft Windows NT compact disc can be used by third-party SNMP monitors to enable SNMP monitoring of the WWW, gopher, and FTP services of Microsoft Internet Information Server.

MIBs
See **Management Information Databases (MIBs)**.

MIME mapping
See **Multipurpose Internet Mail Extension (MIME) mapping**.

Multipurpose Internet Mail Extension (MIME) mapping
A way of configuring browsers to view files that are in multiple formats.

N

name resolution
A configuration that maps friendly names to IP addresses

Network News Transfer Protocol (NNTP)
A protocol for reading messages posted in thousands of news groups on the Internet.

NNTP
See **Network News Transfer Protocol (NNTP)**

O

object-cache scavenger
The code that periodically scans the cache for objects to be discarded It deletes from the cache files that have not been used recently and therefore are unlikely to be used again in the near future

---

P

packet
A piece of information sent over a network.

page
See **Web page**.

password authentication
See **authentication**.

policies
Conditions set by the system administrator such as how quickly account passwords expire and how many unsuccessful logon attempts are allowed before a user is locked out. These policies manage accounts to prevent exhaustive or random password attacks.

port number
A number identifying a certain Internet application. For example, the default port number for the gopher service is 70, and for the WWW service it is 80.

program file
A file that starts an application or program. A program file has an .exe, .pif, .com, .cmd, or .bat file-name extension.

protocol
Software that allows computers to communicate over a network. The Internet protocol is TCP/IP

proxy
A software program that connects a user to a remote destination through an intermediary gateway.

R

RAS
See **Remote Access Service (RAS)**

Remote Access Service (RAS)
A service that allows remote clients running Microsoft Windows or Windows NT to dial in to a network

remote administration
Administering a computer from another computer over the network

Remote Procedure Call (RPC)
A message-passing facility that allows a distributed application to call services available on various computers in a network

261

router
A hardware or software device that directs network traffic.

RPC
See **Remote Procedure Call (RPC)**.

S

script
A group of directives to an application or utility program. A CGI application, for example. *See also* **Common Gateway Interface**.

Secure Sockets Layer (SSL)
A protocol that supplies secure data communication through data encryption and decryption

service
One of the three services offered by the Internet Information Server: WWW, gopher, or FTP.

Simple Mail Transfer Protocol (SMTP)
A protocol used for exchanging mail on the Internet.

Simple Network Management Protocol (SNMP)
A protocol for monitoring your network. *See also* **Management Information Databases (MIBs)**

slow link
A modem connection, usually from 9,600 bps to 28,800 bps.

SMTP
See **Simple Mail Transfer Protocol (SMTP)**.

SNMP
See **Simple Network Management Protocol (SNMP)**.

SQL logging
Logging to a Microsoft SQL Server database instead of to a text file. *See also* **Logging**.

SSL security
See **Secure Sockets Layer (SSL)**

static page
HTML pages prepared in advance of the request and sent to the client upon request. This page takes no special action when requested. *See also* **interactive applications**.

subnet mask
A TCP/IP configuration parameter that extracts network and host configuration from an IP address.

System Data Source Name (DSN)
A name that can be used by any process on the computer. Internet Information Server uses system DSNs to access ODBC data sources. *See also* **Data Source Name (DSN)**.

T

tag files
Files that contain information about files on a gopher server. This information is sent to clients and it typically contains the file name, host name, and port number.

TCP/IP
See **Transmission Control Protocol/Internet Protocol (TCP/IP)**.

throttling
Controlling the maximum amount of bandwidth dedicated to Internet traffic on your server. This feature is useful if you have other services (such as e-mail) sharing the server over a busy link.

Transmission Control Protocol/Internet Protocol (TCP/IP)
A networking protocol that allows computers to communicate across interconnected networks and the Internet. Every computer on the Internet supports TCP/IP.

U

Uniform Resource Locator (URL)
A naming convention that uniquely identifies the location of a computer, directory, or file on the Internet. The URL also specifies the appropriate Internet protocol, such as gopher, HTTP, and so on

URL
See **Uniform Resource Locator (URL)**

Usenet
The most popular news group hierarchy on the Internet

V

virtual directory
A directory outside the home directory that appears to browsers as a subdirectory of

the home directory. For any of the three services (WWW, gopher or FTP), you can configure a virtual directory through the Directories property sheet in the Internet Server Manager.

virtual server
A computer with several IP addresses assigned to the network adapter card. This configuration makes the computer look like several servers to a browser.

volatile objects
Typically, files that the Web site administrator updates frequently.

W

Web browser
A software program, such as Internet Explorer, that retrieves a document from an Web server, interprets the HTML codes, and displays the document to the user with as much graphics as the software can supply.

Web page
A World Wide Web document. Pages can contain almost anything, such as news, images, movies, and sounds.

Web server
A computer equipped with the server software to respond to Web client requests, such as requests from a Web browser. A Web server uses the Internet HTTP, FTP, and gopher protocols to communicate with clients on a TCP/IP network.

Windows Internet Name Service (WINS) server
A protocol for mapping Internet Protocol (IP) addresses to user-friendly names *See also* **Domain Name System**

WINS server
See **Windows Internet Name Service (WINS) server**

World Wide Web (WWW)
The most graphical service on the Internet The Web also has the most sophisticated linking abilities

WWW
See **World Wide Web (WWW)**

INSTALLATION AND ADMINISTRATION GUIDE

Copyright Information

Microsoft Internet Information Server

Version 2.0
Windows NT Server 4.0

Microsoft Corporation

97

UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company, Ltd.

Document Date: 07/96

Contents | Index | ◁ | △ | ▷