

TerminET

Cortafuegos personal

Guía del usuario

Contenido

1	INTRODUCCIÓN	3
1.1	ACERCA DE TERMI NET	3
1.2	CARACTERÍSTICAS MÁS IMPORTANTES	3
2	PRIMEROS PASOS	4
2.1	INSTALACIÓN DE TERMI NET	4
2.2	INICIO DE SESIÓN EN TERMI NET	4
2.2.1	<i>Windows 95/98</i>	4
2.2.2	<i>Windows NT/2000</i>	4
2.3	MODO ADMINISTRADOR	4
2.4	LA INTERFAZ DE TERMI NET	4
3	USUARIOS Y GRUPOS	8
3.1	ADMINISTRACIÓN DE USUARIOS Y GRUPOS	8
3.1.1	<i>Adición de usuarios</i>	8
3.1.2	<i>Creación de grupos</i>	8
4	REGLAS DE TRÁFICO	8
4.1	REGLAS ESTÁNDAR	8
4.2	REGLAS AVANZADAS	9
4.3	CREACIÓN DE REGLAS	9
5	LISTAS WEB	11
5.1	<i>LISTAS NEGRAS</i>	11
5.2	<i>LISTAS BLANCAS</i>	11
5.3	<i>LISTAS GLOBALES Y LOCALES</i>	11
6	PROBLEMAS CON NETBIOS	12

1 Introducción

1.1 Acerca de TermiNET

TermiNET es un cortafuegos personal diseñado para proteger los PC de ataques externos mientras están conectados a Internet, explorando el Web o accediendo a otros servicios de Internet. TermiNET se puede instalar inicialmente en cualquiera de los siguientes modos:

1. El "**Modo cerrado**" bloquea de forma predeterminada todo el tráfico hacia y desde el equipo local. El administrador puede, de forma selectiva, abrir el acceso; por ejemplo, puede permitir sólo FTP o FTP, Telnet y acceso al Web. Para el control de los padres, el acceso se puede limitar a un conjunto de páginas especificado. Se pueden introducir estas páginas directamente como reglas específicas o leerlas de una "Lista blanca".
2. El "**Modo abierto**" no impone condiciones de bloqueo iniciales. El administrador puede cerrar de forma selectiva el acceso específico por aplicación, puerto y protocolo, por ejemplo: bloquear todo el Telnet y FTP, bloquear toda la comunicación entrante en el puerto 25, bloquear el acceso a un conjunto específico de páginas Web. De nuevo, éstas se pueden introducir como reglas específicas o leerse de una "Lista negra" o sitios aceptables.
3. El "**Modo invisible**" permite todo el tráfico saliente, pero bloquea todas las conexiones entrantes salvo las iniciadas localmente. En este modo se puede utilizar el equipo para explorar el Web, FTP, etc., de la forma habitual, pero está protegido de ataques mientras está conectado a Internet.

TermiNET es la solución de seguridad ideal para usuarios de PYMES y de equipos domésticos que desean conectarse a Internet de forma segura pero que no poseen recursos para soportar una gran infraestructura de seguridad.

1.2 Características más importantes

Las características más importantes de TermiNET son:

- Reglas estándar y avanzadas: Función sencilla de casilla de activación para **activar** o **desactivar**.
- La función Lista negra/Lista blanca proporciona la posibilidad de no permitir el acceso a determinados sitios no deseados o de permitir el acceso solamente a sitios aceptables.
- El control de acceso flexible permite que se especifiquen reglas por Dirección IP, URL, Puerto o Protocolo.
- Se pueden configurar reglas basadas en tiempos para que estén activas solamente en días especificados.
- Una interfaz fácil de usar y de estilo semejante al "Explorador de Windows" hace que la configuración de TermiNET sea sencilla e intuitiva, incluso para usuarios no técnicos.

2 Primeros pasos

2.1 Instalación de TermiNet

Introduzca el CD de TermiNET en la unidad de CD del PC. La instalación se debe ejecutar automáticamente. Si se ha desactivado la función de ejecución automática, haga clic en "Inicio"

"Ejecutar" y escriba "D:\setup" siendo D: la letra de la unidad de CD. Siga las instrucciones que aparecen en pantalla para instalar el producto.

Una vez finalizada la rutina de la instalación, el PC se **debe** reiniciar para finalizar la instalación.

2.2 Inicio de sesión en TermiNet

2.2.1 Windows 95/98

Al arrancar el sistema TermiNET se inicia con un conjunto de reglas predeterminadas, según las defina el Administrador. Si se han creado varios perfiles de usuario de TermiNET, hay dos formas de iniciar la sesión como uno de los usuarios definidos: hacer doble clic en el icono de TermiNET en la bandeja del sistema o bien hacer clic derecho en el icono de TermiNET y seleccionar "Inicio de sesión". En cualquier caso, el usuario verá una pantalla de inicio de sesión solicitándole un Id de usuario y una contraseña. La introducción del Id de usuario y de la contraseña activará el perfil de seguridad para el usuario especificado.

2.2.2 Windows NT/2000

Los usuarios inician automáticamente la sesión de TermiNET basándose en el perfil de inicio de sesión de NT.

2.3 Modo Administrador

El modo Administrador permite la especificación del perfil de seguridad predeterminado del usuario, la creación de nuevos perfiles de usuario y la configuración de reglas avanzadas para usuarios específicos. Se accede al modo Administrador haciendo clic derecho en el icono de bandeja del sistema TermiNET y seleccionando "Modo Administrador". Se le pedirá la contraseña de Administrador. Después de introducir la contraseña, aparecerá la pantalla de configuración de TermiNET, que permite realizar funciones administrativas.

Para salir del modo Administrador, cierre la pantalla de configuración utilizando la opción de menú "Archivo -> Salir de Administrador".

2.4 La interfaz de TermiNET

La interfaz de TermiNET (Figure 1) solamente se encuentra accesible utilizando la contraseña del Administrador. Es una herramienta gráfica sencilla de utilizar para definir los perfiles de seguridad para una máquina.

Los menús Archivo, Edición y Ver permiten personalizar la interfaz de acuerdo con las preferencias de los administradores. El menú "Herramientas" -> "Opciones" permite establecer propiedades para todo el sistema.

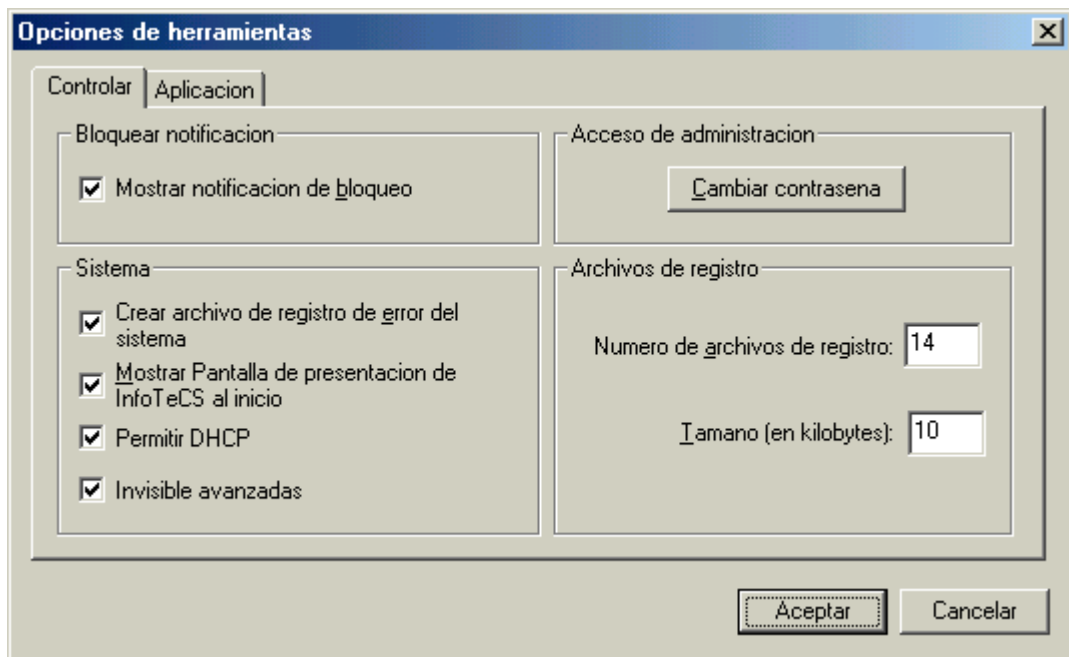


Figure 2

La ficha de control (Figure 2) proporciona acceso a las siguientes opciones:

Mostrar notificación de bloqueo	Quando está activado, el Registro de tráfico mostrará el tráfico bloqueado y el permitido. Cuando está desactivado, solamente se registrará el tráfico permitido.
Crear archivo de registro de error del sistema	Quando está activado, los errores del sistema se escribirán en el archivo \Archivos de programa\Infotecs\Terminet\Data\errorlog.txt
Mostrar Pantalla de presentación de INFOTECS al inicio	Desactívelo para evitar que la Pantalla de presentación de INFOTECS aparezca al iniciar TerminiNET.
Cambiar contraseña	Permite que se cambie la contraseña de administración.
Número de archivos de registro	Establece el número de archivos del registro de tráfico que se registran. Una vez que se alcanza el número especificado de archivos de registro y que el último archivo llega a su tamaño máximo, se sobrescribe el primer archivo.
Tamaño (en kilobytes)	Establece el tamaño en kilobytes hasta el que llegará un archivo del registro de tráfico. Una vez alcanzado este tamaño, el archivo se guarda y se registra otro archivo.

La ficha Aplicación (Figure 3) permite que se creen nuevas aplicaciones estándar.

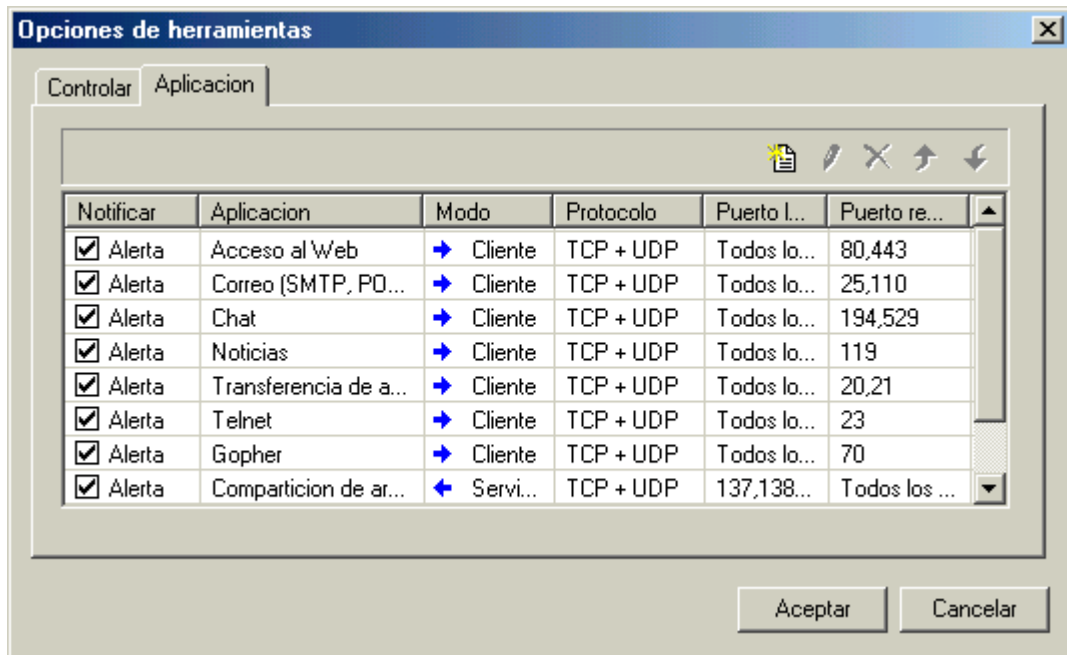



Figure 3

Haga clic en el botón Agregar aplicación  para mostrar el cuadro de diálogo Personalizar aplicación (Figure 4).

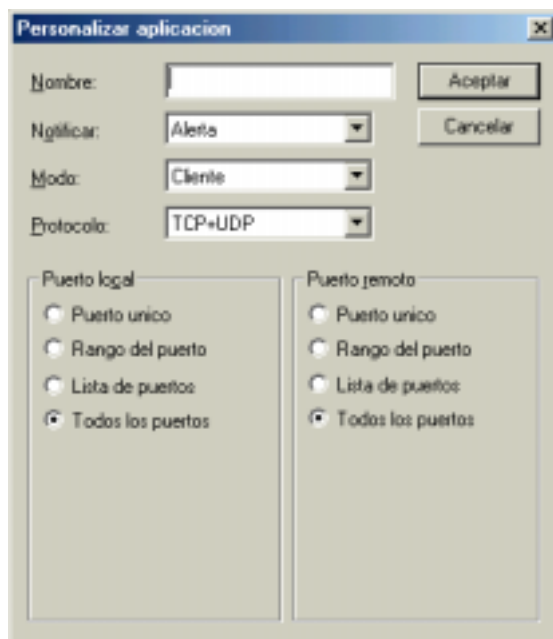


Figure 4

Esta ventana permite establecer las siguientes opciones:

- **Nombre:** Especifique el Nombre de la aplicación personalizada.
- **Protocolo:** Seleccione en la lista desplegable el protocolo que desee para la aplicación.
- **Notificar:** Seleccione Alerta o Ignorar en la lista desplegable. Si se selecciona Alerta, aparecerá una notificación cuando se bloquee el tráfico de este tipo.
- **Dirección:** Seleccione Entrante o Saliente en la lista desplegable.
- **Puerto remoto:** Especifique la configuración del puerto aplicable a la máquina remota para esta aplicación.
- **Puerto local:** Especifique la configuración del puerto aplicable a la máquina local para esta aplicación.

3 Usuarios y grupos

3.1 Administración de usuarios y grupos

3.1.1 Adición de usuarios

Para agregar un perfil de usuario, haga clic derecho en el máximo nivel de la vista en árbol de TermiNET y seleccione "Agregar usuario" en el menú contextual o bien haga clic en el botón Usuario de la barra de herramientas. Aparecerá el cuadro Propiedades del usuario (Figure 5).

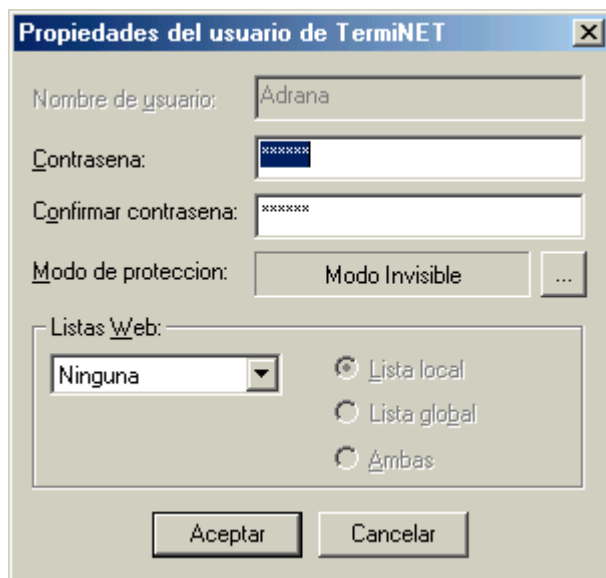


Figure 5

Están disponibles los siguientes campos:

- **Nombre de usuario:** Se utiliza para introducir el Nombre deseado para el usuario.
- **Contraseña:** Introduzca la contraseña precisa para el usuario.
- **Confirmar contraseña:** Introduzca la contraseña por segunda vez para su confirmación.
- **Modo de protección:** Seleccione el Modo de seguridad predeterminado para este usuario.
- **Listas URL:** Determina si este usuario utilizará las Listas blancas o negras de URL y si se utilizará la lista global, la local o ambas.

3.1.2 Creación de grupos

Se pueden utilizar grupos para organizar listas de usuarios dentro de la vista en árbol de TermiNET. Cree un nuevo grupo haciendo clic derecho en el nivel más alto del árbol y seleccionando "Agregar grupo" en el menú contextual y escribiendo el nombre que desea para el Grupo. Los usuarios se pueden agrupar en grupos haciendo clic en sus nombres de usuario y arrastrándolos al grupo deseado. Se puede crear un usuario en un grupo existente haciendo clic derecho en el grupo en la vista en árbol y seleccionando "Agregar usuario" en el menú contextual.

4 Reglas de tráfico

Hay dos tipos de reglas de tráfico que se pueden definir en TermiNet.

4.1 Reglas estándar

Se aplican a todas las direcciones IP y se pueden utilizar para permitir o no el acceso a servicios específicos de forma global. El sistema tiene predefinidas cuatro reglas estándar, Acceso a Web, Correo, FTP y Telnet. Se pueden crear más reglas seleccionando un usuario en la vista en árbol, haciendo clic derecho en el panel Reglas estándar y seleccionando "Agregar regla" en el menú contextual para abrir el cuadro de diálogo Agregar regla (Figure 6).

4.2 Reglas avanzadas

Se aplican a direcciones IP o URL específicos y se utilizan para permitir o no el acceso a sitios y servicios de forma selectiva. Las reglas se agregan seleccionando el usuario al que se aplicará la regla, haciendo clic derecho en la ventana Reglas avanzadas y seleccionando "Agregar regla" en el menú contextual para abrir el cuadro de diálogo Agregar regla (Figure 6).

Si TermiNET está instalado en modo Invisible, solamente se pueden configurar las reglas avanzadas.

4.3 Creación de reglas

El cuadro de diálogo Agregar regla (Figure 6) se utiliza para crear y definir nuevas reglas.

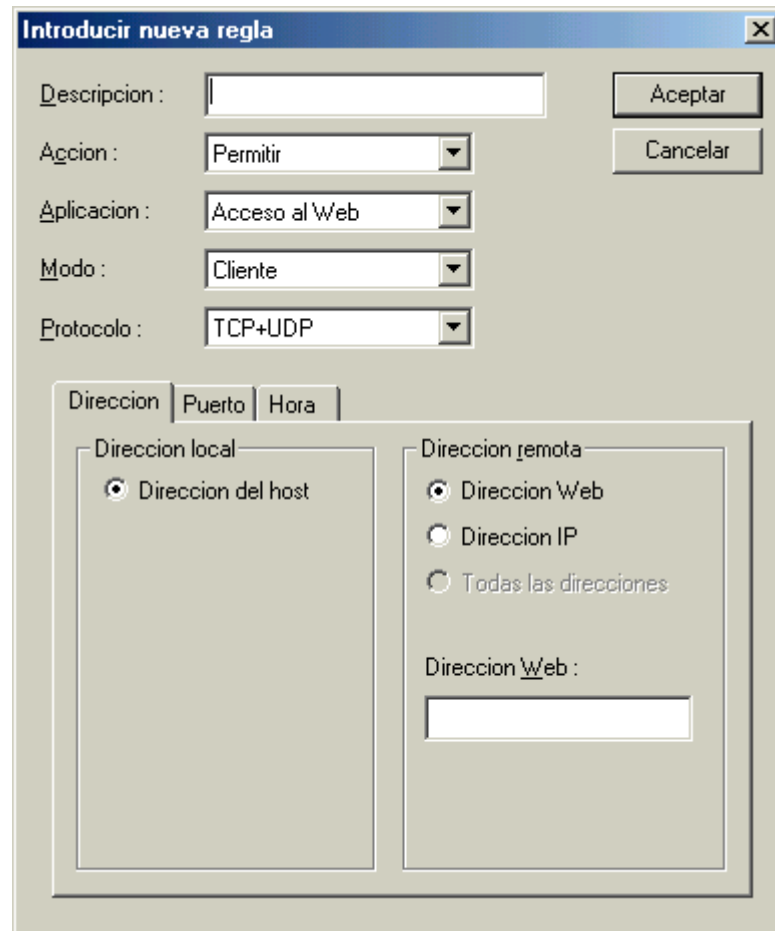


Figure 6

Están disponibles los siguientes campos:

Descripción	Escriba una descripción para la regla que se está creando.
Acción	Decida si la regla va a Permitir o a Bloquear el tráfico definido.
Aplicación	Seleccione una aplicación de la lista predefinida o escriba un nombre nuevo para la aplicación a la que se aplica esta regla.
Modo	Especifique si la máquina local será un cliente o un servidor para esta regla. La especificación de cliente significa que la regla se aplicará al tráfico saliente; la de servidor, que se aplicará al entrante.

Las fichas Dirección (Figure 7), Puerto (Figure 8) y Hora (Figure 9) se utilizan para especificar las funciones avanzadas de la regla.

Dirección:

The screenshot shows the 'Introducir nueva regla' dialog box with the 'Dirección' tab selected. The fields are: Descripción (empty), Acción: Permitir, Aplicación: Acceso al Web, Modo: Cliente, and Protocolo: TCP+UDP. The 'Dirección' section has two columns: 'Dirección local' with 'Dirección del host' selected, and 'Dirección remota' with 'Dirección Web' selected. Below 'Dirección remota' is a text field for 'Dirección Web'.

Figure 7

Para las reglas estándar, la única opción disponible en esta ficha es "Todas las direcciones"

Para las reglas avanzadas se puede especificar el sitio al que se aplica la regla, por dirección URL o IP.

La selección del botón de opción URL permite la entrada de un URL en el campo Dirección.

La selección del botón Dirección IP cambia el campo Dirección a un campo de entrada de dirección IP.

Puerto:

The screenshot shows the 'Introducir nueva regla' dialog box with the 'Puerto' tab selected. The fields are: Descripción (empty), Acción: Permitir, Aplicación: Acceso al Web, Modo: Cliente, and Protocolo: TCP+UDP. The 'Puerto' section has two columns: 'Puerto local' with 'Todos los puertos' selected, and 'Puerto remoto' with 'Lista de puertos' selected. Below 'Puerto remoto' is a text field for 'Lista de puertos' containing '80' and '443', with 'Agregar' and 'Eliminar' buttons below it.

Figure 8

La ficha Puerto se utiliza para especificar el puerto o el rango de puertos al que se aplica la regla. Los puertos se deben configurar para las máquinas local y remota. Están disponibles las siguientes opciones:

- **Puerto único:** Permite que se especifique un número de puerto único para la regla.
- **Rango del puerto:** Permite que se especifique un rango de puertos para la regla.
- **Lista de puertos:** Permite que se especifique una lista de puertos para la regla.
- **Todos los puertos:** Hace que la regla se aplique a todos los puertos.

Hora:

Día	Estado
<input checked="" type="checkbox"/> Lunes	Activado
<input checked="" type="checkbox"/> Martes	Activado
<input checked="" type="checkbox"/> Miércoles	Activado
<input checked="" type="checkbox"/> Jueves	Activado
<input checked="" type="checkbox"/> Viernes	Activado
<input checked="" type="checkbox"/> Sábado	Activado
<input checked="" type="checkbox"/> Domingo	Activado

Esta ficha permite que la regla esté activa solamente en días específicos.

Figure 9

5 Listas Web

Se pueden usar listas Web para permitir o bloquear el acceso a sitios específicos. Las listas de URL pueden ser Listas negras o Listas blancas. Las listas Negras y Blancas son mutuamente exclusivas, es decir, los usuarios configurados para utilizar una lista negra no se pueden configurar para utilizar una blanca y viceversa.

5.1 Listas negras

Las listas negras se utilizan para bloquear el acceso a sitios que puede permitir una regla. Por ejemplo, una regla estándar puede estar configurada para permitir el acceso a todo el Web, pero un sitio determinado, como www.notallowed.com, aparece en la lista negra. En estas circunstancias, el usuario podrá explorar todos los sitios Web salvo www.notallowed.com.

5.2 Listas blancas

Las listas blancas se utilizan para permitir el acceso a sitios que puede bloquear una regla configurada. Por ejemplo, una regla estándar puede bloquear el acceso a todo el Web, pero un sitio determinado, como www.disney.com, aparece en la lista blanca, de forma que el usuario no podrá explorar ningún sitio Web salvo www.disney.com.

5.3 Listas globales y locales

Hay dos tipos de listas blancas y negras: locales y globales. Las listas globales las crea el Administrador y se pueden aplicar a todos los usuarios; las entradas de la lista global se aplicarán a todos los usuarios para los que el Administrador ha especificado el uso de una lista de URL global. Las listas locales se crean solamente para un usuario específico; las entradas de esta lista solamente se aplican al usuario para el que se ha creado la lista.

6 Problemas con NetBIOS

En determinadas condiciones puede tener problemas al acceder a hosts usando NetBIOS sobre TCP/IP en modo Invisible. El problema se produce si la máquina utiliza transmisiones para determinar la dirección IP de un host en la red. En modo Invisible, TermiNet bloqueará los mensajes devueltos de los hosts, evitando el establecimiento de comunicaciones.

En estas circunstancias, es necesario escribir en el archivo "HOSTS" relacionando las direcciones IP de los hosts requeridos con sus nombres NetBIOS. "HOSTS" es un archivo de texto sin formato que se encuentra normalmente en el directorio C:\windows de Windows 98 o en el directorio c:\system32\drivers\etc de Windows NT y se puede modificar con cualquier editor de texto. Un archivo de ejemplo llamado hosts.sam situado en el directorio proporciona información de la estructura de archivos. Un archivo host normal tendría un aspecto como éste:

```
192.168.25.2 myserver.myorg.com
192.168.56.10 nt_server_1
```

Si desea agregar un host con el nombre nt_server_2 con la dirección IP 192.168.35.23, modifique el archivo de esta forma:

```
192.168.25.2 myserver.myorg.com
192.168.55.10 nt_server_1
192.168.35.23 nt_server_2
```

El problema no se planteará si la red tiene configurado un servidor WINS.