Asegurando el acceso Web con

Microsoft Proxy Server 2.0

MOC 836 CCP

TEMARIO

1.− Vista previa de Microsoft Proxy Server 2.0

2.− Instalación de Microsoft Proxy Server 2.0

3.− Arquitectura de Microsoft Proxy Server 2.0

4.− Uso de IIS para administrar Microsoft Proxy Server 2.0

5.− Control de acceso

6.− Publicación en Web segura

7.− Filtrado de paquetes

8.− Uso de Microsoft Proxy Server 2.0 con conexiones Dial−Up

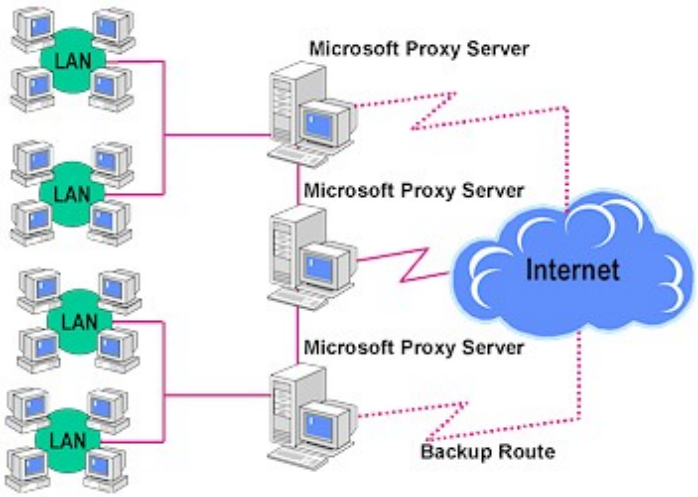
9.− Configuración de múltiples servidores Proxy

10.− Planificación de un servidor Proxy

11.− Monitorización y optimización del Proxy

12.− Resolución de Problemas

Tema 1.− Vista previa de Microsoft Proxy Server 2.0



Microsoft Proxy Server 2.0 es un firewall, servidor de caché de contenidos y proveedor de seguridad. Mediante él, podemos conectar toda una red a Internet.

Hace la función de firewall, o cortafuegos, ya que con dos tarjetas de red podemos aislar nuestra red de intrusos del mundo exterior, mantiene en memoria o caché las páginas Web visitadas por nuestros clientes, permitiendo así el acceso más rápido a las mismas y nos provee de seguridad al poderle implementar filtros de seguridad tanto de entrada como de salida.

Microsoft Proxy Server 2.0 se compone de tres servicios:

1.− WEB PROXY: Soporta HTTP, FTP, Gopher para redes TCP/IP

2.− WINSOCK PROXY: Soporta aplicaciones cliente (Telnet, RealAudio) sobre TCP/IP e IPX/SPX para redes sin TCP/IP.

3.− SOCKS PROXY: Mecanismo de seguridad y conexión cliente−servidor que utiliza la tecnología Socks 4.3ª, soportando aplicaciones cliente y redireccionamiento para clientes no windows. NO soporta UDP. NO autentifica clientes. NO soporta IPX/SPX.

Mejoras de seguridad:

1.− Punto único de contacto LAN− Internet con dos tarjetas de red.

2.− La única IP visible es la del proxy

3.− Filtra paquetes IP por puerto, tipo y URL, ya que los puertos se abren solo el tiempo imprescindible de paso de información.

Beneficios del uso de Microsoft Proxy Server 2.0

1.− Integración con NT Server 4.0, Windows 2000 (con el parche del proxy) e Internet Information Services (IIS), lo que nos concede facilidad de administración, las ventajas de las propiedades de TCP/IP y los filtros a usuarios de NT 4.0 y Windows 2000.

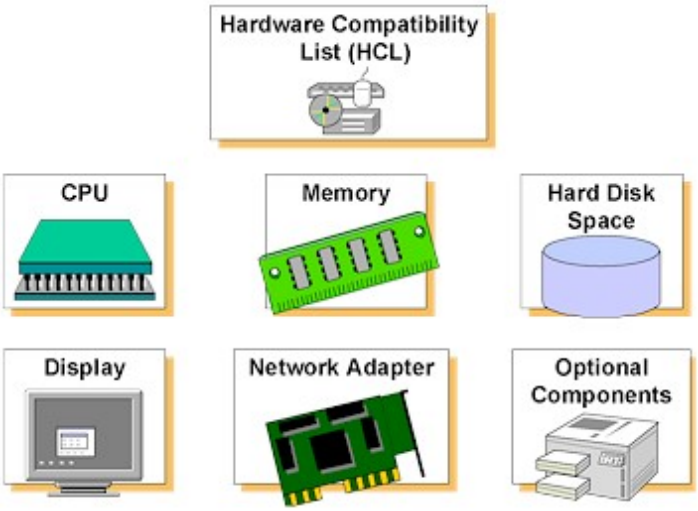
2.− Ancho de banda compartido, lo que proporciona igualdad de recursos a los usuarios y ahorros en hardware.

3.− Conexión de clientes LAN a Internet de una manera fácil, con traducción de protocolo a IPX si es necesario, lo que proporciona la libertad de poder conectar múltiples clientes.

4.− Servicios de caché de documentos, válida para uso local, disminuyendo el tiempo de acceso a las páginas y permitiendo actualizaciones de página transparentes.

5.− Servicios de publicación en Web con IIS, montaje de Intranets y posibilidad de encadenar múltiples servidores proxy en el mismo segmento de red.

Tema 2.− Instalación de Microsoft Proxy Server 2.0



Requerimientos de hardware:

- Hardware Compatibility List (HCL)
- CPU a partir de un 486
- RAM a partir de 24 Mb (para maquinas Intel)
- Disco Duro 10 Mb para la instalación en sí

100 Mb mínimo para la caché

0.5 Mb por cada cliente proxy en la red

- Tarjetas de red (2 como mínimo para aislar la red)
- Adaptadores opcionales dependiendo del tipo de conexión a Internet de que dispongamos (RDSI, ADSL)

Requerimientos de software:

- Windows NT Server 4.0 o Windows 2000 Server
- Internet Information Services (por lo menos la versión 2.0)
- Service−pack correspondiente del S.O.
- TCP/IP instalado en el servidor
- Microsoft Proxy Server 2.0

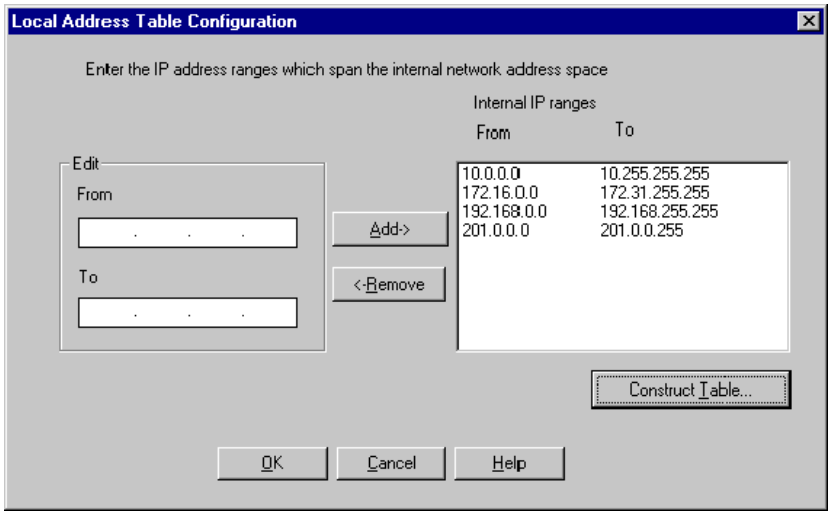
Antes de Instalar verificar:

- Espacio disponible en Disco Duro
- El sistema de archivos de la partición es NTFS
- Usar siempre la cuenta de Administrador o una personalizada con privilegios de administrador
- Configurar correctamente tanto las tarjetas de red instaladas en el servidor como la conexión externa a Internet de que dispongamos.

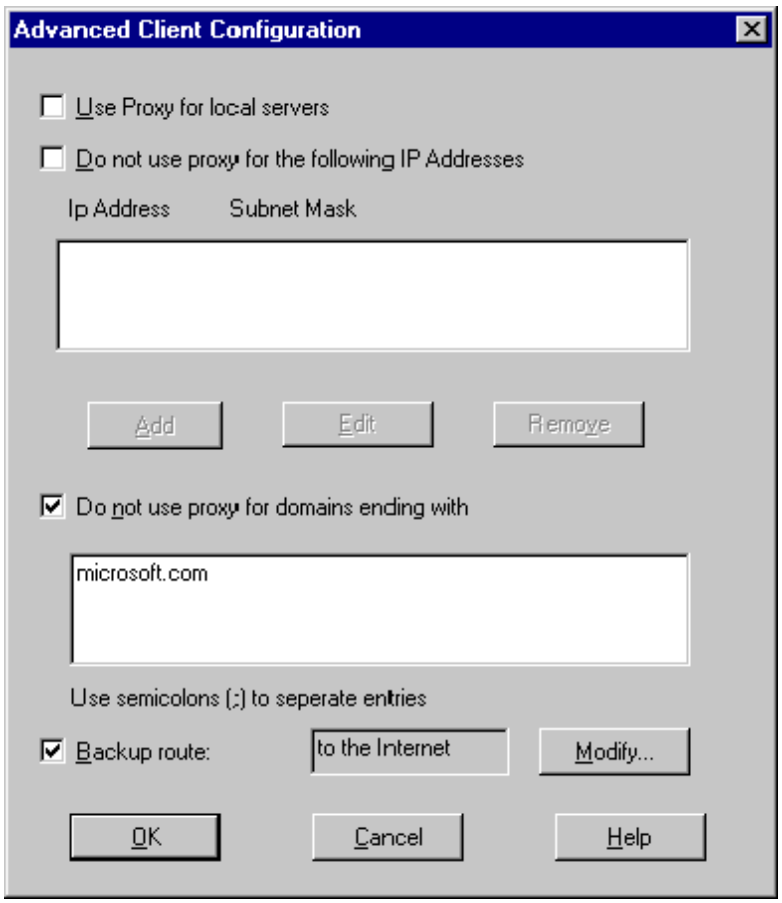
Proceso de instalación:

- Ejecutar el comando Setup o Instalar desde el CD−ROM
- Introducir los datos legales (nombre, compañía, Nº de serie)
- Cambiar (si procede) el directorio de instalación, que está por defecto en C:\Msp
- Elegir las opciones de instalación, las cuales están todas seleccionadas predeterminadamente

- Seleccionar el tipo de cliente que vamos a usar por su S.O.
- Selección del tamaño de la caché en disco duro
- Configuración de la Tabla Local de Direcciones (LAT)



- Configuración Avanzada de los clientes



- Finalización y reinicio del sistema

La **LAT o Tabla Local de Direcciones** se define como Pares de direcciones IP que definen los espacios de red, pudiendo ser sencillos (una sola IP) o múltiples (mas de una IP).

Funciones de la LAT en el **servidor**:

- Define las direcciones IP de la red interna
- Se puede generar manual o automáticamente según las direcciones de las tarjetas de red instaladas en el servidor correspondiente
- Es fácilmente modificable
- NO debe incluirse la IP externa de conexión a Internet en la LAT

Funciones de la LAT en los **clientes**:

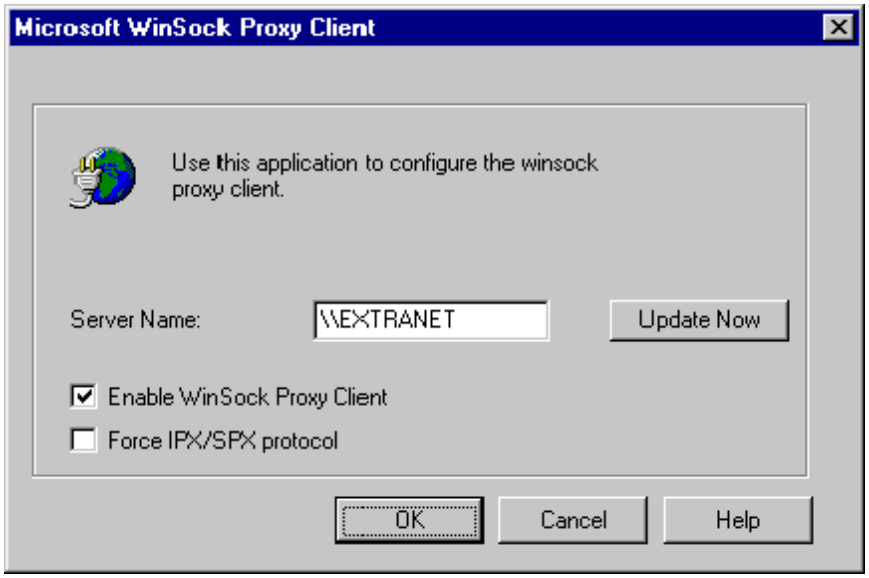
- Se instala en \Mspclnt\Msplat.txt
- Se renueva regularmente cada 5 horas
- Al llegar una conexión se utiliza para redirigir, si es interna, directamente, y si es externa, al servicio Winsock Proxy
- NO intentar reescribir a mano, porque el refresco automático anularía esos cambios, en su lugar sustituir por locallat.txt
- El cliente puede usar Msplat.txt y Locallat.txt indistintamente para redirigir la señal al lugar correspondiente o al servicio que le dé salida.

Cambios que produce Microsoft Proxy Server 2.0 en el Sistema Operativo **del servidor**:

- Se añaden a la consola de administración del IIS del servidor los tres servicios necesarios para la ejecución de Microsoft Proxy Server 2.0
- Se crea la LAT
- Se crea la memoria caché (de 100 Mb predeterminadamente)
- Se instalan contadores del monitor de sistema
- Se crea la carpeta \Msp en el servidor

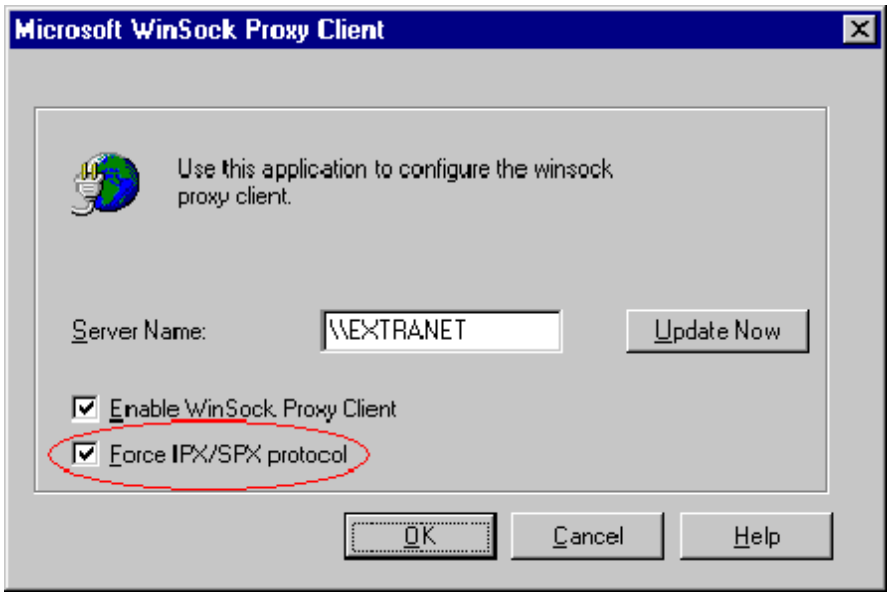
Instalación de los clientes:

- Conectar con el servidor proxy de nuestra red
- Conectar allí con el recurso compartido que se crea de una manera automática \Mspclnt, donde encontraremos un comando Setup o Instalar, el que nos permitirá instalarnos el cliente Proxy
- NO REINICIAR CUANDO LO PIDA
- Comprobación del canal de conexión con el servidor mediante el icono del Panel de Control **Cliente WSP**, con el botón indicador de actualizar ahora (o Update now)

- 

  Una vez que la comprobación ha sido realizada con éxito, reiniciar la máquina

Para forzar el protocolo IPX/SPX en redes que no soporten TCP/IP el método es similar al de antes con una variación: marcar la casilla de forzar protocolo IPX/SPX en el cliente WSP.



Tema 3.− Arquitectura de Microsoft Proxy Server 2.0

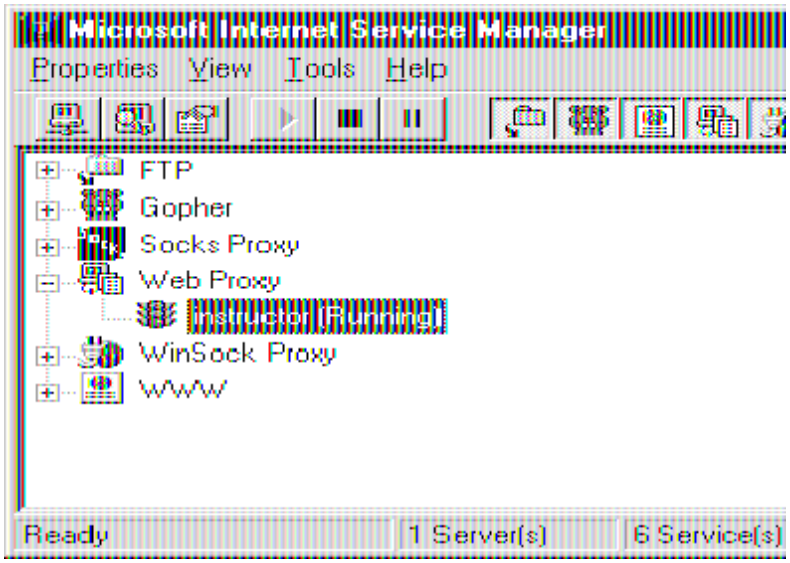
Un proxy se define como una autoridad o poder de actuar por otro, que es lo que realmente hace, conectar a Internet clientes que, de otro modo, no serian capaces de acceder a Internet por otra vía (sin coste adicional de hardware).

Los servicios del proxy son el puente a los nuevos métodos de acceso a datos de Internet además de aislar y asegurar la propia red interna

Normalmente la maquina con el proxy es en la única en la que convergen las dos redes existentes en nuestra corporación, la interna y la que da acceso al exterior o a Internet

Hay tres servicios fundamentales a tener en cuenta:

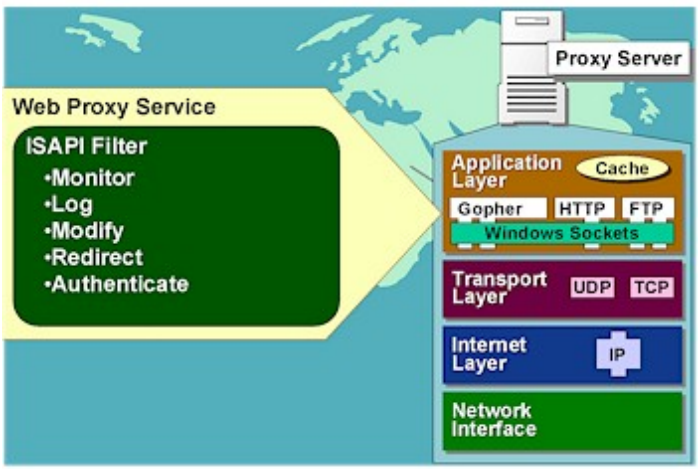
- **WEB PROXY:**



  - Soporta peticiones de browsers o navegadores que sean compatibles con el estándar CERN (modelo GET−POST)
  - Soporta IP Agregation, o múltiples servidores proxy en matriz con una sola dirección IP que les identifica
  - Da servicio y paso a HTTP, FTP y Gopher
  - Proporciona la seguridad al nivel de usuario en Windows NT Server 4.0 o Windows 2000
  - Soporta canales seguros como SSL y HTTPS
  - Fácilmente administrable desde la consola del IIS

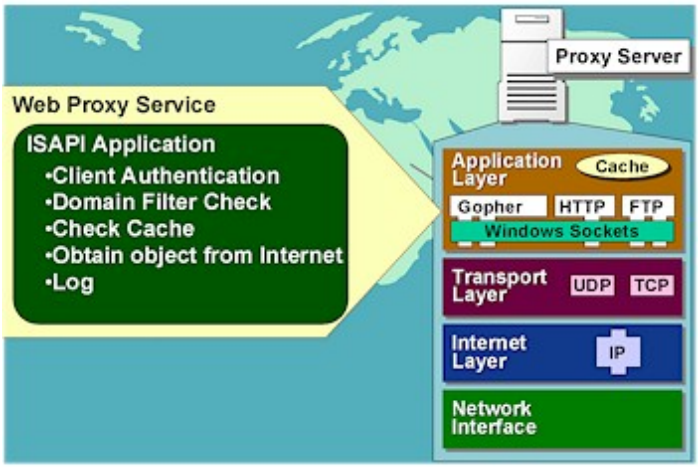
  - Consta de dos componentes básicos:

- Filtro ISAPI (Internet Server Application Programming Interfaz)



  - Extensión usada por el servidor cada vez que le llega una petición HTTP
  - Abre un filtro por cada petición, identificándola por su IP o con la URL
  - Se encuentra en el archivo w3proxy.dll
  - Soporta peticiones CERN, las que enruta al proxy, y HTTP, las que no son modificadas y llegan tal y como salieron

- Aplicación ISAPI



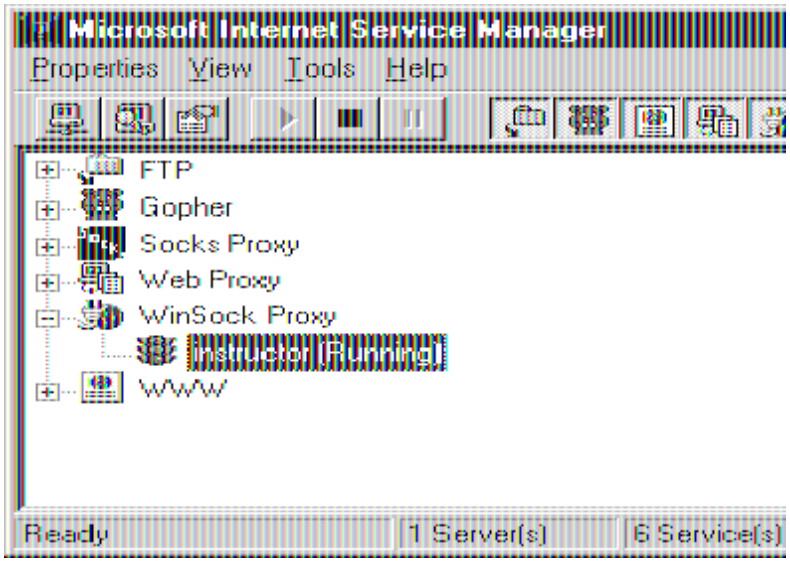
  - Crea HTML dinámico (o DHTML) para la integración Web de aplicaciones
  - NO se invoca una por proceso
  - Esta en el archivo w3proxy.dll
  - Autentifica clientes, hace filtros de dominio y busca en la/s caché/s o en Internet
  - Si la petición es correcta, se le extrae el protocolo, el nombre de dominio y se usa la API apropiada de Windows Sockets

  - Proceso:

- resolución de nombres DNS
- conexión al sitio remoto
- envío de petición de página
- recibo de respuesta
- lectura de datos
- redirigir el contenido al cliente y a la caché correspondientes

  - Las peticiones ya hechas se mantienen un tiempo gracias a un servicio de IIS (Server Keep−Alives)

2. WINSOCK PROXY



- Usado por aplicaciones Windows que utilizan los Sockets para comunicarse entre ellas
- Ventajas:
- Soporta TCP/IP e IPX/SPX
- Autentifica usuarios de Windows NT Server 4.0 y Windows 2000 (con el parche correspondiente)
- Filtra paquetes de información
- Capacidad de restringir URL's
- Bloquea intentos de entrada del exterior
- Soporta SSL y HTTPS

Un **SOCKET** es un mecanismo que intercomunica procesos entre aplicaciones en la misma u otra máquina conectada a la red, definido por un grupo de API's que regulan la comunicación entre procesos y aplicaciones. Soporta TCP/IP y UDP.

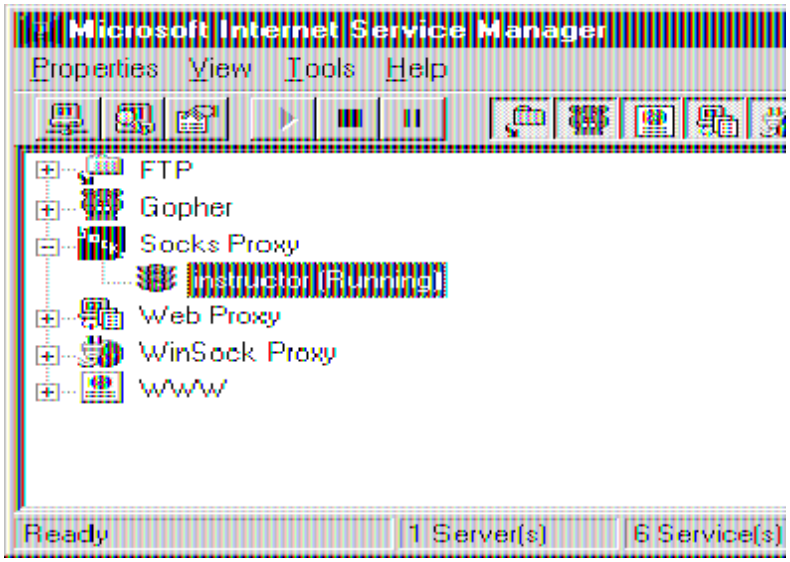
Los canales de comunicación se representan por estructuras llamadas **Sockets**, con un par de datos que los identifican: la dirección, a la que se identifican para facilitar la comunicación, y el puerto, que debe coincidir en las maquinas que se comunican, y que identifica el canal de comunicación que estamos usando.

El servicio **Winsock Proxy** o WSP permite a una aplicación comportarse como si tuviera conexión directa a Internet, salvando los elementos intermedios que existan en la red. En los clientes, intercepta las peticiones y establece rutas de comunicación a Internet mediante el servidor proxy. Es un servicio transparente.

En el **servidor** lo encontramos como un servicio de Windows NT Server 4.0 o Windows 2000 Server, siendo el encargado de crear una conexión virtual con Internet transfiriendo datos en el canal cliente−servidor. Traduce IPX/SPX si es necesario.

En el **cliente** intercepta los mensajes de petición de las aplicaciones, controlando el canal, pasándole las peticiones o completando los procesos de esas aplicaciones, dependiendo del estado de la petición de la aplicación correspondiente. Existen versiones de 16 y 32 bit. Se activa e instala al instalar el cliente proxy (cliente WSP). La recomendación mas usual es utilizar lo menos frecuentemente este canal como se pueda, por su impacto en el rendimiento de la maquina (ya que trabaja con RPC). **Este canal trabaja en UDP en el puerto 1745.**

3. SOCKS PROXY



- Establece un canal seguro de comunicación con Internet
- Proporciona compatibilidad de servicios con clientes no windows
- Soporta TCP/IP e identificación de protocolo
- Utiliza autentificación de IP

El protocolo **SOCKS** es un protocolo que funciona como un proxy, permitiendo interconexión en red sin accesibilidad IP gracias a dos operaciones: Connect y Bind.

- CONNECT establece conexiones con servidores de aplicaciones. Los requerimientos de esta operación son altos: versión del protocolo socks, código de comandos socks, dirección IP de destino, puerto TCP de destino, identificador de usuario (o User ID) y un campo nulo para operaciones internas. El proceso a seguir es:

  - recepción y proceso del paquete
  - envío de respuesta concediendo o no permiso de uso
  - si el permiso se concede se crea el canal y la comunicación es inmediata
  - si el permiso se deniega se cierra la conexión y se informa del fallo mediante un mensaje HTML con el navegador.

- BIND da control de acceso a datos dependiendo de la cabecera TCP

El método de acceso al canal depende del protocolo que usemos:

- TCP/IP

  - dos API's TCP quieren intercomunicarse
  - la dll o librería dinámica winsock proxy client se inicia
  - se recibe una LAT vía winsock proxy por el canal de control
  - winsock proxy enruta a local o remoto según corresponda
  - si el nombre no se resuelve correctamente se interpreta siempre como local

- IPX/SPX

  - Winsock proxy convierte la petición IPX local en TCP de Internet por la trama de configuración de IPX
  - Si la red no aguantara TCP/IP, todas las conexiones se asumen como remotas

- El canal de control usaría IPX
- Al intentar intercomunicar API's habría que reformar completamente los parámetros de la API por IPX, lo que significa una reforma total, causa por la cual se debe usar una API especial y dedicada a IPX/SPX

Uso de Web Proxy y Winsock Proxy conjuntamente:

- El cliente Web lanza una petición al servidor proxy
- El cliente Winsock intercepta la conexión TCP
- Winsock mira la IP en la LAT y redirige en consecuencia, convirtiendo la señal si fuera IPX/SPX
- Se usa el servicio Winsock para crear las conexiones con ISAPI y cliente−servicio
- Las peticiones se pasan al servicio Winsock Proxy, quien las redirige a la caché (ISAPI)
- ISAPI busca en la caché y, si no encuentra la página solicitada, sale a Internet a buscarla, guardándola posteriormente en caché para su uso por otros clientes y para acceder mas fácilmente a ella en caso de nueva petición de pagina por parte de clientes WSP.

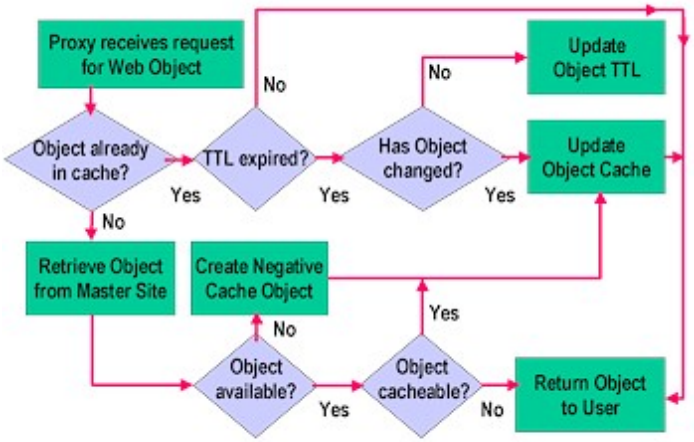
La **CACHE** es un espacio en disco duro, generalmente de 100 Mb, destinado a guardar copias de las páginas Web solicitadas al servidor proxy.

En la caché **NO** se guardarán páginas que contengan identificadores personales seguros, como contraseñas, o datos volátiles de identificación

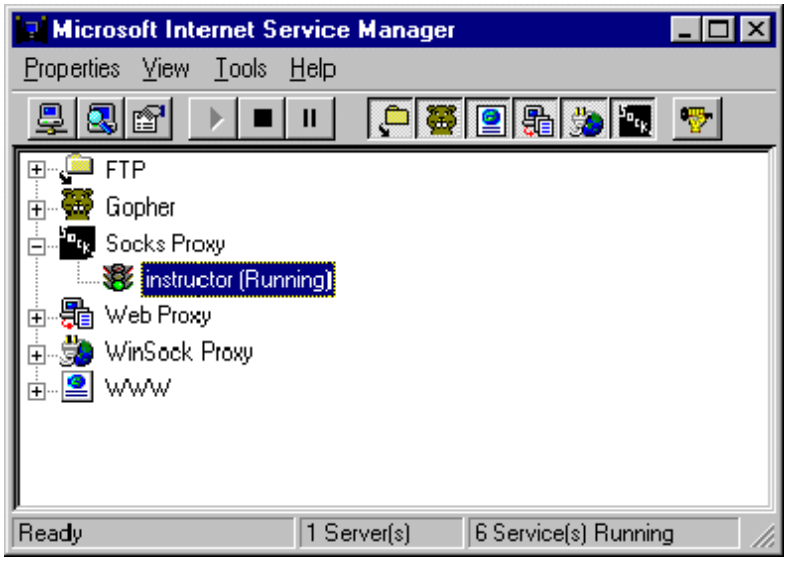
Tipos de caché:

- CACHÉ PASIVA (o caché bajo demanda)
    - Modo básico de cacheado
    - Intercepta las peticiones de los clientes y determina si la información (las páginas) pueden o no ser cacheadas
    - A cada objeto página se le asigna un TTL (o TDV, en español) que es el tiempo de vida útil hasta que ese objeto vuelva a recibir una petición
    - Cuando el espacio se va agotando, se calculan el TTL, la popularidad y el tamaño de ese objeto para eliminar elementos de la caché de un modo estructurado
    - Podemos actualizar la caché desde IE 5.0 presionando F5
- CACHÉ ACTIVA
    - Trabaja junto con la pasiva para optimización de los datos en la misma
    - Hace caché por factores:

- Popularidad, o número de peticiones que ese objeto recibe por parte de los clientes
- TTL, o tiempo de vida, con mayor facilidad de ser refrescado un objeto cuanto menor sea éste
- Carga del servidor, o tamaño de los objetos de la caché, que va a depender enteramente del espacio en disco duro del que disponga el servidor proxy en cuestión



Tema 4.− Uso de IIS para administrar Microsoft Proxy Server 2.0



Los servicios de Microsoft Proxy Server 2.0 se integran en la consola del IIS que tengamos montado en ese momento en el servidor

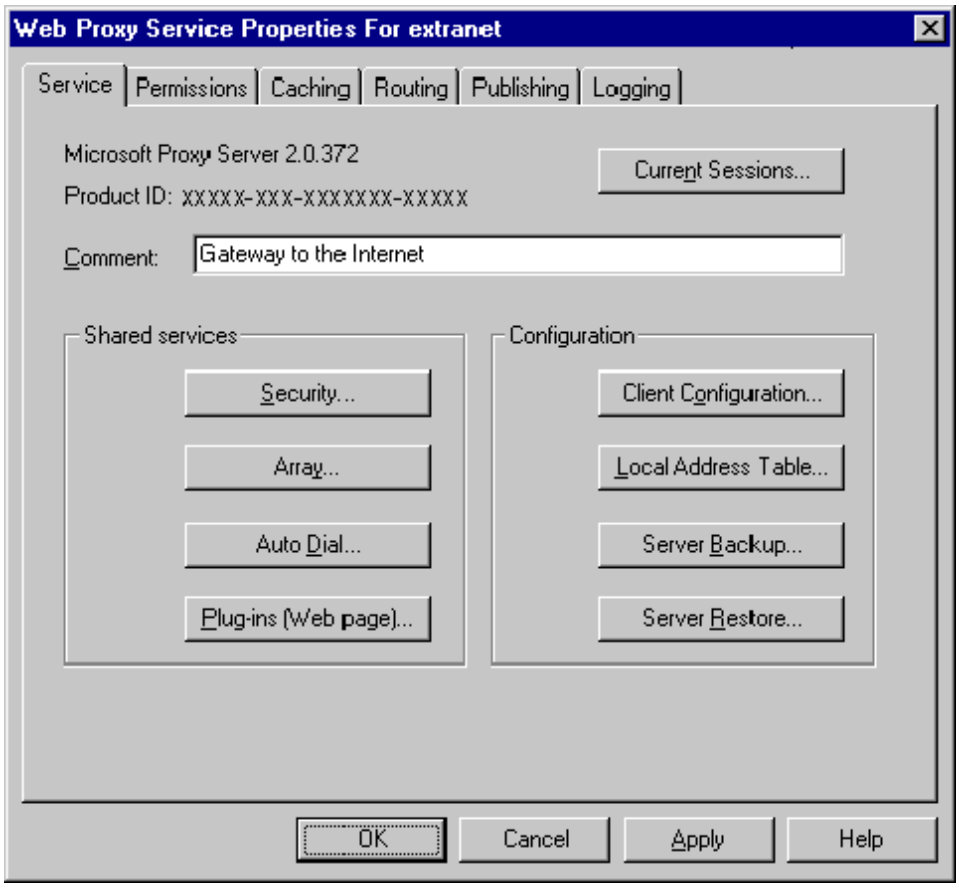
Hay que tener siempre en cuenta que se comportan como servicios de Windows NT Server 4.0 o Windows 2000 Server, por lo que están sujetos a los fallos y actuaciones típicas de los servicios en estos sistemas operativos.

Todas las pantallas comentadas a continuación aparecen al hacer click con el botón izquierdo de nuestro ratón en cualquiera de los tres servicios que ya conocemos de Microsoft Proxy Server 2.0

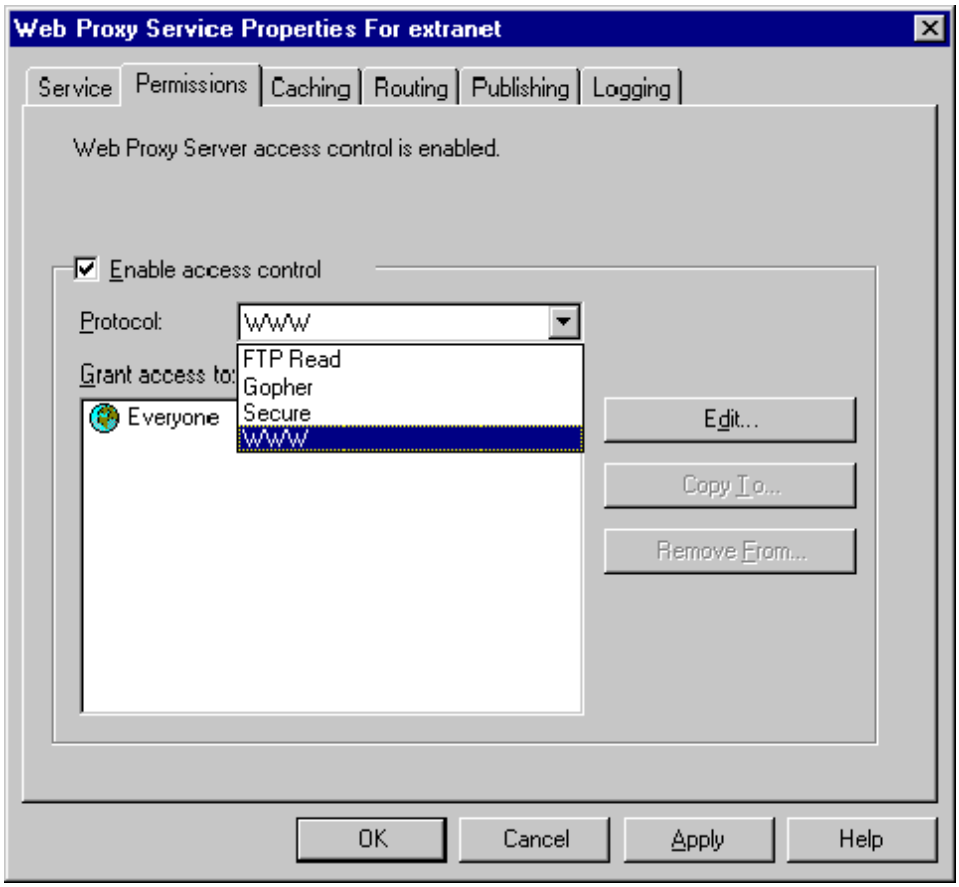
La primera pantalla de los tres servicios, denominada Service o Servicios, es común para los tres, siendo explicada solo una vez en el caso del servicio Web Proxy.

Pantallas de configuración de los servicios del proxy:

- **WEB PROXY**



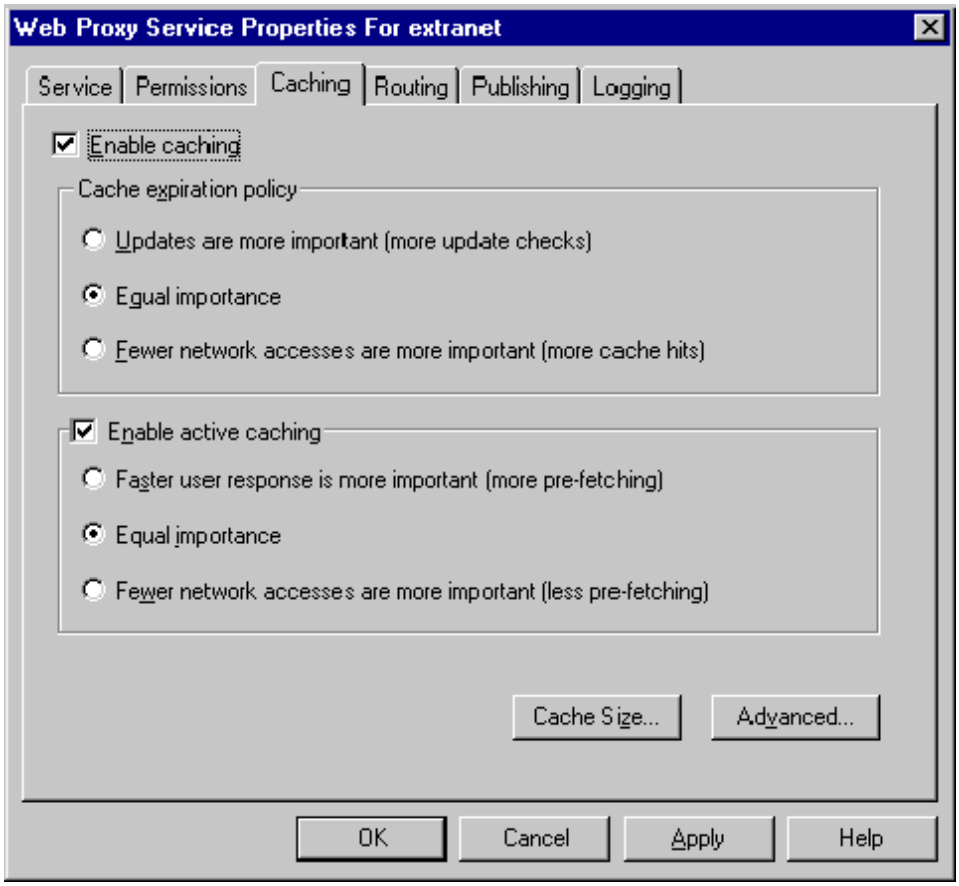
- Información sobre la versión de Microsoft Proxy Server 2.0 y la clave de instalación del producto
- Botón de acceso a la tabla de sesiones actuales de las que es objeto en ese momento Microsoft Proxy Server 2.0
- Comentario sobre el servidor proxy o sobre el servicio Web proxy
- Botón de seguridad, que da acceso a la configuración de seguridad del servicio Web Proxy
- Botón de configuración y modificación de matrices de servidores proxy
- Botón de configuración del auto−marcado de acceso a Internet
- Botón de acceso a páginas Web con complementos y accesorios del Microsoft Proxy Server 2.0
- Botón de acceso a la configuración de los clientes
- Botón de acceso a la configuración de la Tabla Local de Direcciones (LAT)
- Botón de acceso a la copia de seguridad del servidor proxy
- Botón de acceso al menú de restauración de datos del servidor proxy



La pantalla de Permisos se utiliza para administrar los permisos de los usuarios y de los grupos que tienen acceso a los protocolos de Internet del servidor proxy.

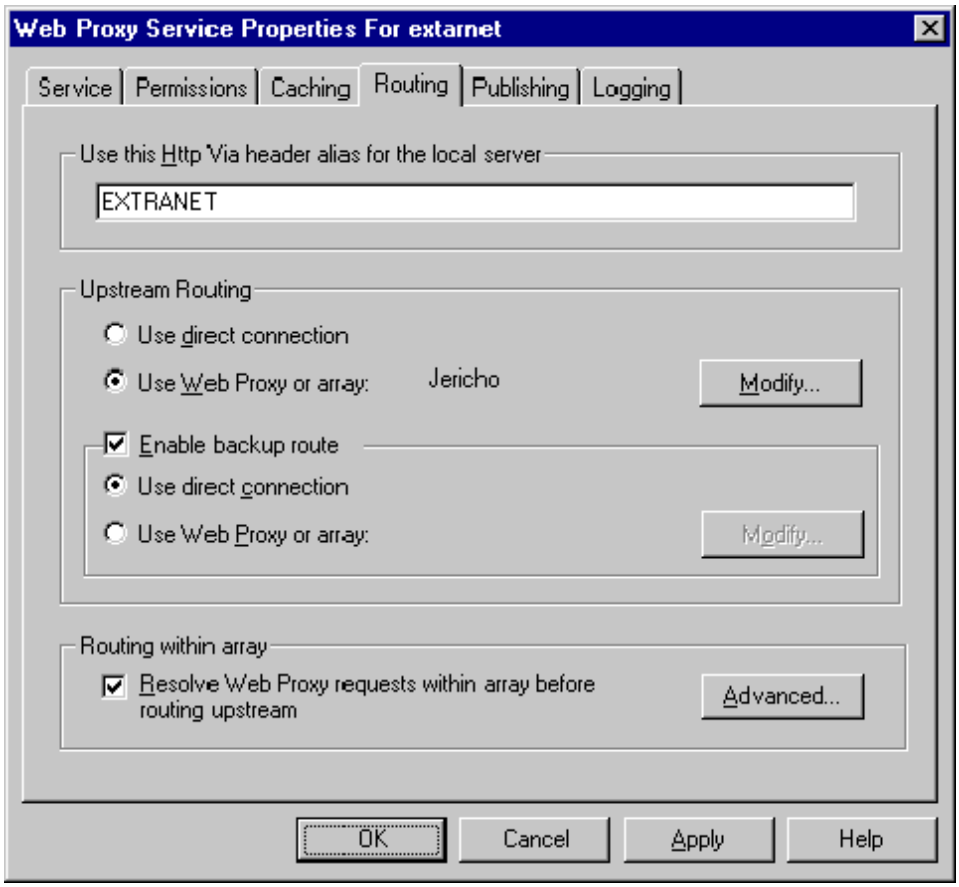
Debemos utilizar el administrador de usuarios del sistema operativo que utilicemos para albergar el servidor proxy y crear uno o más grupos especiales que den acceso a nuestros usuarios a los servicios y que nos simplifiquen a nosotros la administración del servicio proxy.

En esta pantalla podemos, lo primero, activar o no los filtros de usuario mediante el check−box correspondiente, tras lo cual podemos seleccionas cualquiera de los cuatro protocolos o servicios de acceso a Internet y decidir a que usuario o grupos de usuarios vamos a conceder acceso añadiéndolos con el botón de editar en el servicio o protocolo correspondiente.



La pantalla de cacheado nos permite activar la caché, tanto la pasiva como la activa, mediante los check−box correspondientes.

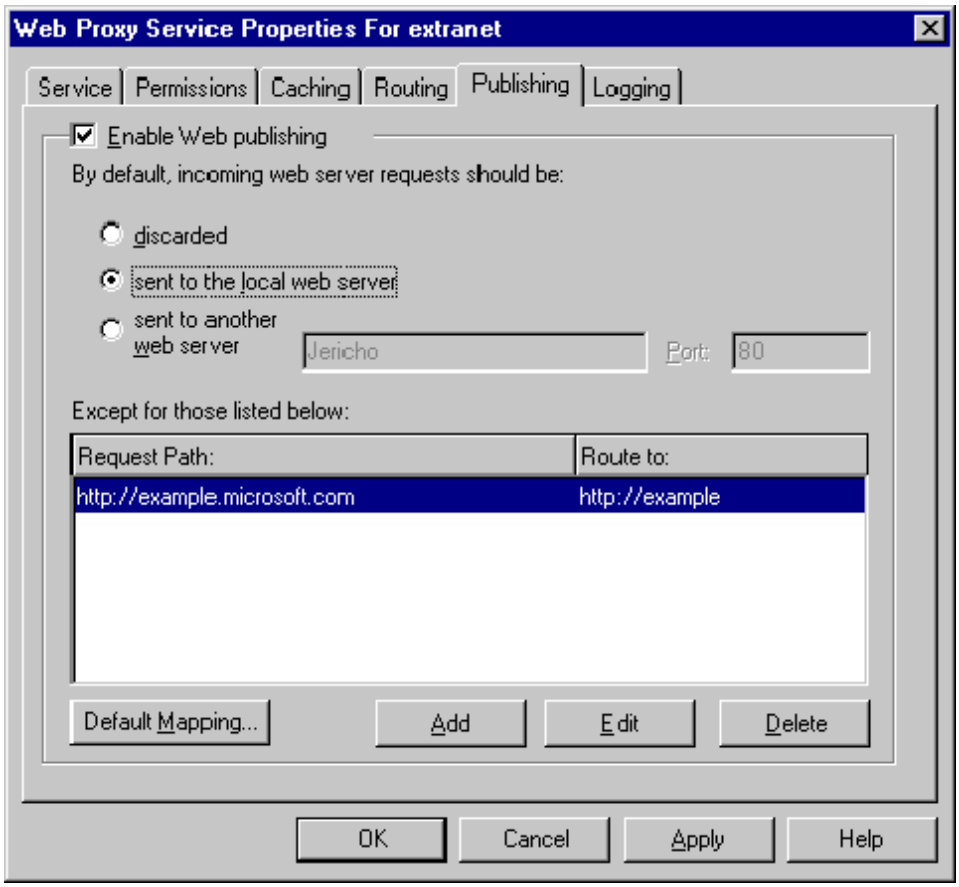
Cuando activamos las caché, nos dan tres opciones, que configuran el nivel de actualización de las páginas o los objetos en la caché, dando el nivel central igual importancia a los dos componentes del proxy, el acceso a datos desde los clientes y las actualizaciones de las páginas desde el exterior; hacia arriba, da mas importancia a los accesos de usuarios, y hacia abajo da mas importancia a las actualizaciones de objetos desde el exterior.



La pantalla de enrutamiento nos permite dirigir peticiones de clientes de objetos de Internet.

Nos permite el enrutamiento de peticiones mediante matrices de servidores proxy o directamente a Internet.

Se utiliza normalmente en conjunción con el cliente WSP instalado a nuestros clientes de red para configurar las opciones del Web Proxy para ellos.

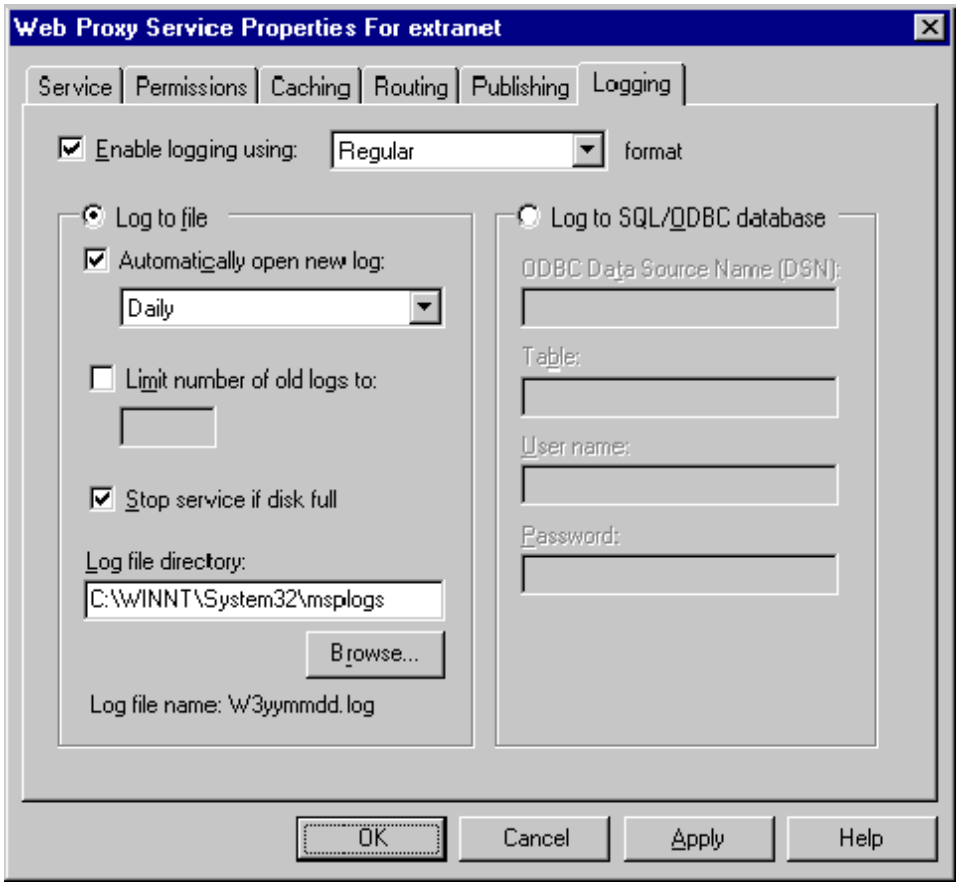


La pantalla de publicación Web nos permite configurar reverse proxies y reverse hosting.

Un reverse proxy es el que atiende a peticiones de Internet y redirige dicha petición al servidor HTTP interno o local.

Mediante reverse hosting, nuestro servidor proxy podrá mantener una lista de múltiples servidores que tienen permiso para publicar en Internet, atendiendo y redirigiendo peticiones de y hacia ellos.

Esta pantalla configura el servidor proxy para responder a peticiones de servidores Web por clientes externos redirigiendo dichas peticiones a nuestro servidor local o a otro servidor de nuestra matriz de servidores proxy.

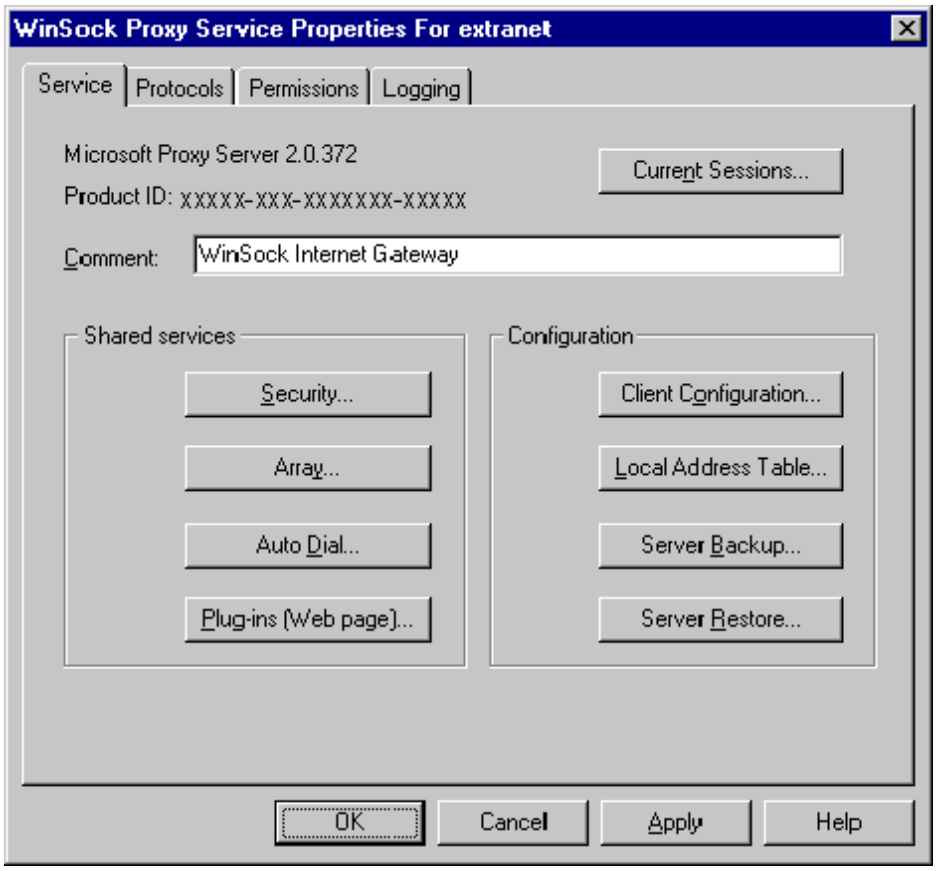


La pantalla de logging nos servirá para almacenar en archivos de texto, en hojas de calculo o en bases de datos la información generada por Microsoft Proxy Server 2.0

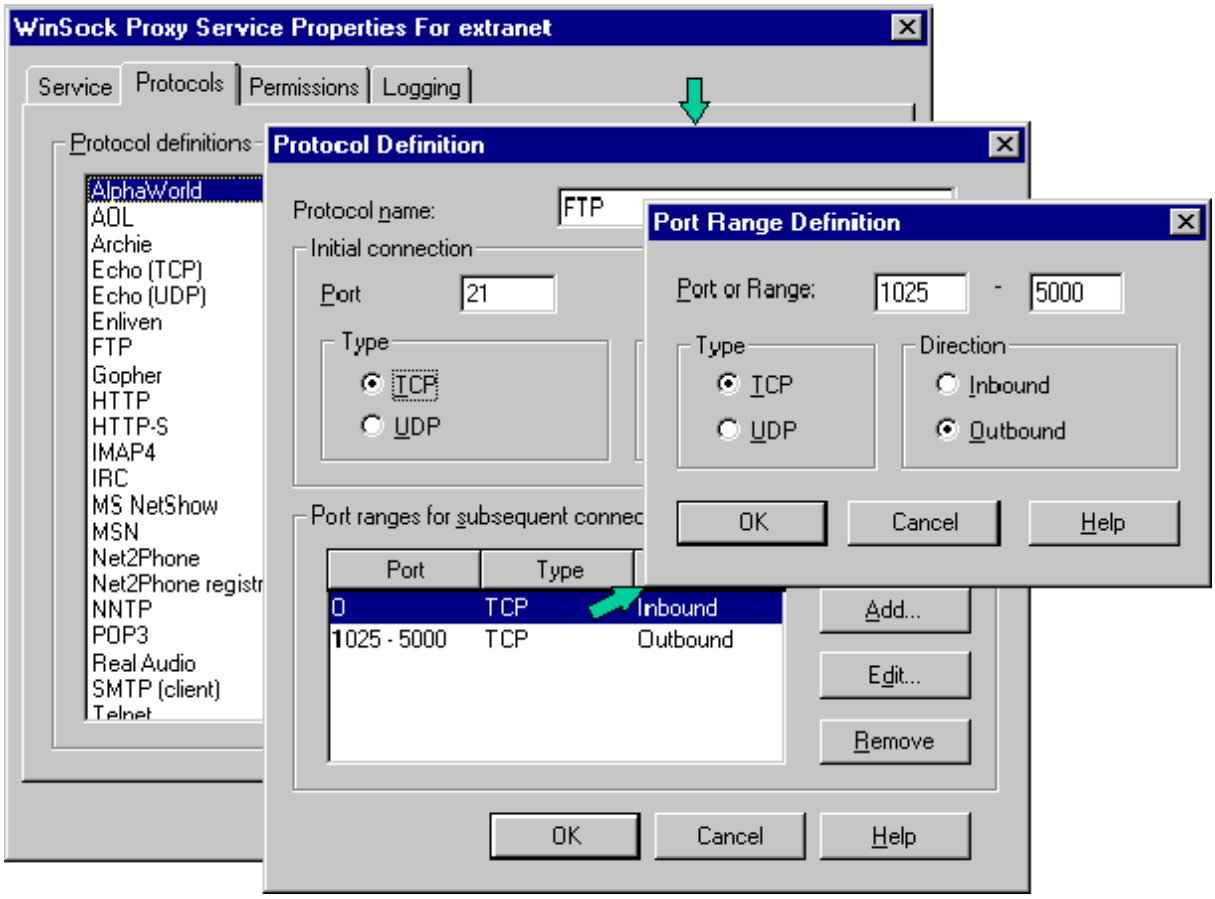
Almacenar esta información resulta útil e importante, ya que forma parte del esquema de seguridad y de las tareas cotidianas de optimización y auditoria de un servidor proxy, por lo que debe de tomarse en serio.

El servidor proxy puede coleccionar información sobre todas las peticiones de Internet que hacen los clientes en texto o sobre el canal SQL/ODBC para almacenar información sobre el servidor, los clientes, la conectividad y sobre los objetos.

- **WINSOCK PROXY**



La pantalla de servicios, como comentamos en el servicio Web Proxy, es común a los tres, siendo ya comentada y explicada en ese servicio.

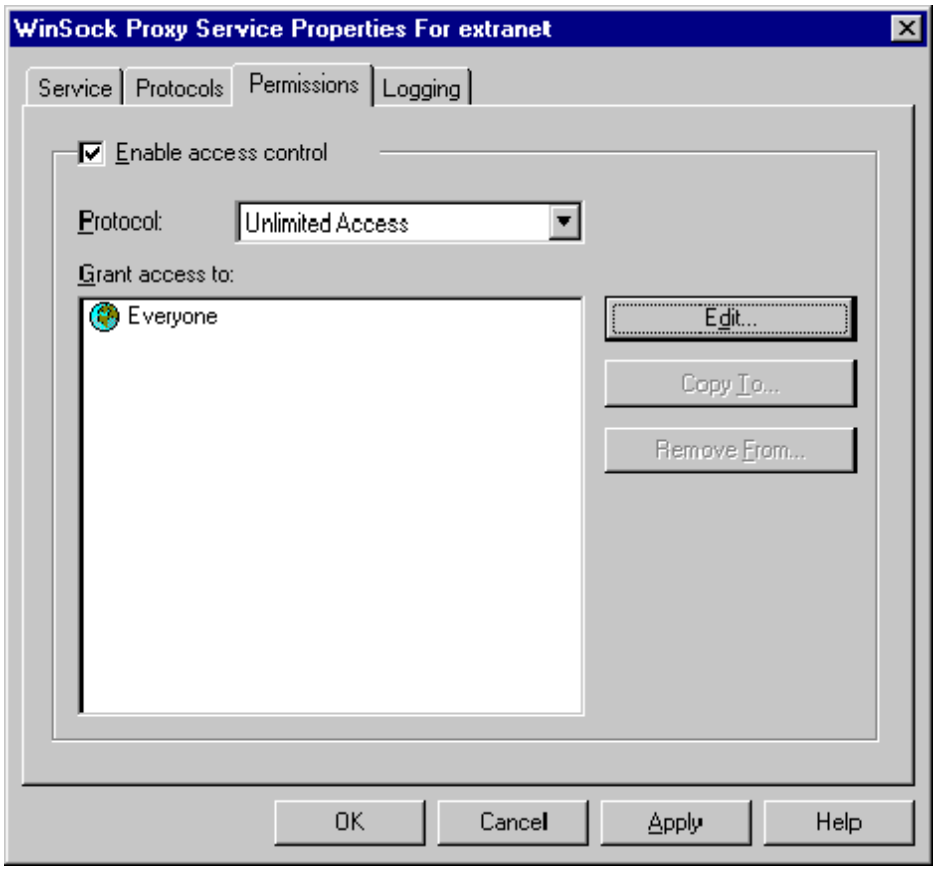


La pantalla de protocolos nos permite determinar el tipo de aplicación socket que se debe usar para acceder a Internet mediante el servicio Winsock Proxy

Podemos crear, configurar y eliminar cualquier protocolo mediante la botonera correspondiente de la pantalla, pudiendo determinar casi cualquier aspecto del protocolo que añadamos o configuremos.

Cuando se crea un nuevo protocolo, este no tiene ningún permiso asociado a él, por lo que deberemos asignárselos manualmente.

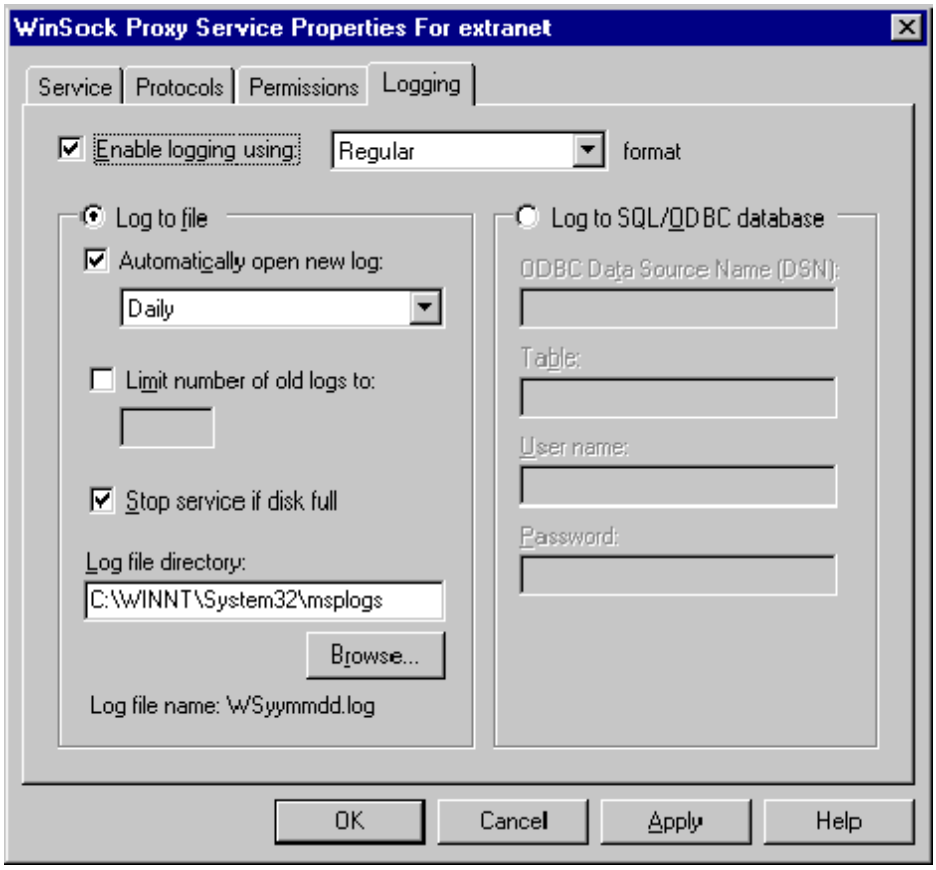
La configuración ideal es tener solo designados aquí los protocolos que realmente vayamos a usar, recomendándose el borrado de todos y la posterior agregación de los que estrictamente usemos, teniendo siempre especial atención sobre aquellos que permitan el acceso desde el exterior hacia nuestra red interna, pues son la mejor puerta que podemos dejar abierta aun hacker para introducirse en nuestro sistema.



La pantalla de permisos, como ya hemos comentado anteriormente, nos servirá para asignar permisos a usuarios y grupos (sobre grupos hechos a medida normalmente), especificados sobre los protocolos anteriormente configurados en la pantalla de protocolos.

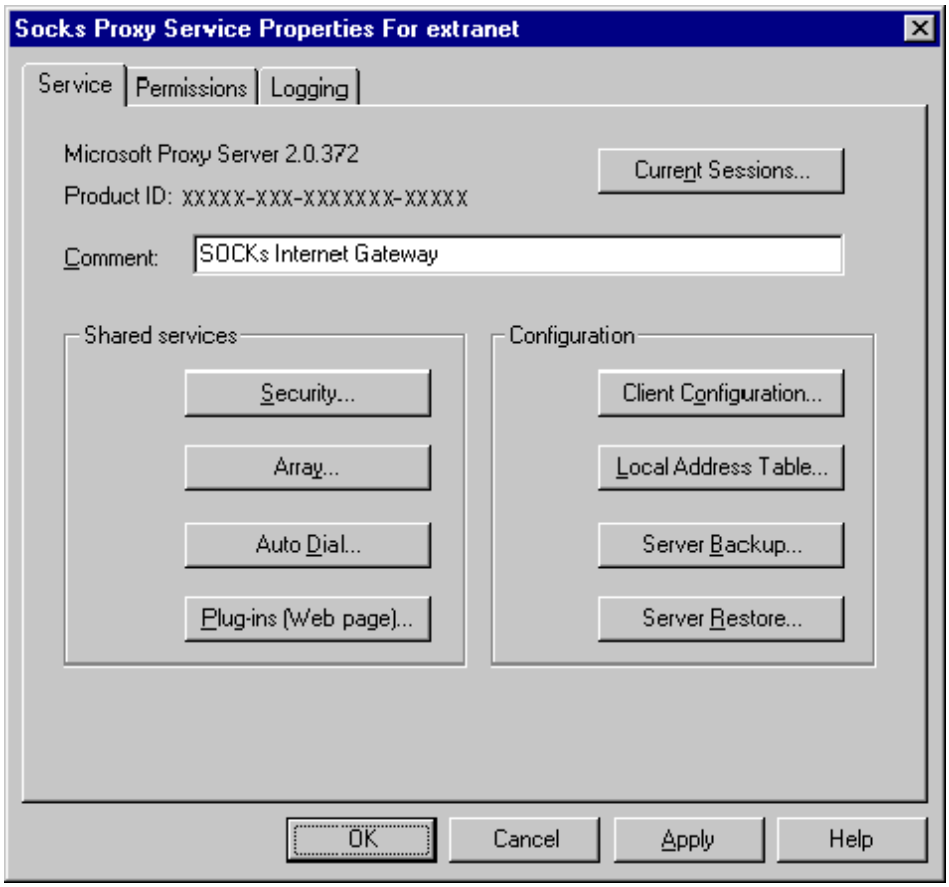
Todo aquel usuario o grupo que aparezca reflejado en la pantalla de acceso, lo tendrá efectivamente.

Ningún permiso en Microsoft Proxy Server 2.0 es implícito, lo que quiere decir que solo los permisos asignados de una manera manual serán los que aparezcan en estas configuraciones de permisos de usuarios y grupos.

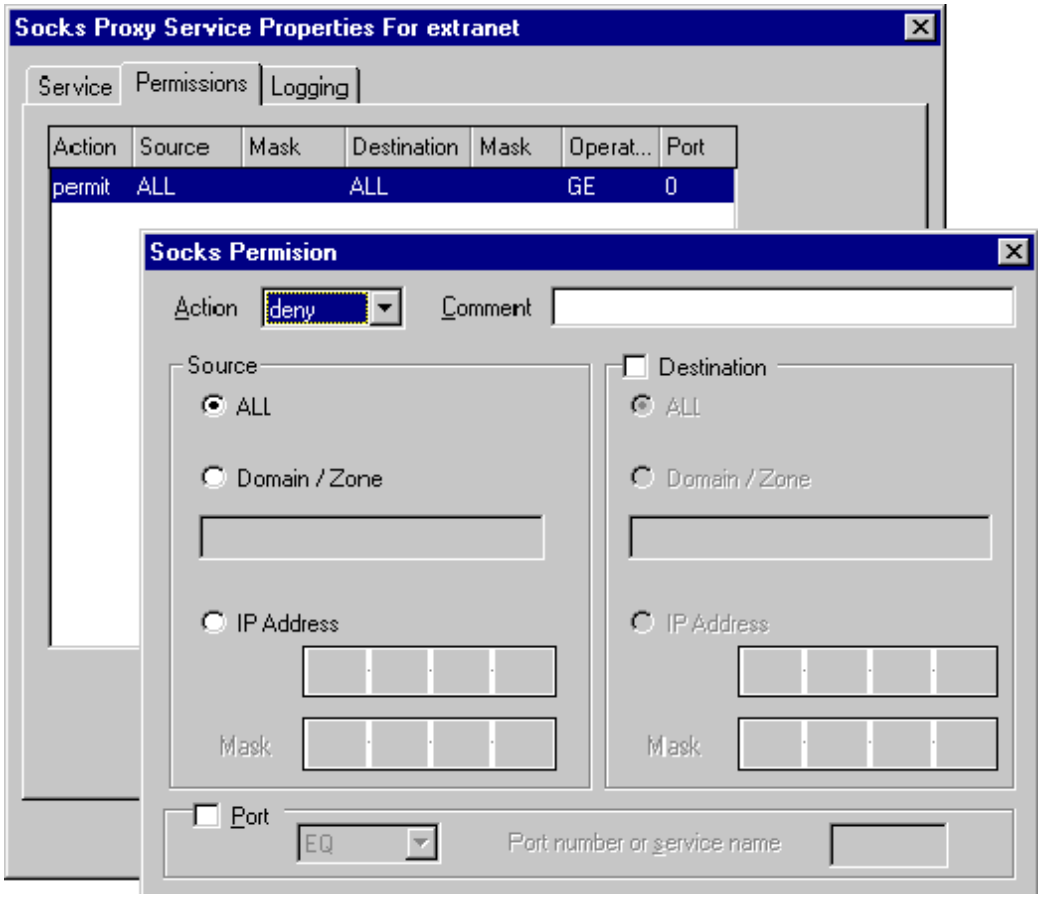


La pantalla de logging ya fue explicada y comentada también anteriormente en el servicio Web Proxy, por lo que remitimos al mismo para la configuración de la información recibida por los distintos servicios de Microsoft Proxy Server 2.0

- **SOCKS PROXY**



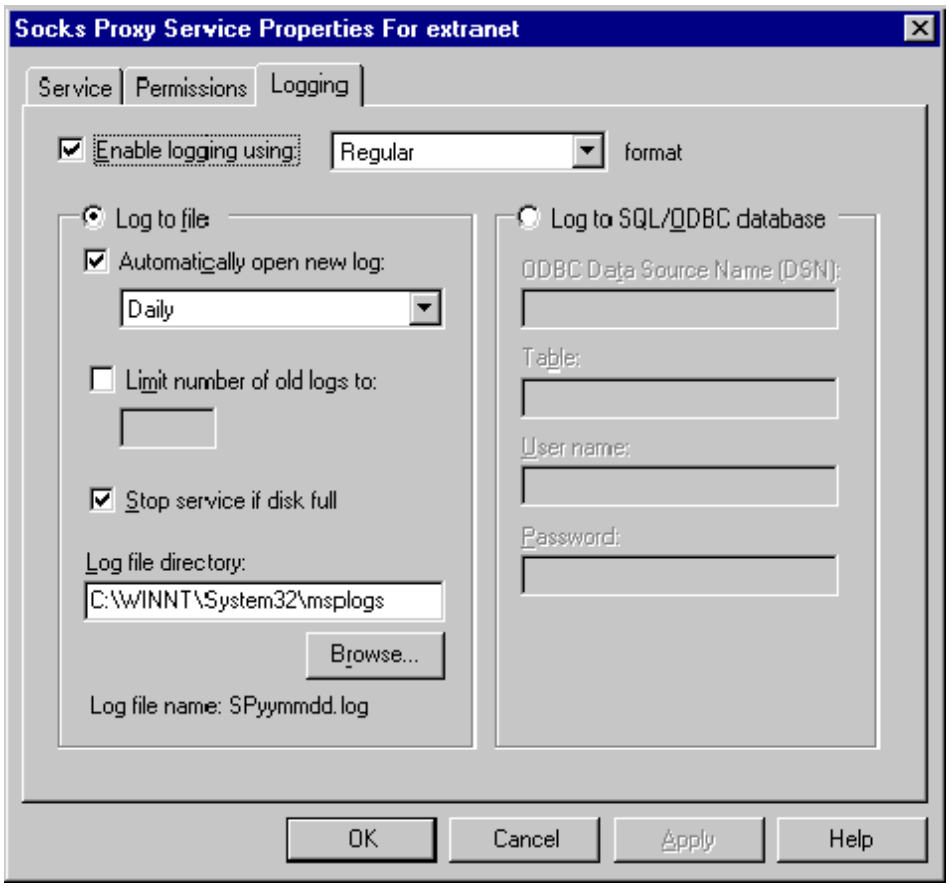
La pantalla de servicios, como comentamos en el servicio Web Proxy, es común a los tres, siendo ya comentada y explicada en ese servicio.



La pantalla de permisos, como las demás explicadas anteriormente, se refieren a los permisos sobre usuarios y grupos (normalmente creados a tal efecto) que van a tener acceso al canal de comunicación o socket

Cada uno de los canales o sockets que tengamos definido tiene sus propias configuraciones a determinar, así como sus permisos específicos a usuarios y grupos.

Podemos configurar aquí los destinos, orígenes, tipos de puerto, y especificaciones especiales de cada uno de ellos.



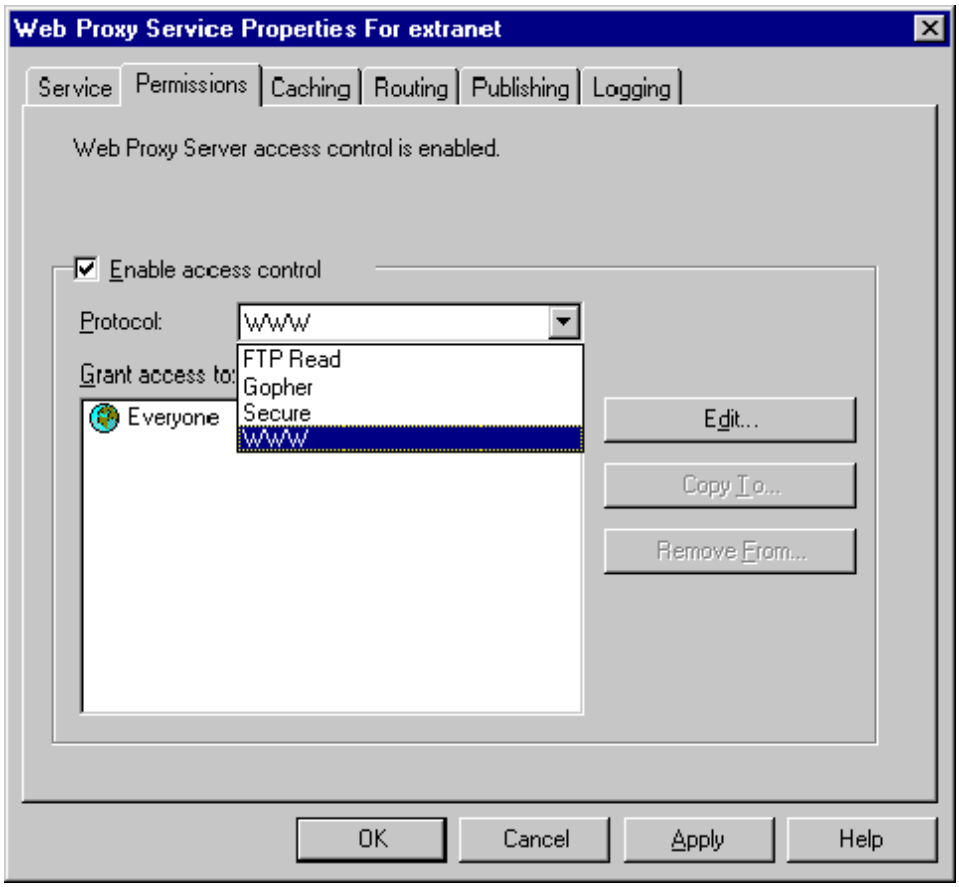
La pantalla de logging ya fue explicada y comentada también anteriormente en el servicio Web Proxy, por lo que remitimos al mismo para la configuración de la información recibida por los distintos servicios de Microsoft Proxy Server 2.0

Tema 5.− Control de acceso

- **Control hacia fuera de la red**

Para controlar el acceso hacia fuera de nuestra red tenemos tres métodos que podemos utilizar para ello:

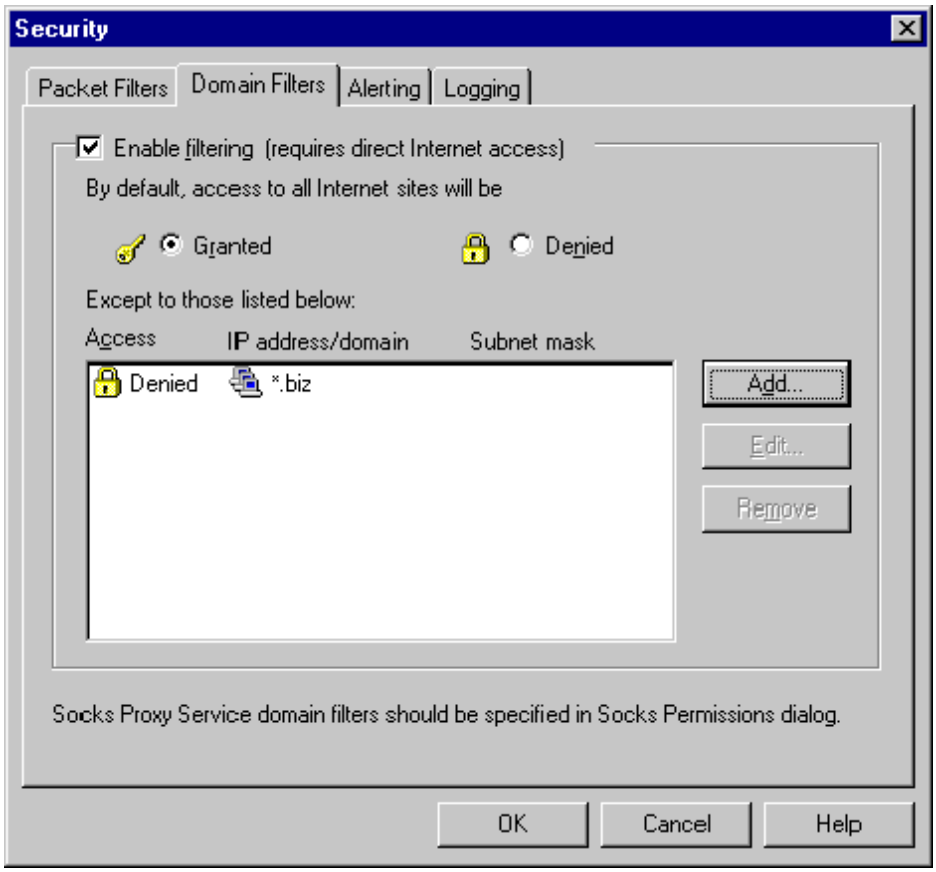
- Control del acceso mediante los servicios



La regla básica a tener en cuenta es SOLO conceder permisos a los usuarios que de verdad necesiten de ellos. Si no los necesitan, no loa activaremos como regla de seguridad básica. Normalmente vamos a limitarlos a uno o dos grupos creados especialmente para tal fin y no más de esos grupos especialmente creados para tal efecto.

El servicio que vamos a usar para ello es, como vemos en la imagen, en Web Proxy, ficha permisos, y ahí seleccionaremos el servicio a permitir o denegar y los grupos que vamos a incluir especialmente en ellos.

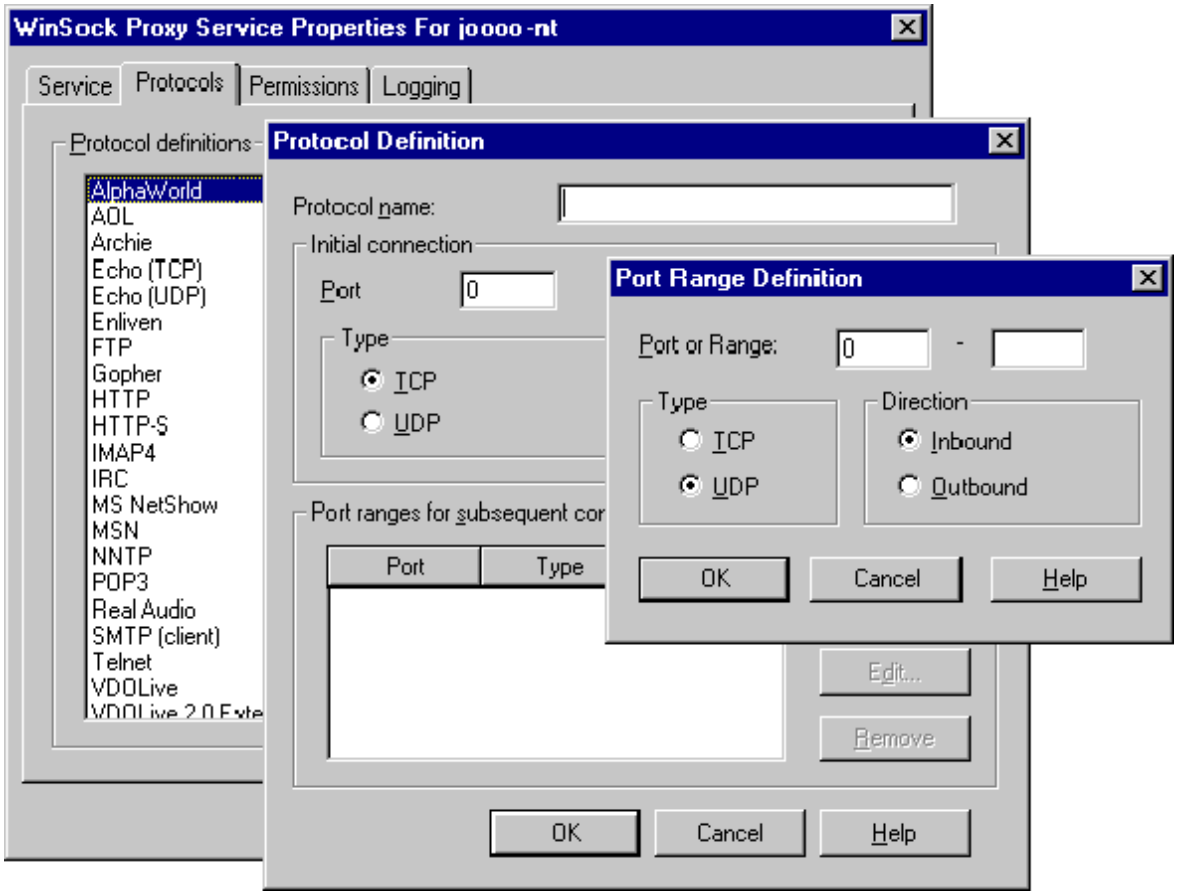
- Control del acceso mediante la IP, la subred o el dominio



Al determinar este tipo de seguridad lo primero que tenemos que determinar es si queremos denegar o permitir generalmente el acceso, eligiendo el grupo mas grande, y especificando luego las excepciones a la regla (si a casi todos los usuarios les denegamos el acceso excepto a 5, el grupo general será denegar, con la s 5 excepciones de los usuarios que sí tienen acceso a los servicios de Internet).

Es muy importante planificar y seleccionar antes de ejecutar este paso, pues podemos perdernos en complicadas configuraciones de seguridad que nos reporten un trabajo administrativo grande, pudiendo hacerlo de maneras bastante mas simplificadas y fáciles para nosotros como administradores.

- Control del acceso mediante el puerto

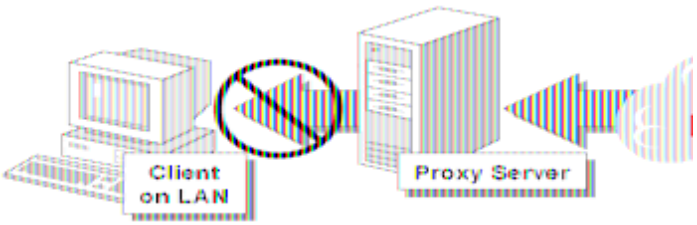


Con el servicio Winsock Proxy, podemos controlar el acceso a Internet especificando que puerto es usado por los protocolos TCP y UDP, como ya explicamos en el tema 4.

- **Control hacia adentro de la red**

Microsoft Proxy Server 2.0 y nuestra red solo van a tener una presencia intermitente en Internet si la interacción con la red de redes se hace solo de dentro hacia fuera, limitando en mucho el riesgo de intromisiones externas a nuestra red.

En el momento que tenemos que proveer de acceso a usuarios que se encuentran en el exterior de nuestra red, los riesgos aumentan considerablemente a razón del número de usuarios a los que tengamos que abrir puertas de nuestra red.



Cuando implementamos Microsoft Proxy Server 2.0, la red se encuentra completamente asegurada de dos maneras: forzando a que las conexiones utilicen la LAT para comunicarse (o IP forwarding), y deshabilitando la escucha de puertos de entrada, por lo que solo los que nosotros habilitemos manualmente son los que realmente nos dan servicio como tales.

IP forwarding permite el paso libre de paquetes entre las dos tarjetas de red, la interna y la externa, lo que expone en efecto la red a ataques externos.

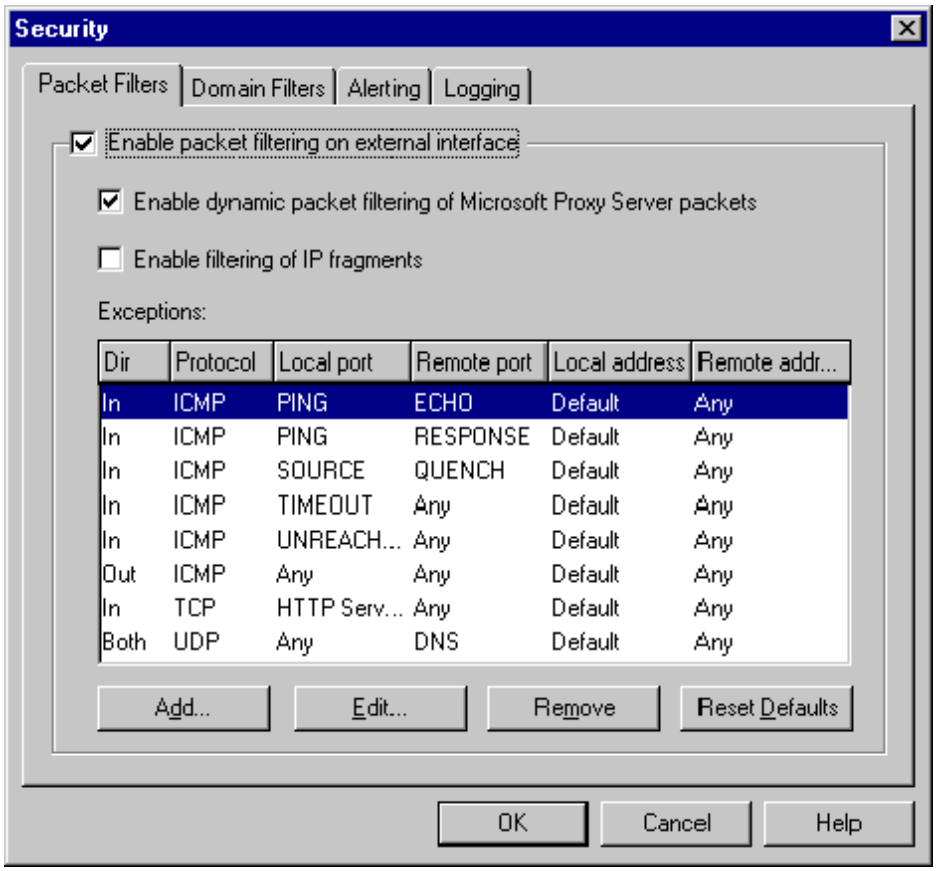
Si nos aseguramos que la red interna funcione con TCP/IP, podemos asegurarnos de que todos los paquetes de información se enrutan a través del servidor proxy, lo que previene filtraciones de datos del exterior no autorizados.

Para conseguirlo, tenemos que desmarcar la casilla de *Permitir IP Forwarding* de las propiedades del protocolo TCP/IP.

Debemos considerar también la posibilidad de implementar Microsoft Proxy Server 2.0 en un PDC o DC de bosque con una relación de confianza unidireccional siempre que sea posible, en un dominio aparte de nuestra red como protección adicional, limitando los ataques a esa máquina en especial, preservando el resto de nuestra red de intrusos.

Recomendaciones generales de seguridad:

- Dar permisos a usuarios SOLO cuando sea necesario
- Reforzando las políticas de contraseñas y seguridad
- Renombrando la cuenta por defecto Administrador e incluso el grupo entero de Administradores, tanto el global como el local.
- Usar las contraseñas y usuarios de NT para conceder los accesos a los servicios (NT Challenge/Response)
- Ser muy conservador al habilitar puertos de entrada
- Manejar cuidadosamente los puertos TCP/IP
- NUNCA DAR ACCESO ILIMITADO a no ser estrictamente necesario, y siempre a usuarios muy específicos y controlados



El filtrado de paquetes intercepta y evalúa esos paquetes que llegan desde Internet antes de que alcancen al servidor proxy.

Podemos configurarlo para que acepte o deniegue paquetes específicos, datagramas o fragmentos de paquete que puedan pasar por nuestro servidor proxy.

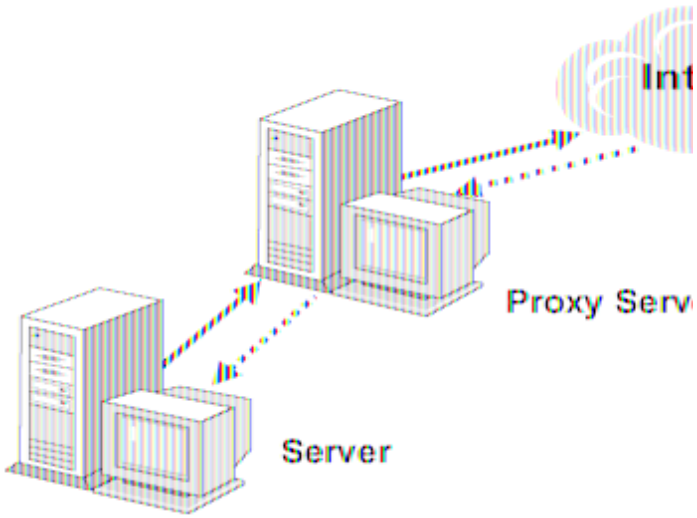
Dynamic Packet Filtering designa puertos para que se abran estrictamente el tiempo que necesiten para recibir, transmitir, o las dos opciones, cerrando entonces los puertos inmediatamente, lo que ofrece un alto nivel de seguridad con mínima administración. Es altamente recomendable su activación.

Static Packet Filtering nos permite un nivel de control mucho mas especifico, agregando carga administrativa a nuestra labor como administradores, pero asegurándonos que solo los paquetes específicos configurados por nosotros sean los únicos con acceso por parte de los usuarios.

Microsoft Proxy Server 2.0, al integrarse con IIS, toma ventaja de esa aplicación a usar SSL Tunneling de una manera predeterminada, el cual soporta encriptación de datos y autentificación de servidores.

Si queremos usar Point−to−Point Tunneling Protocol (PPTP) para proveer de seguridad adicional a los usuarios, podemos configurar el servidor proxy para que acepte y enrute este tipo de paquetes.

Tema 6.− Publicación en Web segura



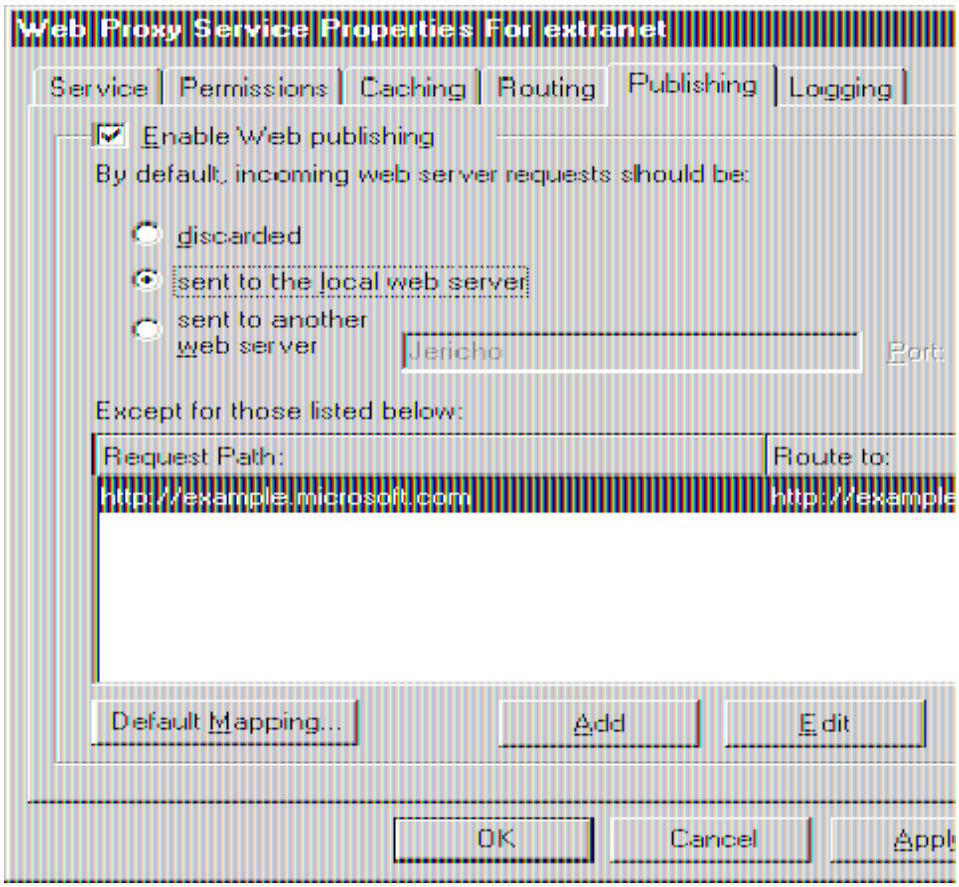
La publicación se refiere al guardado de material en un servidor Web para que puedan ser accedidos por cualquiera con acceso Web: Esto se aplica tanto a Internet como a las Intranets, o redes locales que intercambian información de manera Web.

Publicar en Internet aumenta el riesgo de exposición de nuestra red a usuarios externos, comprometiéndola, al mantener nuestro servidor una presencia continua en Internet, pudiendo ser objeto de ataques mediante exploradores de IP's u otros métodos más o menos eficaces de intrusión.

Microsoft Proxy Server 2.o usa el servicio reverse proxy para impersonalizar el servidor hacia Internet sin perder, sin embargo, los servicios y funcionalidad internas.

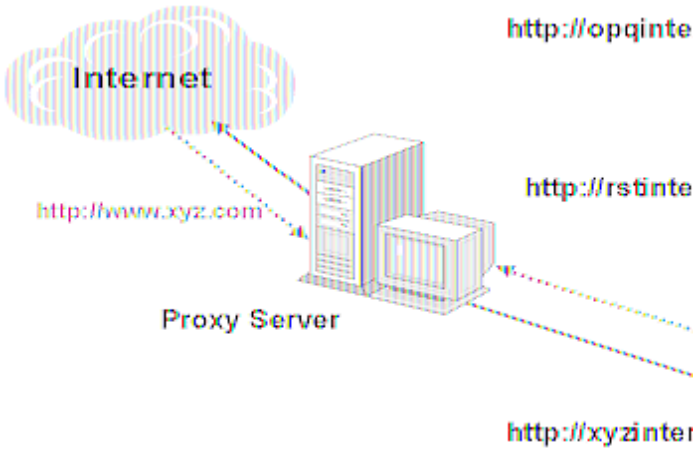
Reverse Proxy provee al servidor proxy de la característica de poder procesar peticiones entrantes hacia un servidor Web y de responder en su lugar. Se denomina reverso porque las peticiones son redirigidas hacia un servidor Web interno, en vez de hacerlo hacia uno de Internet, que sería el proceso normal.

Reverse Hosting mantiene una lista de los servidores con permisos de publicación en Internet. Lo que provee al servidor proxy de posibilidad de respuesta hacia estos servidores, sin ninguna evidencia ni rastro de que los datos pasen por el servidor proxy antes de dirigirse al servidor Web, por lo que la seguridad no se encuentra comprometida al seguir existiendo un solo camino de paso hacia Internet.



Durante la instalación de Microsoft Proxy Server 2.0, los servicios de Internet (IIS) son automáticamente configurados para no escuchar peticiones desde Internet, las que son ignoradas. Es muy recomendable utilizar máquinas distintas para IIS y para Microsoft Proxy Server 2.0, e incluso situar los clientes en dominios distintos para evitar interferencias y conflictos.

Las excepciones están contempladas en la opción de *Except*, donde podremos configurar la URL entrante y a cual debe redirigirse ésta una vez filtrada por Microsoft Proxy Server 2.0, exceptuando los servicios FTP y Gopher, en los puertos 21 y 70, respectivamente, para los que tendremos que establecer una configuración completamente manual.



Reverse hosting, entonces, nos servirá para que cualquier servidor en nuestra LAN pueda publicar en Internet, creando una ruta inversa al mapear una URL a un servidor Web especifico de nuestra red interna.

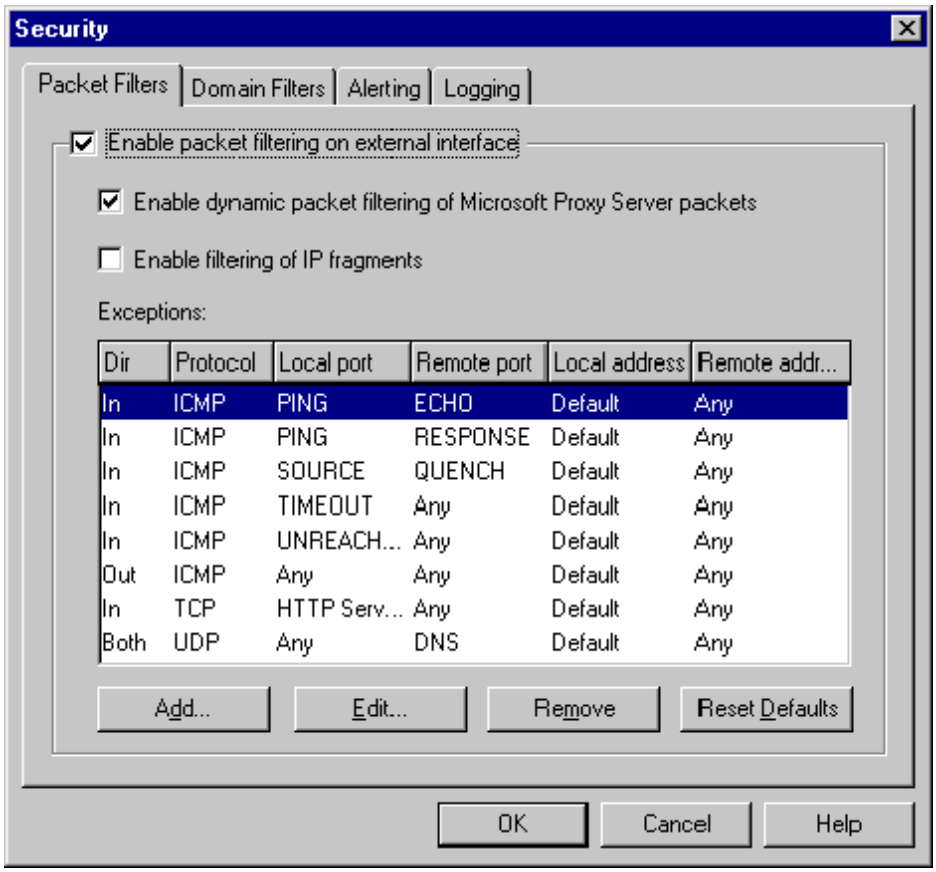
Tema 7.− Filtrado de paquetes

Las características de seguridad de Microsoft Proxy Server 2.0 nos permiten controlar el flujo de información de y desde nuestro servidor proxy, interceptando y permitiendo o denegando el acceso a servicios específicos o mandando alertas cuando paquetes o acciones sospechosas ocurran en nuestra LAN.

Filtrado de paquetes

Packet filtering intercepta y evalúa los paquetes antes de que pasen por los niveles altos de los protocolos o que lleguen a las aplicaciones, aplicando filtros predeterminados, actuando así de Firewall o cortafuegos.

Hay que tener en cuenta que este aspecto de seguridad del proxy solo se aplica a la tarjeta de red externa, la que conecta la red al exterior, a Internet, y que cada servidor proxy SOLO acepta una tarjeta al exterior.

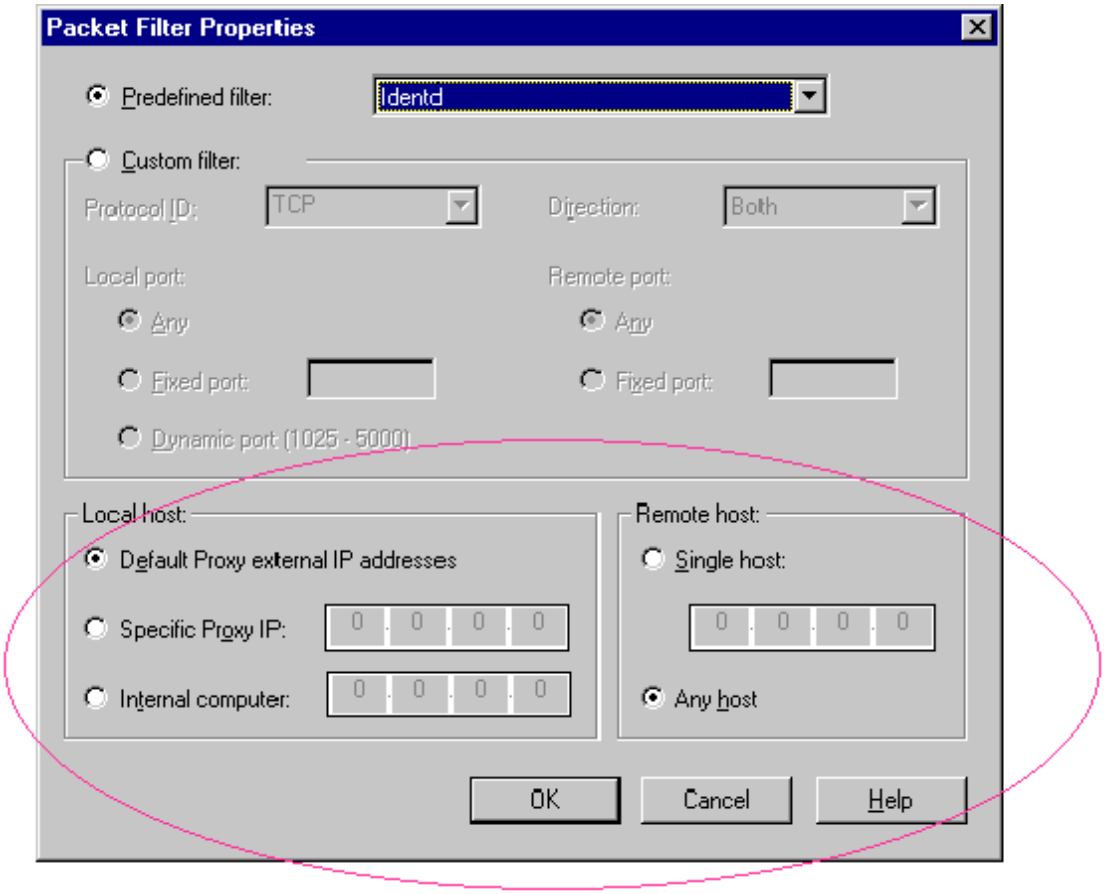


La pantalla del filtrado de paquetes la podemos encontrar en cualquiera de los tres servicios del proxy. Cada entrada dentro de las excepciones especifica parámetros de configuración de un tipo especifico de paquete.

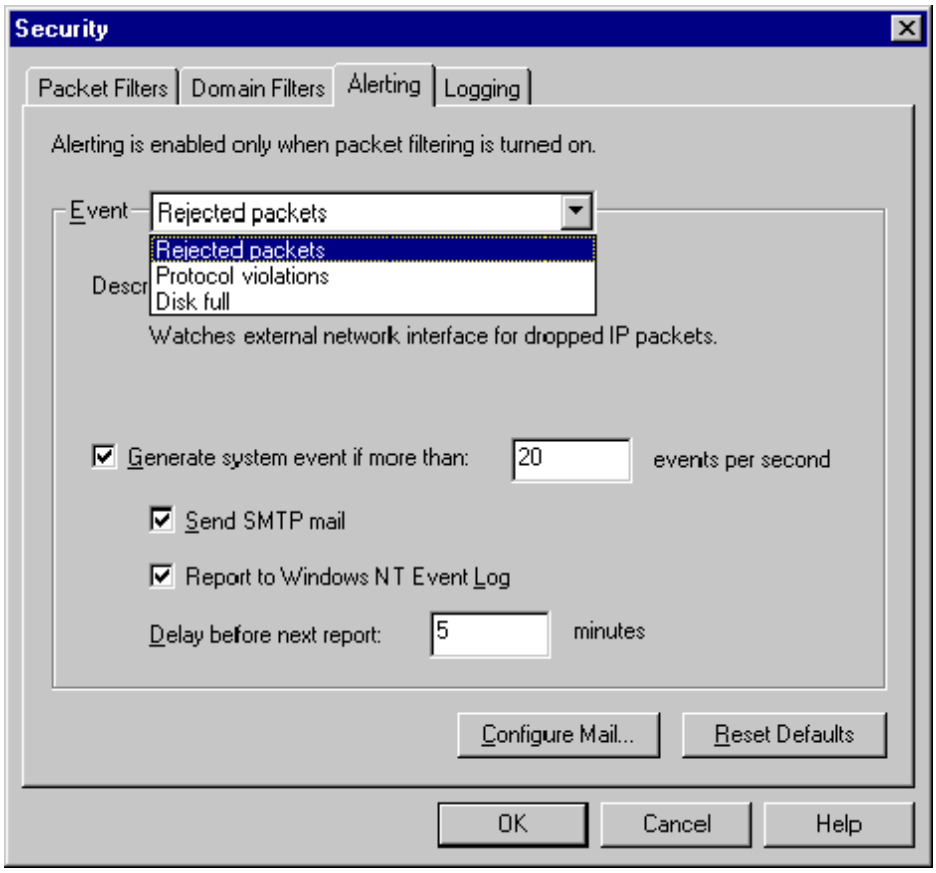
Hay que tener en cuenta que algunos protocolos, como PPTP, necesitan mas de un filtro para funcionar correctamente, por lo que es muy conveniente informarnos y documentarnos adecuadamente antes de la implantación de estos filtros.

Tener en cuenta siempre que los filtros de paquete definen EXCEPCIONES, por lo que si no hemos definido un filtro para un puerto especifico, no tendrá escucha efectiva en ese puerto.

Para crear o modificar filtros de puerto, al presionar el botón de añadir (add) o modificar (edit), aparecerá la pantalla de configuración de esos filtros.



Recordar siempre que Microsoft Proxy Server 2.0 soporta múltiples direcciones IP asignadas a la misma tarjeta de red externa.



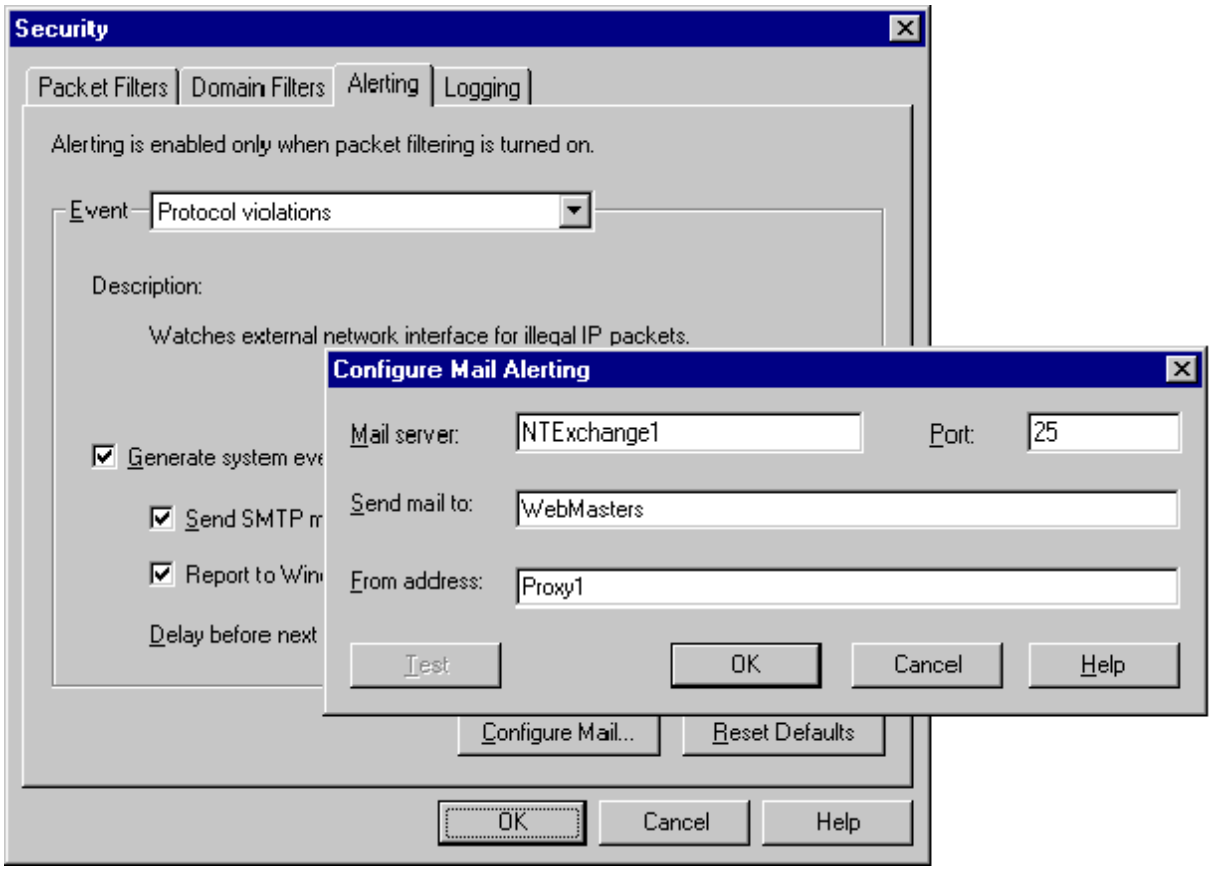
Las alertas corresponden a los resultados de la monitorización de eventos o procesos que ocurren en nuestro servidor proxy.

Es obligatoria la activación del filtrado de paquetes (packet filtering) para que las alertas puedan estar disponibles.

Eventos para los que podemos generar alertas:

- Paquetes rechazados (rejected packets) por nuestra tarjeta de red externa.
- Violaciones de protocolo (protocol violations), o paquetes sin la forma adecuada del protocolo del que dicen que proceden.
- Disco lleno (disk full), o espacio insuficiente en disco duro

Configuración de alertas por E−mail

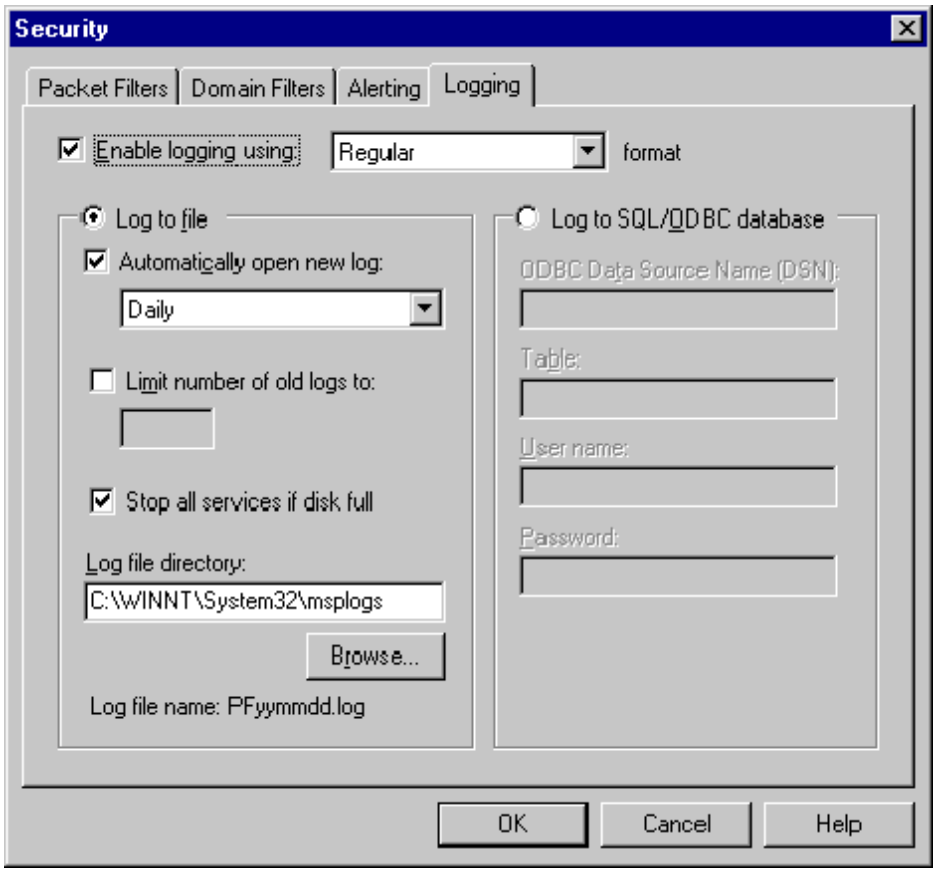


Las alertas pueden ser enviadas por SMTP a los buzones designados, recomendándose el enviado a servidores de correo internos, no externos, por causas obvias de seguridad.

Para mandar un mensaje SMTP mediante un servidor Exchange se requieren cuentas de NT legítimas, por lo que la combinación de estas cuentas con la seguridad del servidor proxy será decisiva en la seguridad del servidor.

Para la utilización de este servicio, hay unos pasos previos que debemos ejecutar antes:

- Crear una cuenta de usuario de correo
- Crear un perfil MAPI nuevo o seleccionar uno existente
- Instalar el software de cliente de correo (outlook, eudora)
- Configurar el cliente de correo para que se inicie automáticamente e iniciarlo para ser capaz de recibir correos.



Las alertas del filtrado de paquetes se pueden almacenar en un archivo log dedicado o en una base de datos creada a tal efecto. El archivo log se guarda predeterminadamente en %systemroot%/system32/msplogs/Pfyymmdd.log

El archivo recoge información sobre las áreas:

- Información de los servicios

- Fecha de recepción
- Hora de recepción

- Información remota

- Dirección IP de la máquina que origina el paquete
- Puerto que es usado para comunicarse con la máquina remota
- Protocolo que se usa para la comunicación

- Información local

- Dirección IP de la máquina destino (normalmente el servidor proxy)
- Puerto destino usado para la comunicación

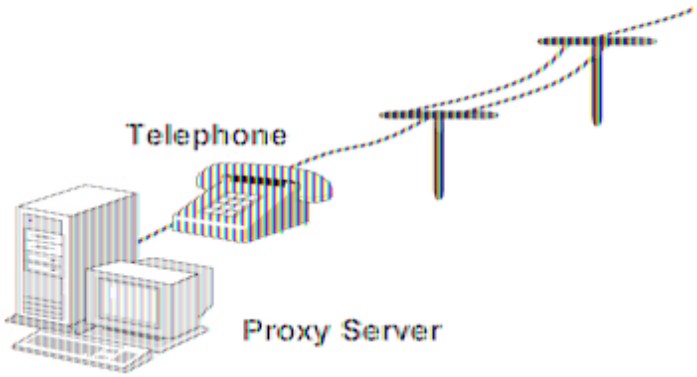
- Información de los filtros

- Valor de acción (aceptado, rechazado)
- Interface por el que entra la información (para TCP/IP v6)

- Información de los paquetes

- Cabecera IP entera del paquete
- La parte del paquete IP que ha activado la alerta

Tema 8.− Uso de Microsoft Proxy Server 2.0 con conexiones Dial−Up



Microsoft Proxy Server 2.0 puede ser configurado para llamar automáticamente a un ISP (Internet Services Provider) para establecer una conexión a Internet. Esta característica se denomina AutoDial.

¿En qué casos ocurre el AutoDial?

- Cuando no se encuentra un objeto en la caché
- Con el servicio Winsock proxy, a petición de los clientes
- Con el servicio Socks Proxy, a petición de los clientes

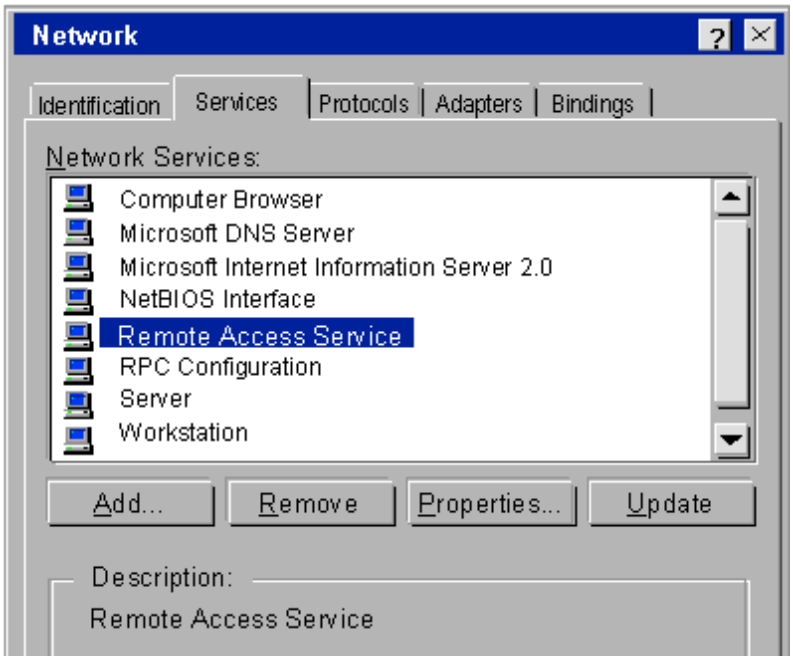
La característica AutoDial suele usarse para minimizar el tiempo que un servidor proxy permanece conectado a Internet, reduciendo riesgos y costes, pudiendo también utilizarse como línea de apoyo, en el caso en que nuestra línea habitual hacia Internet está ocupada o caída.

Utilizada en conjunción con la característica de los usuarios de limitar el tiempo de conexión, nos da un sistema de seguridad fiable y robusto, permitiendo configurar la cantidad de horas diarias de que nuestros usuarios hacen provecho cada dia.

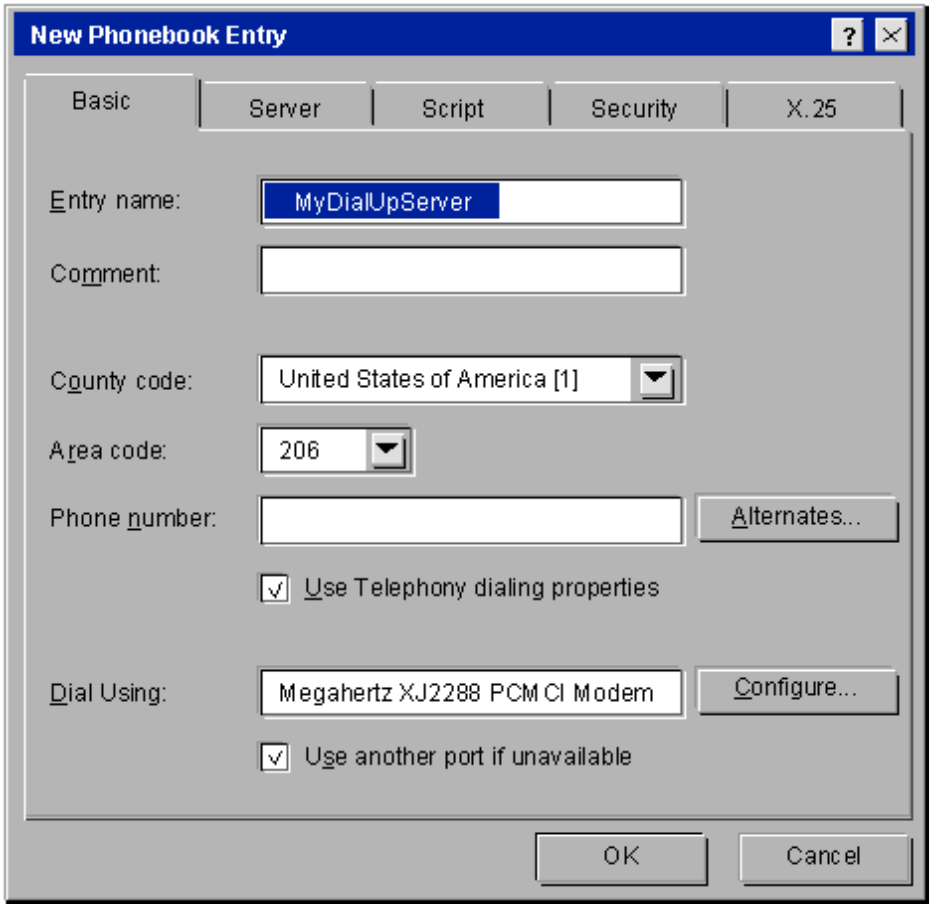
Para la correcta implementación de AutoDial, se deben seguir estos pasos:

- Instalación del Servicio de Acceso Remoto (RAS) de Microsoft Windows NT Server 4.0 o Windows 2000 Server

    - Instalación de RAS



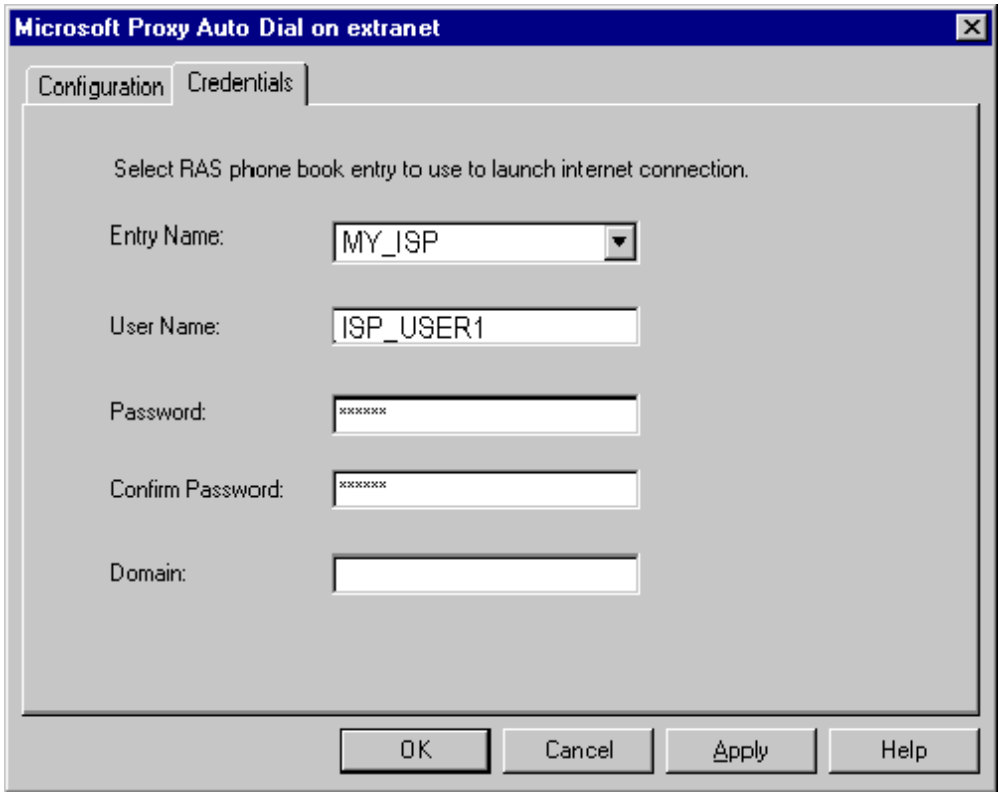
- Configuración de las entradas de teléfono



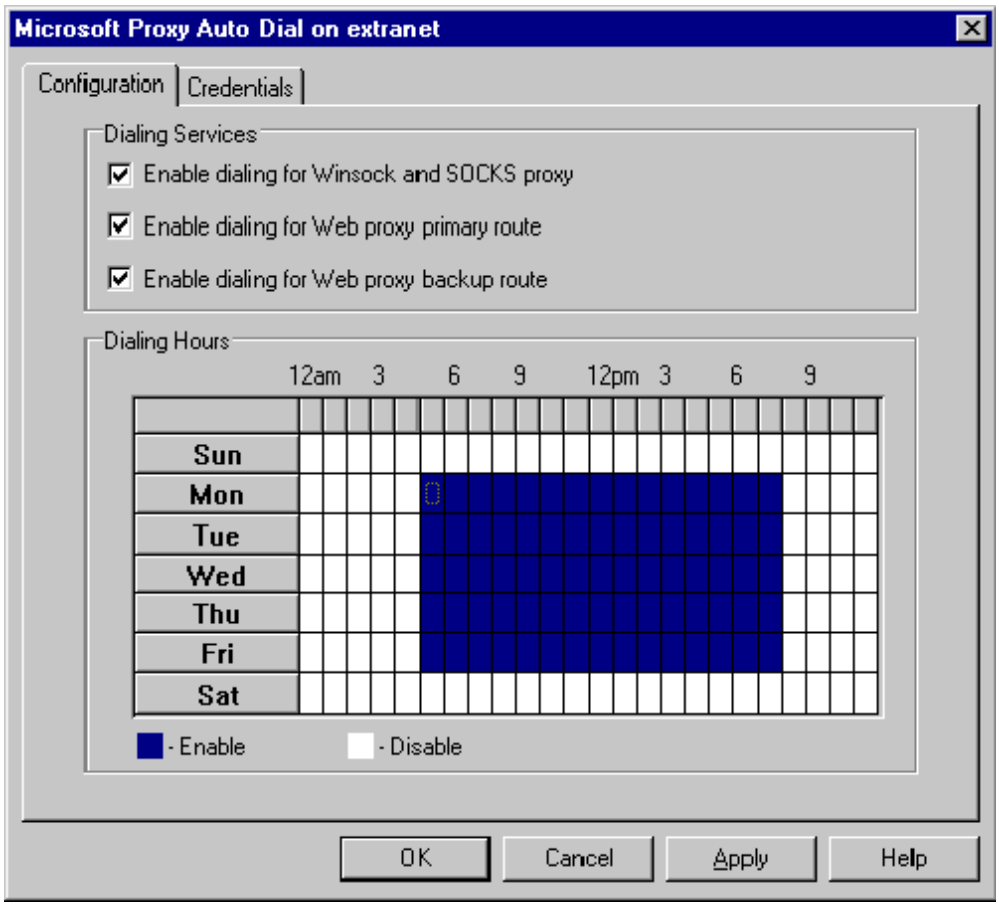
- Configuración de los servicios del RAS

- Configuración del servicio del proxy AutoDial

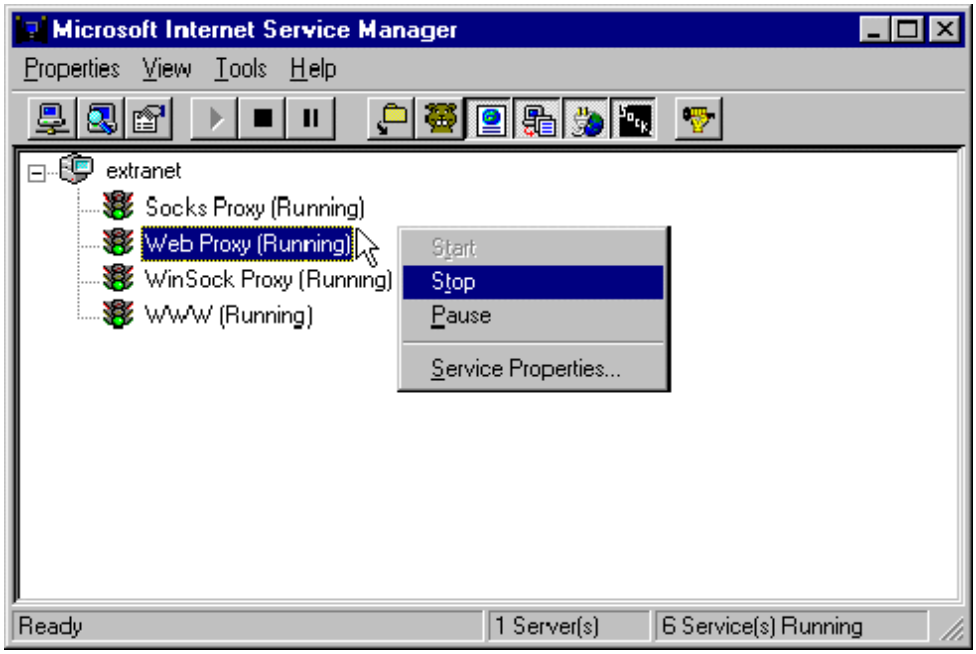
- Configuración de las credenciales de AutoDial



- Configuración de las horas de llamada de AutoDial



- Reinicio de los servicios del servidor proxy



Tema 9.− Configuración de múltiples servidores Proxy

Una Red de Area Local (LAN) puede soportar mas de una gateway de servidor proxy, siendo un tema importante el cómo balancear la carga de una manera equitativa a todos los servidores proxy de la red.

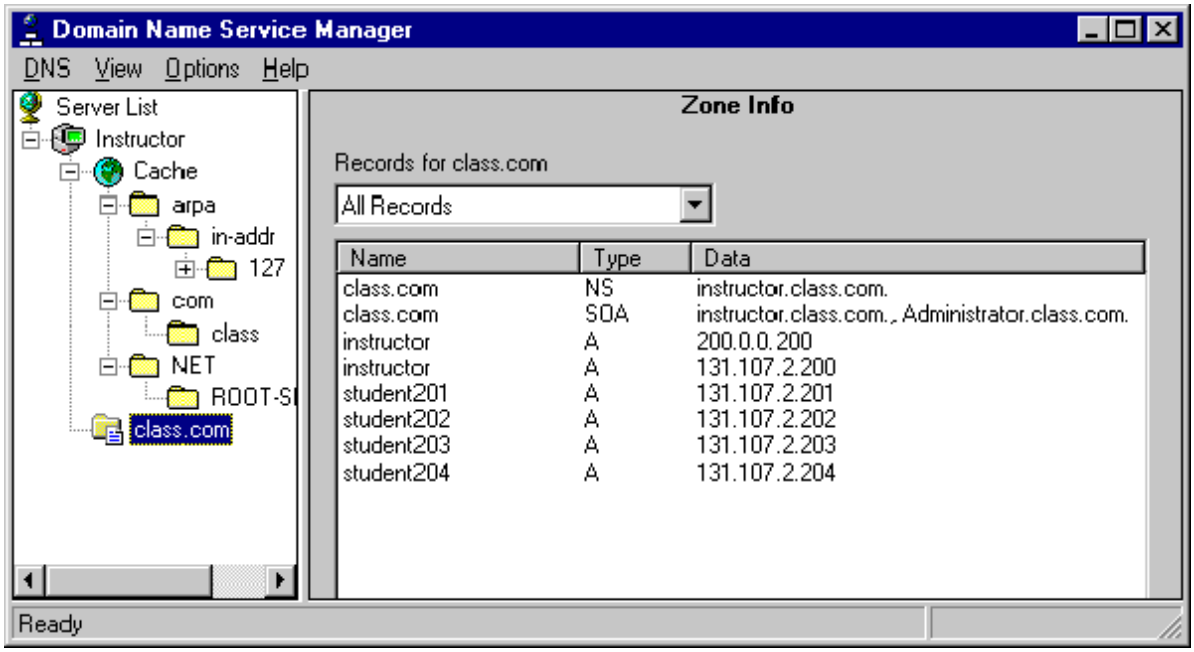
Configuración mediante un servidor DNS:

El Sistema de Nombres de Dominio (DNS) provee al S.O. de una jerarquización de directorios que permite distinguir cualquier nombre de Internet de los demás.

El InterNIC (Internet Network Information Center) requiere que los sitios con conexión directa a Internet, como los ISP, dispongan de dos servidores DNS en dos localizaciones geográficas y en dos máquinas distintas como alternativa a fallos.

El DNS se basa en registros, siendo los más importantes:

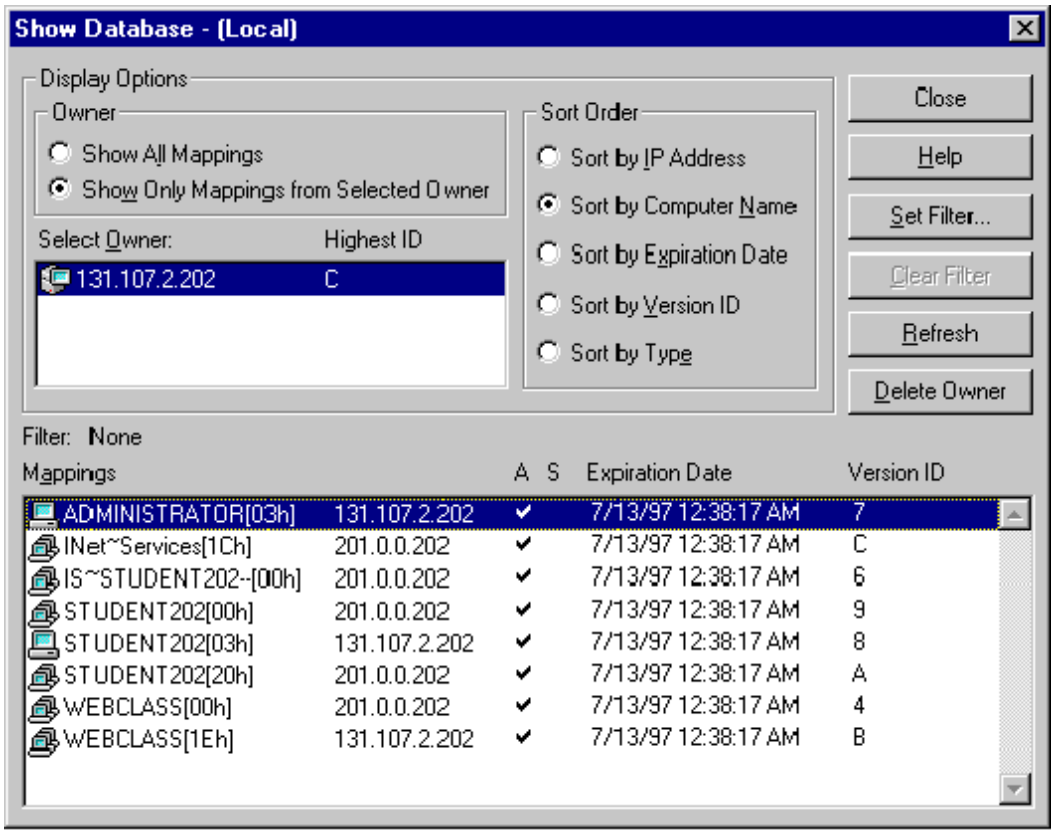
- **SOA** (Start Of Authority), que es el usuario con nivel de administración que puede manipular la zona
- **NS** (Name Server), que es la máquina en la que está instalada en si la zona DNS
- **A** (Host), que son los que realmente relacionan los nombres de máquinas con direcciones IP
- **CNAME**, que son alias de las entradas A y redirigen a otro punto de la zona (Por ejemplo, miempresa.com)



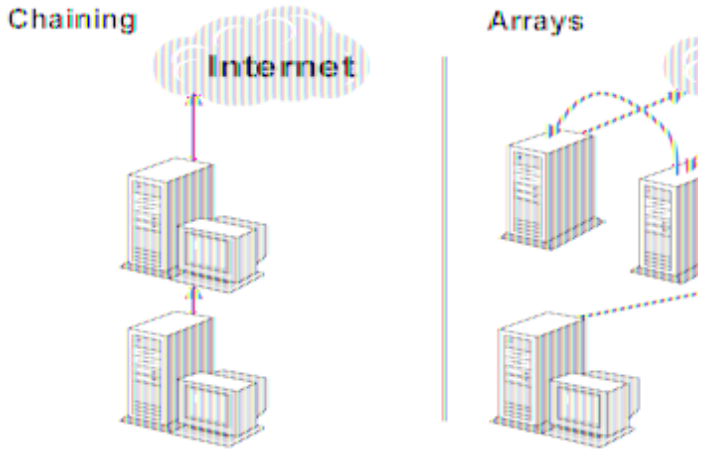
Configuración mediante un servidor WINS:

Windows Internet Name Service (WINS), es básicamente una base de datos en la cual se guardan todos los nombres Netbios de las máquinas, usuarios y, al fin y al cabo, objetos de una red.

Esa base de datos puede ser consultada por los servidores proxy para localizar clientes, gateways e incluso otros servidores proxy de la red.



Caché distribuida:



Microsoft Proxy Server 2.0 permite la distribución de la caché a lo largo de multiples servidores proxy.

Hay dos métodos para ello:

- **Chaining:** Conexión jerárquica de servidores proxy individuales. Las peticiones recorren toda la cadena hasta encontrar el objeto que desean obtener. Es un buen método de distribución de cargas y de tolerancia a fallos.
- **Arrays:** Permite a un grupo de servidores proxy ser tratados y administrados como si fueran una unidad lógica.

    - beneficios:

    - las paginas residen solo en un servidor proxy, anulando la duplicidad de objetos y optimizando el espacio en la caché.
    - aumento del rendimiento de los clientes
    - Aumento del tamaño de la caché, lo que agiliza las búsquedas.

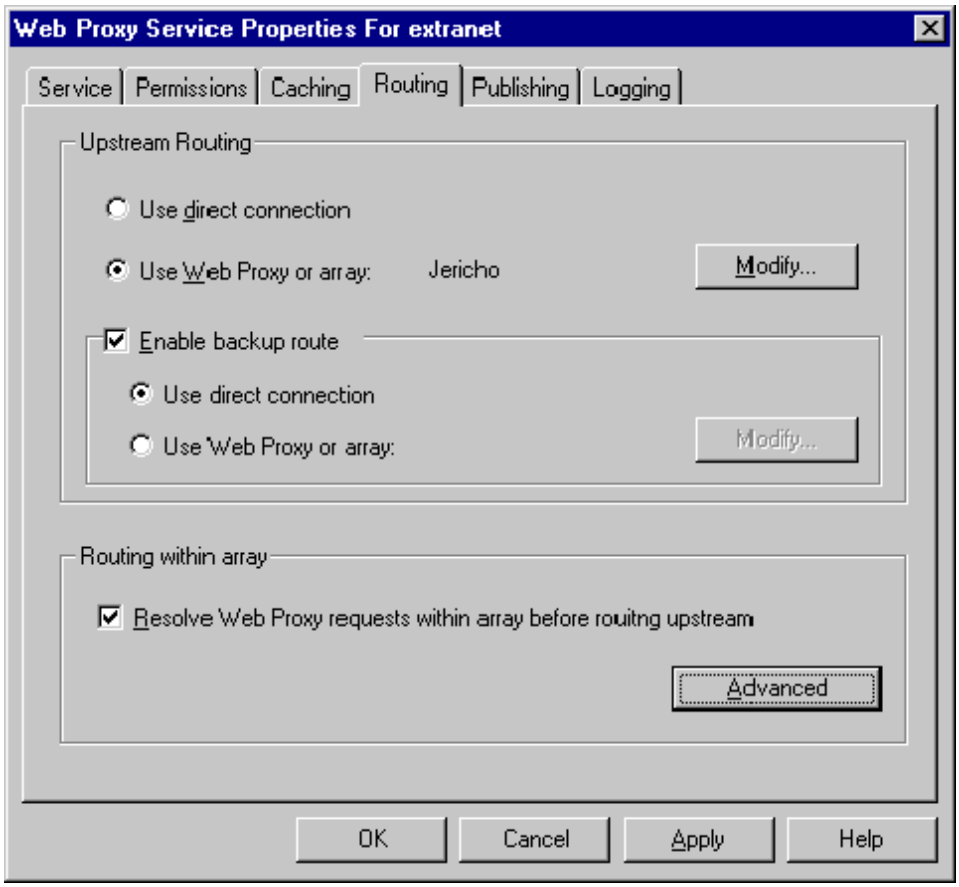
    - Donde se recomienda su uso

    - empresas con una central de proceso conectada a Internet
    - conexiones ISP consolidadas
    - proxies corporativos trabajando detrás de firewalls de hardware
    - Empresas con un volumen tan grande que necesiten mas de un servidor proxy para el correcto funcionamiento de la conexión a Internet

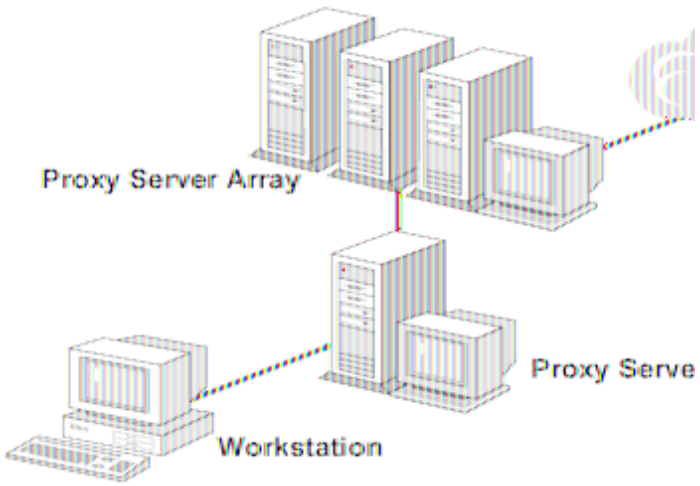
Configuración de rutas de servidores proxy:

Una petición de un cliente puede ser resuelta dentro de la misma matriz o array antes de que salga al exterior, detectando el algoritmo de enrutamiento el estado del servidor proxy antes de redirigir a él los paquetes. Esto solo es posible con clientes Web Proxy.

En la pantalla enrutamiento del servicio Web Proxy encontramos la manera de configurar esta función



Configuración de matrices (o arrays) de proxies:

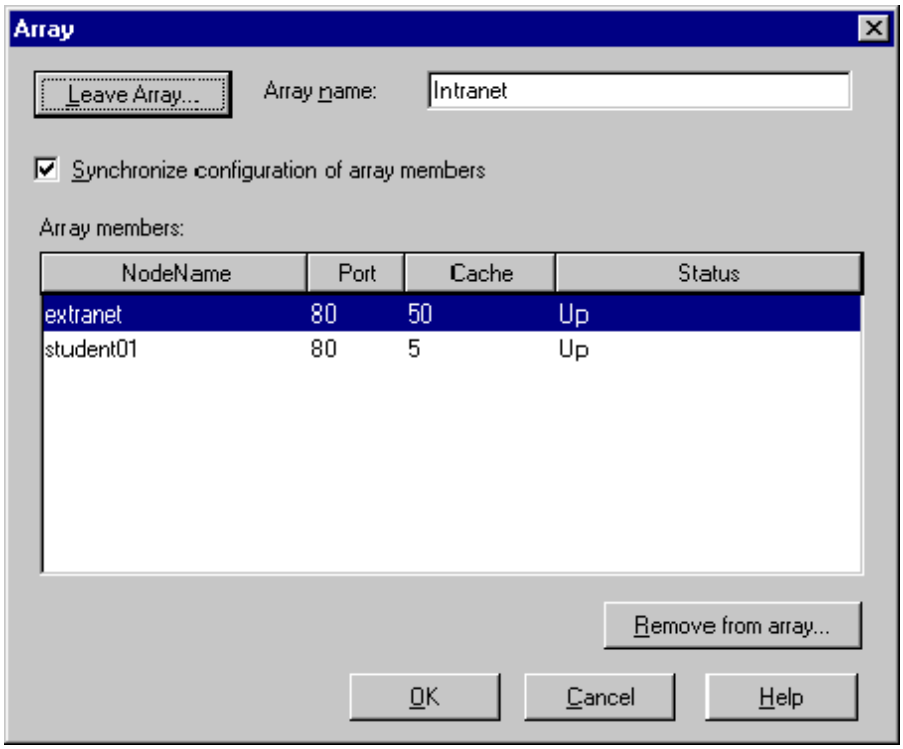


Podemos crear y configurar matrices o arrays desde la pestaña de servicios de cualquiera de los tres servicios, pero solo deberíamos administrar uno cada vez para evitar conflictos entre los distintos servidores. Cada uno de los servidores proxy mantiene una lista de los miembros de la matriz que están disponibles y cuales no.

Cada miembro individual usa el hash para tomar decisiones de enrutamiento. El **HASH** es una función matemática que asume tres funciones: la lista de servidores disponibles, la URL de la petición cliente y un factor de carga.

Solo los administradores del sistema son capaces de cambiar la pertenencia a una matriz.

En la pantalla de servicios nos encontramos con el botón de array o matriz que nos lleva a la siguiente pantalla de configuración, donde podremos crear o unirnos a matrices.



Caché Array Routing Protocol (CARP)

Microsoft Proxy Server 2.0 incluye Carp para expandir la escalabilidad y eficiencia de los servidores proxy que pertenecen a una matriz o array.

Características de Carp:

- Carp usa una serie de algoritmos que son aplicados arriba del todo del código HTTP. El explorador Web sabe exactamente en cual de los miembros de una matriz está guardado exactamente un objeto.
- Carp tiene escalabilidad positiva, siendo más eficiente cuantos más servidores proxy se agreguen a una matriz.
- Carp protege las matrices proxy de la duplicación de contenidos
- Carp ajusta automáticamente la pertenencia de servidores a la matriz
- Carp no requiere protocolos complicados, basándose en HTTP
- Carp es compatible con todos los estándard actualmente en el mercado

Mecanismo básico de Carp:

- Todos los servidores proxy trabajan con una lista de pertenencia que se renueva automáticamente según un TTL que chequea regularmente para encontrar servidores proxy activos.
- Una función HASH se computa para el nombre de cada uno de los servidores proxy y para cada una de las peticiones URL.
- El valor HASH del servidor proxy se combina con el de la URL, resultando su suma la pertenencia a uno u otro servidor proxy, manteniéndose ahí, a partir de ahora, eliminando la necesidad de mantener

tablas de cacheado para todos los objetos que se almacenan en dichas cachés.

Tema 10.− Planificación de un servidor Proxy

Determinación de objetivos:

- Aplicaciones: determinar el tipo de aplicaciones que serán usadas en cada una de las redes y la cantidad de datos o paquetes que serán transferidos a través del servidor proxy.
- Tipos de servicios: dependiendo del tipo de servicio determinaremos la configuración hardware del servidor proxy para soportar HTTP, FTP, Gopher, PPTP, encapsulado de audio y video, POP3, IRC y otros.

Anticipación de volumen:

- Anticipación de volumen ante la escasez de espacio en el disco duro y mal funcionamiento de la caché.
- Estructura física de los servidores, en solitario o en matriz, conectados o no directamente a Internet y el ancho de banda entre matrices.
- Limitar el acceso dependiendo de su tipo, localización, tipo de usuario y ancho de banda.
- Estimar al alza las capacidades de hardware de las máquinas en las cuales vamos a implementar el servidor proxy.

Determinar requerimientos de hardware y software:

- Analizar la organización de la que disponemos a la hora de estimar las capacidades en nuestra red, analizando lo que tenemos, lo que nos hace falta y lo que nos haría falta en caso de expansión.
- Analizar la estructura de dominios, el tipo de clientes y de usuarios y la capacidad de ancho de banda de nuestra empresa.

Línea base de Hardware:

Entorno	**Procesador**	**Espacio en disco**	**RAM**
Instalación	Intel 486	125 Mb	Por lo menos 24 Mb
De 1 a 300 máquinas	Intel Pentium 133	Hasta 2 Gb	Por los menos 32 Mb
De 300 a 2.000 máquinas	Intel Pentium 166	De 2 a 4 Gb	Por los menos 64 Mb
De 2.000 a 3.500 máquinas	Intel Pentium 200	De 8 a 16 Gb	Entre 128 y 256 Mb
ISP's con mas de 1.000 conexiones redundantes diarias	Alpha AXP 300	16 Gb	De 128 a 512 Mb

Conexiones a red:

- *Conexión analógica mediante módem*: Microsoft Proxy Server 2.0 puede operar con líneas analógicas mediante teléfono desde 28.8 Kbps. Este tipo de módem esta generalmente conectado a un puerto serie. En Microsoft Windows NT Server 4.0 es además necesaria la instalación de un servidor de acceso remoto (Ras para poder hacer uso de los protocolos SLIP y PPP)
- *Líneas RDSI*: propuestas como estándar de PYMES, RDSI es para ellos el transporte más económico y fácilmente administrable del mercado, brindando velocidades desde 64 Kbps a 128 Kbps en modo digital. En contraste con las líneas analógicas, con una RDSI podemos tener más de un canal de datos simultáneamente.
- *Líneas T−1:* Una línea T−1 es el estándar americano de comunicaciones, proporcionando velocidades de hasta 1.5 Gbps siendo, por tanto, la recomendación para empresas de más de 1.500 usuarios. La única

desventaja es el coste de este tipo de líneas, tanto de la línea en sí como de su implantación.

Conexiones de Hardware:

- Módem analógico, desde 14,4 hasta 56 K de velocidad es adecuado para una conexión de un solo usuario, sirviendo también de Gateway hacia Internet.
- Linea RDSI, desde 64 a 128 K de velocidad es adecuado para empresas pequeñas de no más de 25 puestos, siendo compatible con la mayoría de los sistemas operativos del mercado.
- Router: Un router es un dispositivo que conecta dos redes y encamina tráfico de una a otra, siendo el ideal para crear Virtual Private Networks (VPN) o Redes Privadas Virtuales que encaminen tráfico entre nuestras sedes utilizando el canal de Internet de una manera segura.
- Conexiones de Software: una máquina cliente con cualquier sistema operativo Windows necesita software de conexión para poder comunicarse con Internet, siendo los más usuales Serial Line Interface Protocol (SLIP) y Point−to−Point Protocol (PPP), por lo que es aconsejable la documentación y experimentación sobre ellos.

Análisis de costes:

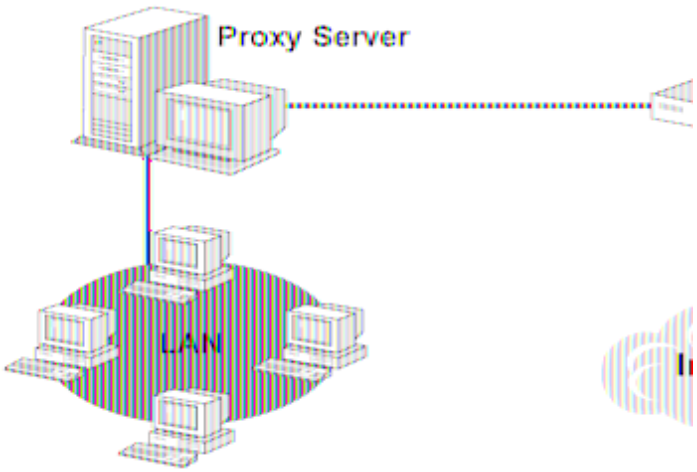
- Ancho de banda: este elemento es el más importante dentro de nuestra conexión a Internet por determinar la velocidad de transferencia de datos o paquetes entre las distintas sedes. Este elemento debería depender de los picos de utilización de nuestra red, fácilmente monitorizables desde el monitor de sistema.
- La elección entre una conexión bajo demanda y una conexión permanente dependerá de las necesidades de nuestra empresa y los requerimientos de nuestros clientes, siempre teniendo en cuenta el riesgo que supone una conexión 24 horas al día a Internet frente a ataques no deseados desde fuera de nuestra LAN.

Preparación de la organización:

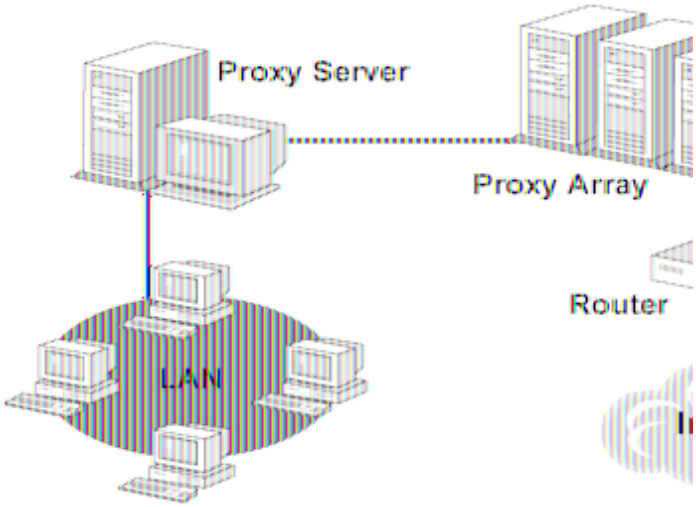
Antes de la implementación del servidor proxy necesitamos preparar nuestra organización determinando que tipo de clientes vamos a usar, configurándolo adecuadamente y formando a los usuarios y administradores de nuestra empresa sobre las nuevas tecnologías que vamos a implantar.

Situaciones empresariales:

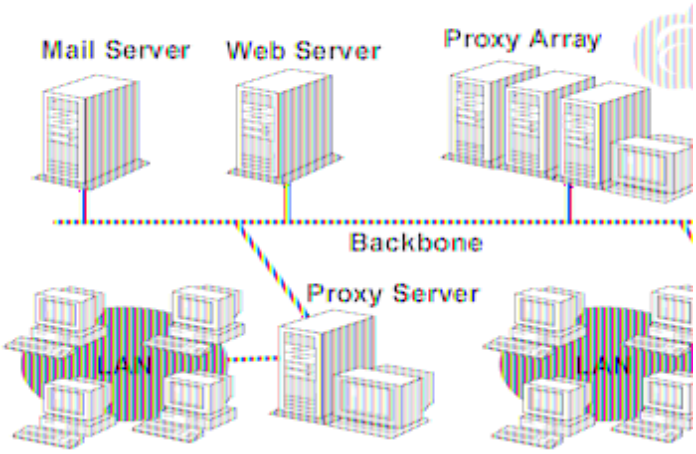
- Red de pequeña empresa, configurada normalmente con un solo segmento LAN, TCP/IP, menos de 200 clientes, servicios básicos Web (FTP, HTTP y Mail), con una línea RDSI como base. En este escenario es necesaria sólo una máquina con Microsoft Proxy Server 2.0 con una tarjeta de red (preferiblemente a 100 Mbps) y una tarjeta adaptadora RDSI. La LAT sólo contiene direcciones del espacio IP interno, con la caché minimizada y optimizada hacia las sesiones de usuario.



- Red de mediana empresa, configurada normalmente por una oficina central y varias sucursales con varios segmentos LAN, TCP/IP, conexión bajo demanda a Internet mediante un ISP, con una media de entre 200 y 2.000 clientes, en la cual se recomienda una matriz de hasta 3 proxys instalado el principal en una máquina con Microsoft Windows NT Server 4.0 con el servicio RAS instalado en ella. La resolución de nombres se hará normalmente por DNS.



- Red de gran empresa, configurada normalmente con varios segmentos LAN, más de un protocolo, conexión dedicada, hasta 10.000 clientes y normalmente con Extranet corporativa donde se instala la página web de la empresa. La resolución de nombres puede hacerse por DNS, WINS o por cualquier otro tipo de resolución de nombres. Las extranet deben constar de dominios aparte con máquinas dedicadas exclusivas a IIS y Microsoft Proxy Server 2.0.



Tema 11.− Monitorización y optimización de

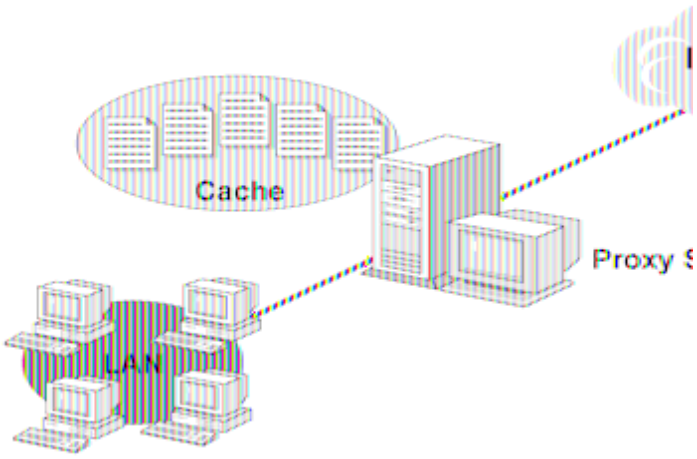
Microsoft Proxy Server 2.0

Determinación de factores:

	La CPU no es uno de los factores determinantes en el desarrollo del servidor proxy, pero si el numero de clientes pasa de unos 500, podemos considerar la posibilidad de implementar placas duales con dos

	CPU
	La memoria RAM es quizá el factor más importante en el desarrollo del servidor proxy, en especial la paginación, la cual, si se convierte en excesiva, ralentiza de una manera espectacular el rendimiento del servidor proxy
	El disco duro, y su velocidad de transmisión, son factores importantes también a la hora de implementar la caché, pudiéndose incluso plantear la posibilidad de usar discos duros separados del sistema en si y específicos para la caché
	La red no es un factor tan importante como pueda parecer, ya que todas las transacciones de páginas se realizan por ella, pero si es aconsejable su monitorización para su correcto uso

Determinación de la caché:



La caché debe ser optimizada basándose en el uso del servidor proxy, determinando claramente el ancho de banda y el uso esperado por los clientes de nuestra red.

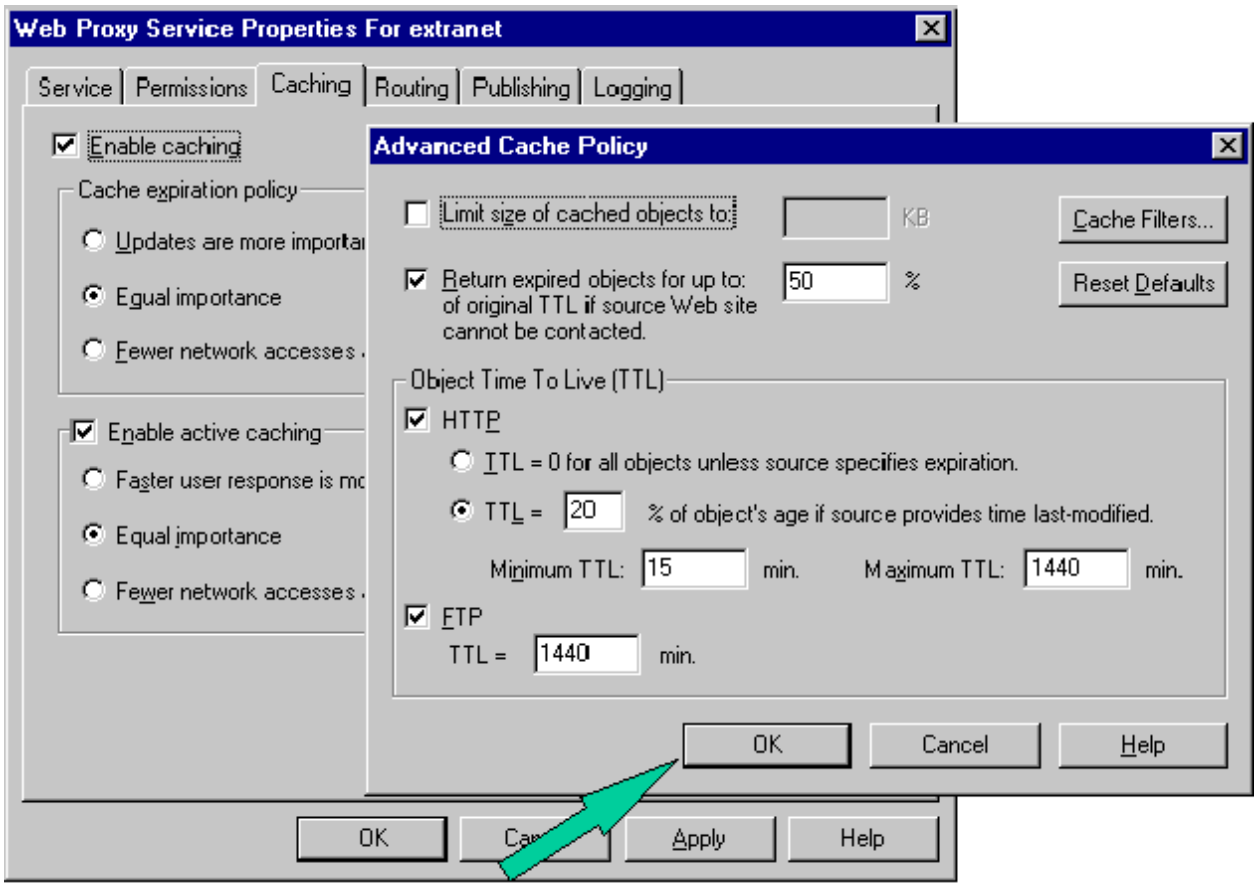
Debemos chequear habitualmente el espacio en disco duro para asegurar el optimo crecimiento de la caché en nuestro servidor proxy.

Chequear especialmente el TTL de los objetos de HTTP y FTP, por ser los más peligrosos de ocupar sitio de una manera enorme.

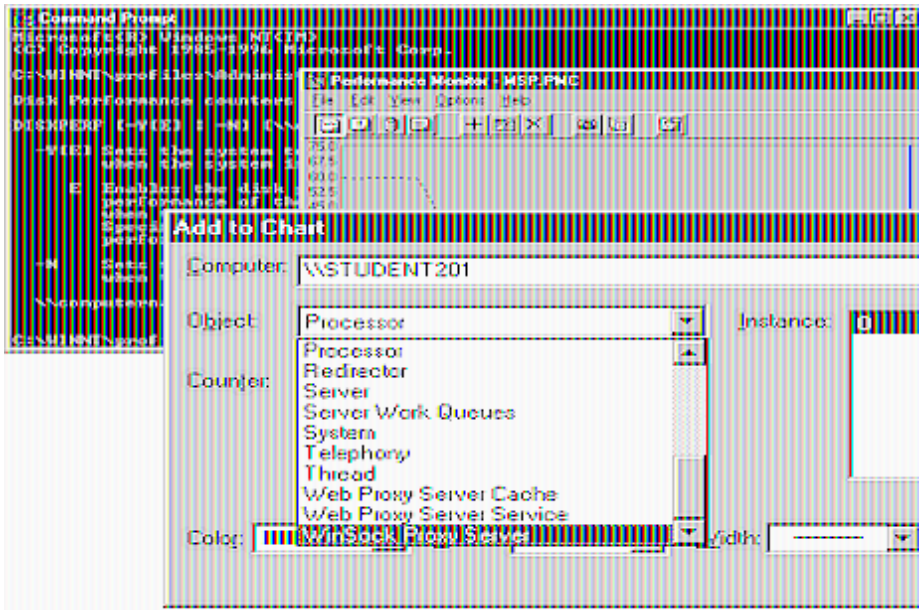
Limitar el tamaño de los objetos en la caché para maximizar el numero de objetos en la misma.

Distribuir, siempre que sea posible, la caché en diferentes discos duros para optimizar el rendimiento de la misma.

Cada vez que el servidor proxy inicia, los objetos en la caché son objeto de diferentes tests para determinar su estado y arreglar determinados errores que puedan ralentizar el rendimiento de la misma.



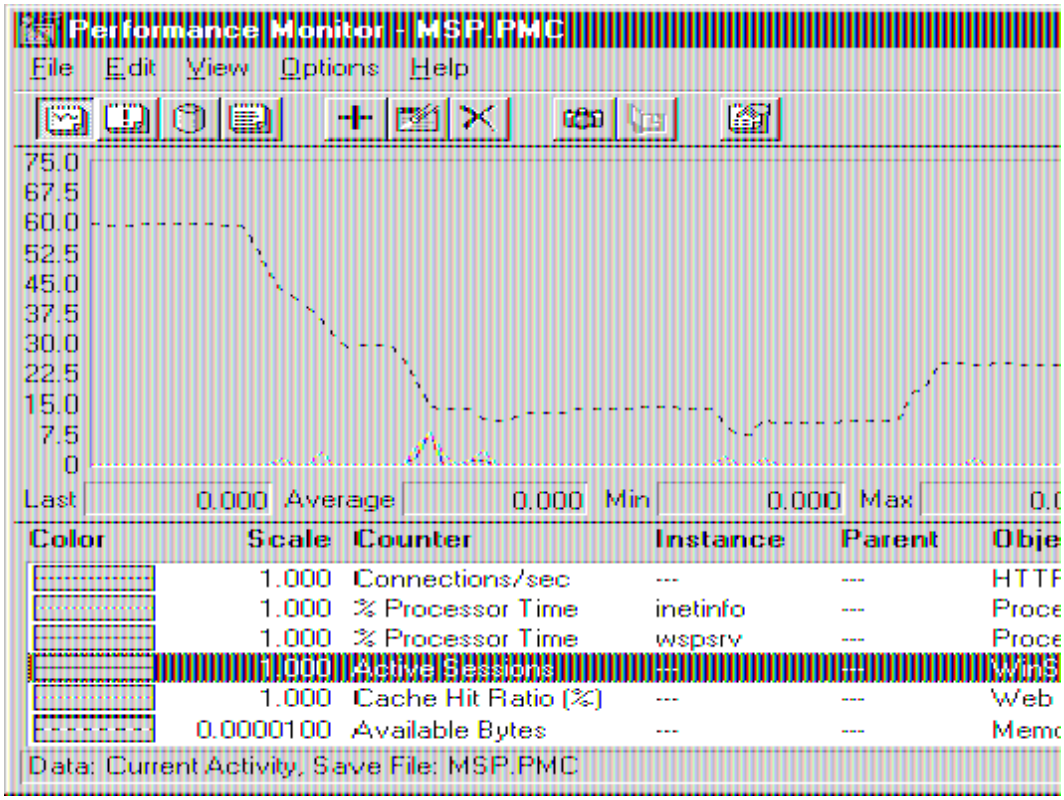
Los contadores del monitor de desarrollo nos servirán para desarrollar una línea de base que nos permita monitorizar correctamente los estados de nuestro servidor proxy



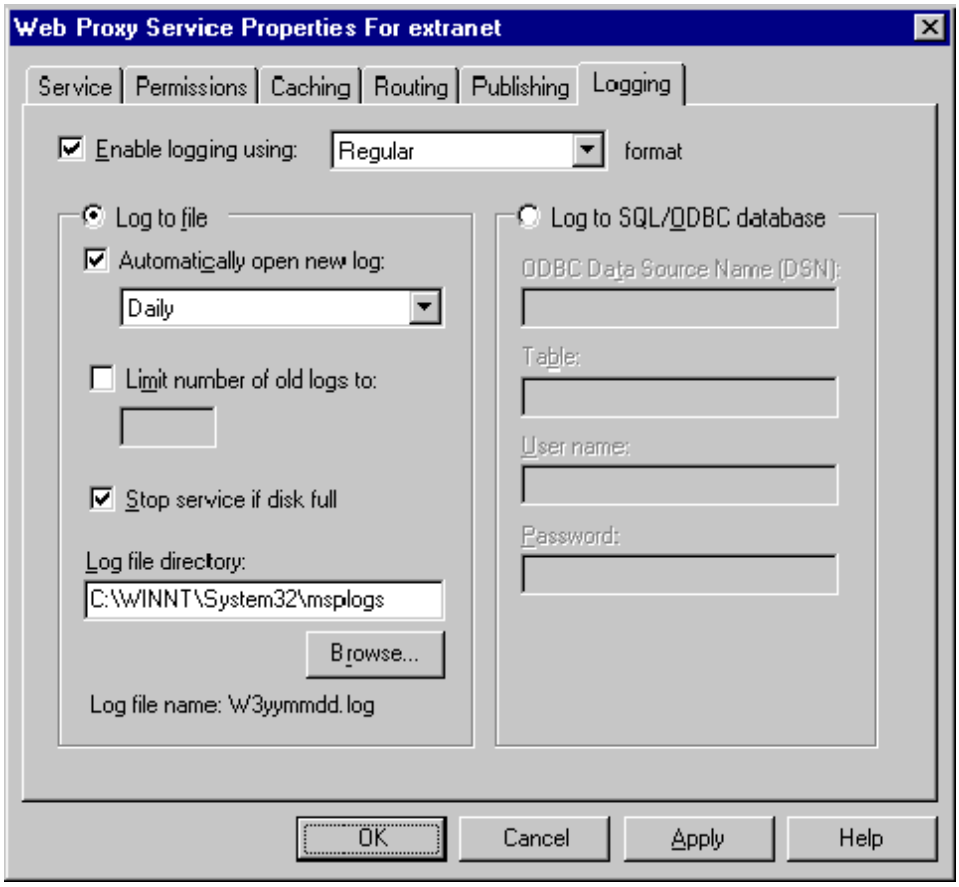
Contadores por defecto que instala Microsoft Proxy Server 2.0:

- Tiempo de procesador *(%ProcessorTime*), que revela el tiempo de CPU usado por un determinado servicio
- Sesiones activas (*Active Sessions*), o cuanta gente esta usando el servidor al mismo tiempo
- *Caché Hit ratio (%)*, que indica el porcentaje de peticiones que está sirviendo el servidor proxy

- Peticiones por segundo (*Requests/sec.*), que da información de las peticiones que han sido hechas alguna vez al servidor proxy
- *Current Average Miliseconds/request*, o tiempo en milisegundos que tarda el servidor proxy en atender una petición
- *Sites denied*, que ofrece información de los sitios de los sitios visitados en que nuestros clientes han sido rechazados
- *Sites granted*, que ofrece información de los sitios de los sitios visitados en que nuestros clientes han sido aceptados
- *Total users*, o contador acumulativo que expone datos sobre el total del numero de usuarios que alguna vez han hecho uso de Microsoft Proxy Server 2.0 para acceder a la red
- *Current users*, o usuarios soportados actualmente por el servidor proxy
- *Máximum users*, o número de usuarios máximo conectados simultáneamente al servidor proxy
- *Inet bytes total/sec.*, o cantidad de datos procesados entre el servidor proxy e Internet
- *Bytes in caché*, o cantidad de datos almacenados actualmente en la caché
- *Max bytes caché*, o numero máximo de datos que alguna vez han sido guardados en la caché
- *Active refresh bytes rate*, que determina la necesidad o no de ampliar la caché activa.



Uso y configuración de los archivos *.log



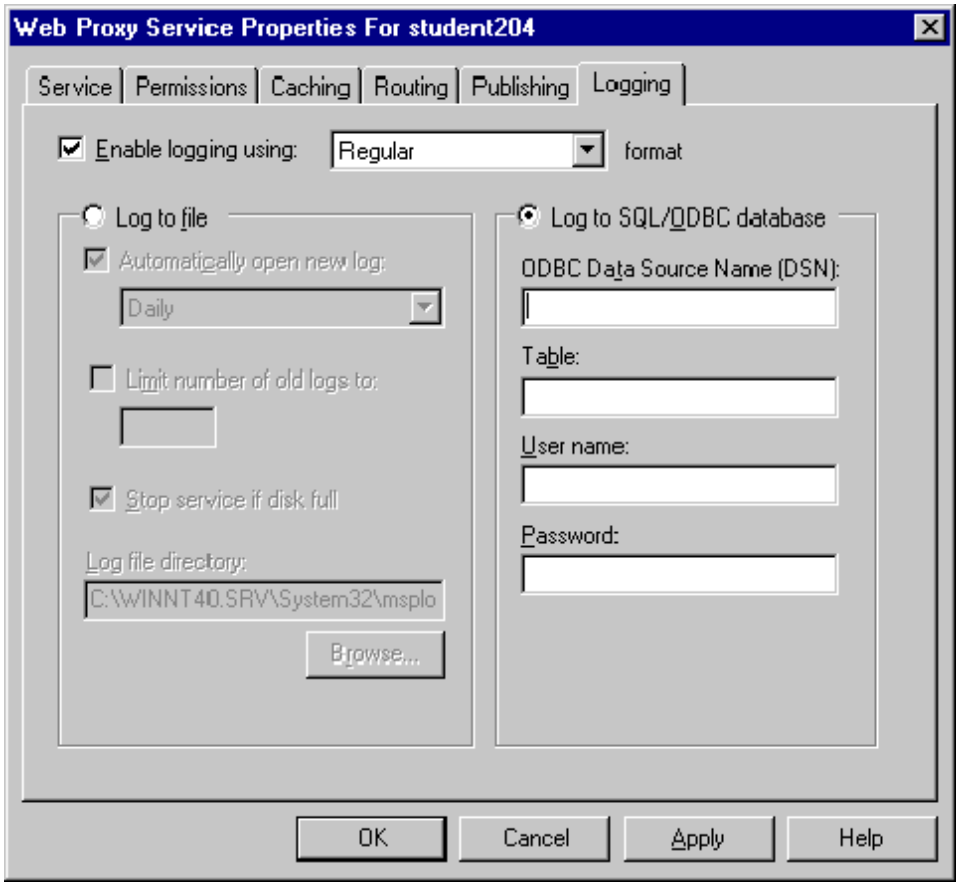
Los archivos log pueden ser almacenados en archivos de texto con las siguientes opciones de configuración:

- Abrir periódicamente un archivo *.log nuevo, pudiendo especificar si lo queremos diario, semanal o mensual
- Limita el numero de archivos *.log en nuestro sistema
- Para los servicios si el disco duro está lleno, debiéndose liberar espacio en él para poder reiniciar los servicios
- Permite especificar el directorio y el nombre de los archivos *.log de nuestro sistema, siendo el formato predeterminado WSWyymmw.log
- Hay dos modos de crear un archivo *.log: *regular*, o modo de ahorro de espacio en disco duro, y *verbose*, o modo de detalle completo

Modos de configuración de los archivos *.log:

Campos del archivo *.log	**Regular**	**Verbose**
Authentication status		X
Bytes received		X
Bytes sent		X
Client agent		X
Client machine name	X	X
Client platform		X
Client user name	X	X
Destination address		X
Destination name	X	X

Destination port	X	X
Log date	X	X
Log time	X	X
Object MIME		X
Object name	X	X
Objetc source	X	X
Operation		X
Processing time		X
Protocol name		X
Proxy name	X	X
Referring server name		X
Result code	X	X
Service name	X	X
Transport		X



Los archivos log pueden ser también almacenados en una base de datos, tanto por el canal ODBC como en una base nativa como Microsoft SQL 7.0 u Oracle.

Este modo incrementa los recursos que Microsoft Proxy Server 2.0 tiene que dedicar a la tarea, restándoselos al propio sistema o al rendimiento del propio proxy.

Los datos a aportar para su configuración son escasos: canal ODBC, nombre de la tabla donde se van a almacenar los datos, y el nombre de usuario y so contraseña para las posteriores modificaciones de la propia

tabla.

Estrategias para reducir conexiones a Internet:

- Incrementar el tamaño de la caché para incrementar la posibilidad de que la página pedida por el usuario se encuentre en la misma.
- Habilitar la caché activa
- Incrementar los TTL para permitir que los objetos estén más tiempo en la caché
- Minimizar el uso de aplicaciones WinSock y Socks

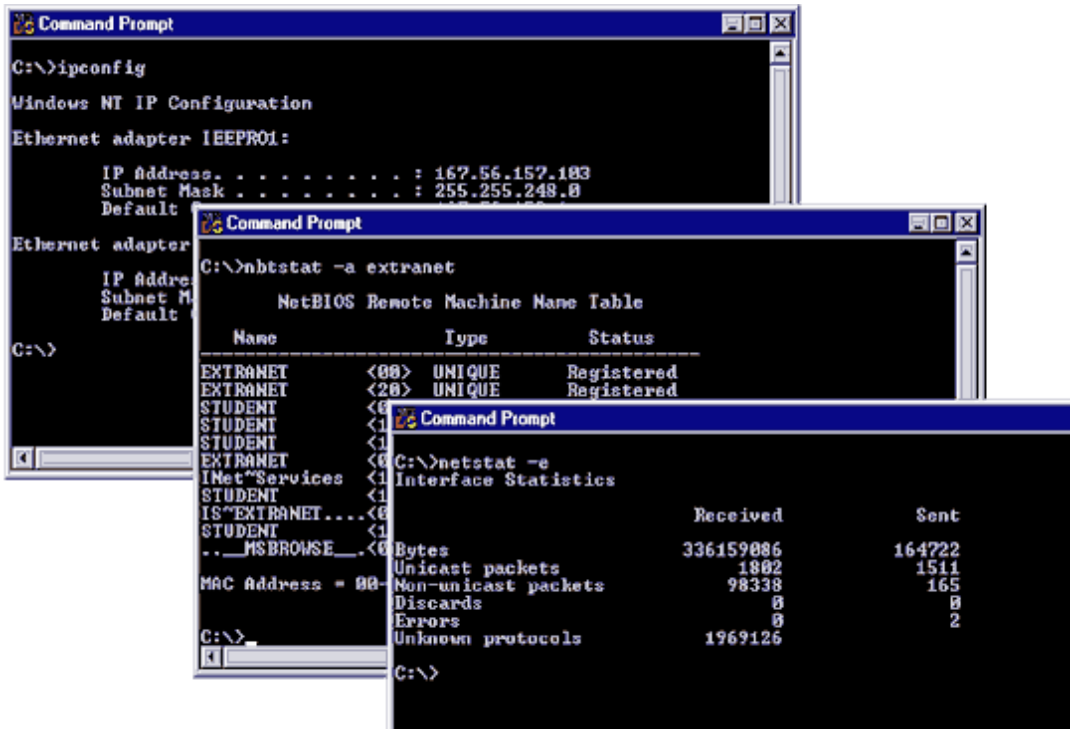
Tema 12.− Resolución de Problemas

Recursos para la resolución de problemas:

- Microsoft TechNet
- Internet (www.microsoft.com)
- Servicios On−Line (MSN, The Microsoft Network)
- Librerías descargables de Microsoft (MSDL)

Herramientas de resolución de problemas:

- Editor del registro
- Monitor de sistema (tanto en NT Server 4.0 como en Windows 2000)
- Visor de sucesos (con visor dedicado en Windows 2000)
- Archivos *.log, tanto de texto como en bases de datos
- Herramientas de análisis de red



Comandos de configuración y resolución de problemas:

- TCP/IP

- Arp (Address Resolution Protocol)
- Hostname (nombre del host o maquina cliente)
- Ipconfig (configuración de entorno de TCP/IP)
- Nbtstat (conexiones NetBios sobre TCP/IP)
- Ping (comando espejo de comprobación de conexión con hosts)
- Route (tabla de enrutamiento de TCP/IP)
- Tracert (ruta a sistemas remotos)

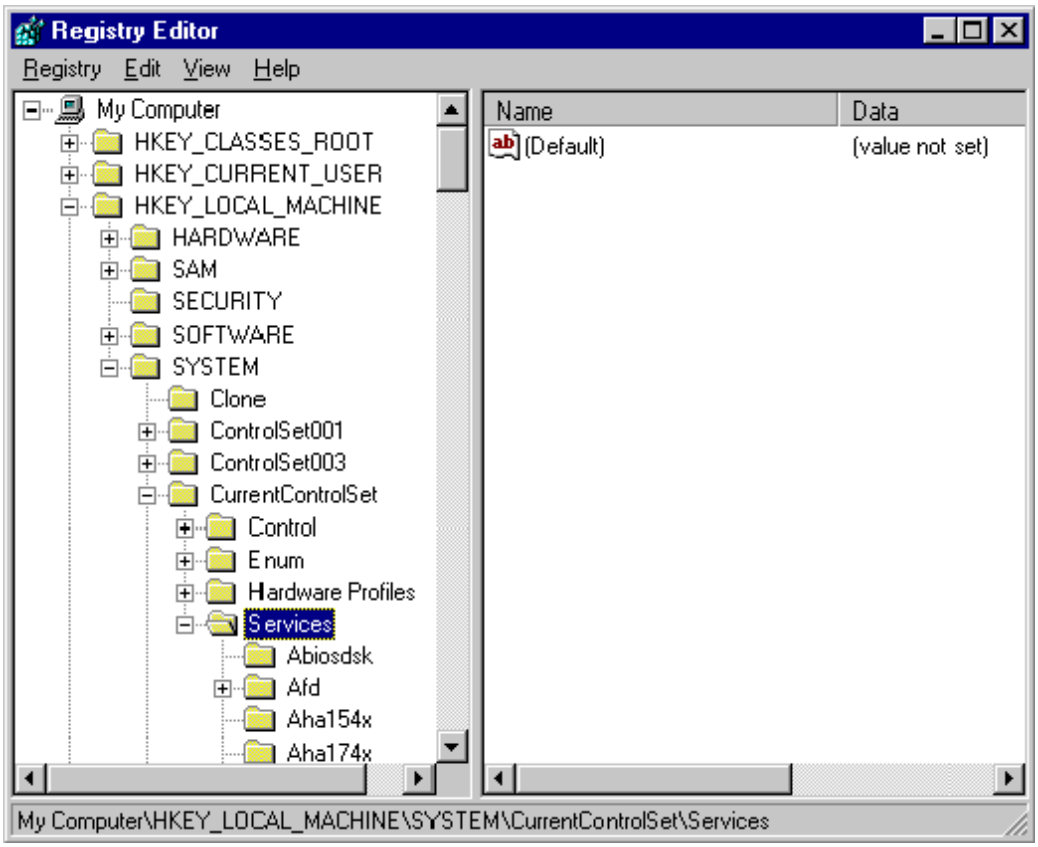
- IPX/SPX

  - Ipxroute config (configuración de enlaces IPX)
  - Ipxroute servers (tabla SAP de servidores)

- Comandos de Microsoft Proxy Server 2.0

  - CHKWS16, que identifica la configuración del cliente proxy, solo para clientes Windows 3.11
  - CHKWS32, que identifica la configuración del cliente proxy, para clientes 95, 98 NT y 2000.

Entradas del registro:



Las entradas del registro que queramos buscar y que se refieran al servidor proxy se encuentran en **HKEY_LOCAL_MACHINE/System/CurrentControlSet/Services**

Errores más comunes de un servidor proxy:

- Errores del servidor, localizados en un archivo de texto en C:\MPSSETUP.LOG
- Errores de tarjeta de red, localizados en el mismo archivo
- Instalación de la caché en FAT (donde no es posible)

- Errores Web Proxy,o errores del propio servicio tipificados en pantallas HTTP en el explorador, con errores como:

HTTP/1.0 500 Server Error (−number)

- Errores de la caché Web Proxy, o errores normalmente de configuración de la caché o de disco duro (fragmentación, sistema de archivos)
- Errores WinSock Proxy, o errores de protocolos, conectividad, nombres de servidores o de resolución de nombres y de aplicaciones TCP/IP de otros fabricantes
- Errores Socks, o errores del canal de configuración y manejo de datos del servidor proxy
- Errores de identificación y enrutado de paquetes
- Errores de las matrices de proxies, por intentos de administración de mas de un servidor simultáneamente o rendimiento muy pobre de la matriz
- Errores de clientes (ya sabeis, esos que dicen que trabajan), por defectos de instalación, protocolos o mala configuración de los clientes de correo o los exploradores

Qué hacer ante un error de los clientes:

- Chequear que el servidor proxy y la conexión con el ISP están configurados correctamente y que funcionen bien
- Determinar si otro administrador no ha parado o pausado algún servicio del proxy
- Revisar la LAT, asegurándonos de que contiene la máquina que da problemas
- Entrar como Administradores en el servidor proxy e intentar la conexión a Internet
- Revisar los registros de los archivos *.log y del visor de sucesos por si alli hubiera algún rastro de problemas
- Entrar como el cliente desde su estación de trabajo o desde el servidor para intentar desde allí acceder a Internet o delimitar la causa del problema
- Verificar la configuración de red del cliente
- Chequear el cliente proxy en la máquina cliente
- Hacer Ping desde el cliente hacia el servidor
- Usar comandos de configuración para intentar dar con el problema
- Reinstalar el cliente proxy en la máquina cliente

3

Las pantallas que aparecen en esta sección corresponden a IIS 2.0, pudiendo cambiar de apariencia dependiendo de la versión de IIS que estemos utilizando

Las pantallas que aparecen en esta sección corresponden a IIS 2.0, pudiendo cambiar de apariencia dependiendo de la versión de IIS que estemos utilizando

Las pantallas que aparecen en esta sección corresponden a IIS 2.0, pudiendo cambiar de apariencia dependiendo de la versión de IIS que estemos utilizando

Para mas información sobre los socks acceder a:

www.socks.nec.com/index.htm

www.socks.nec.com/socks4.protocol

Las pantallas que aparecen en esta sección corresponden a IIS 2.0, pudiendo cambiar de apariencia dependiendo de la versión de IIS que estemos utilizando

1

2

4

3

5

6

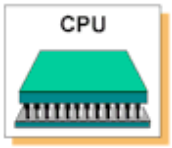
7

8

9

10

11



1

2

3

4

5