CHAPTER 10

Systems Management

Windows 95 is the first version of Windows expressly designed for manageability. The design ensures that management of the Windows 95 PC is accessible both locally and remotely via a privileged network manager. Network security is used to determine administrator-privileged accounts using pass-through security. Windows 95 also provides for PC users to be logically separated from the underlying configuration of their PCs so that the PC and user configurations and privileges can be managed independently. As a result, network managers can allow users to "rove" on the network—that is, log on from virtually any PC on the network and then operate from a desktop that has the correct settings and network privileges. The logical separation also means that a single PC can be shared by multiple users, each with a different desktop configuration and different network privileges.

Given the proliferation of PCs connected to corporate networks, the Windows 95 PC must be able to participate in any network-wide management schemes. Windows 95 is designed to meet various network management criteria by providing built-in support for several of the key network management standards. With this infrastructure built into Windows 95, network management applications will be able to provide tools for network managers to keep PCs and networks running more efficiently and cost effectively.

Open management interfaces are key to the management implementation in Windows 95. Where a standard exists, Windows 95 implements an enabling technology to embrace the standard—for example, an SNMP agent is supplied to enable remote management of Windows 95 PCs via any number of third-party SNMP consoles. Where no standard exists, the management interfaces are documented in the Win32 API set. Microsoft expects that management software will be available for Windows 95 from a wide range of vendors.

The following list outlines the key components of the management infrastructure in Windows 95:

- The Registry
- The Registry Editor
- User Profiles (the user component of the Registry)
- Hardware Profile (the system component of the Registry)
- System Policies (the network and system policy component of the Registry)
- The System Policy Editor
- Remote Administration Security (the remote admin authentication scheme)
- Remote Procedure Call (the mechanism used to remotely administer Windows 95)
- NetWatcher

- The System Monitor
- The SNMP Agent
- The DMI Agent
- Backup Agents, such as Cheyenne ARCServe and Arcada MTF

The discussion of the management infrastructure in Windows 95 is organized as follows:

- The Registry
- User Management
- System Management
- Network Management

The Registry

The Registry is the central repository in which Windows 95 stores all its configuration data. The Windows 95 system configuration, the PC hardware configuration, Win32–based applications, and user preferences are all stored in the Registry. For example, any Windows 95 PC hardware configuration change that is made via a Plug and Play device is immediately reflected in a configuration change in the Registry. Because of these characteristics, the Registry serves as the foundation for user, system, and network management in Windows 95.

The Registry essentially replaces the various MS-DOS and Windows 3.11 configuration files, including AUTOEXEC.BAT, CONFIG.SYS, WIN.INI, SYSTEM.INI, and the other applications .INI files. However, for compatibility purposes, instances of CONFIG.SYS, WIN.INI, and SYSTEM.INI files may exist on a Windows 95 PC for backward compatibility with either 16-bit device drivers or 16-bit applications that must run on Windows 95. For example, 16-bit applications will probably continue to create and update their own .INI files.

The Registry concept in Windows 95 is built upon the Registry concept first implemented in Windows NT. The Registry is a single configuration datastore built directly into the operating system. Although it is logically one datastore, physically it consists of three different files to allow maximum network configuration flexibility. Windows 95 uses the Registry to store information in the following three major categories:

- User-specific information, in the form of User Profiles, is contained in the USER.DAT file.
- Hardware or computer-specific settings (the Hardware Profile) are contained in the SYSTEM.DAT file.
- System Policies are designed to provide an override for any settings contained in the other two Registry components. System Policies may contain additional data specific to the network or corporate environment, as established by the network manager. They are contained in the POLICY.POL file. Unlike SYSTEM.DAT and USER.DAT, POLICY.POL is not a mandatory component of a Windows 95 installation.

Together, these three components comprise the Registry. Breaking the Registry into these three logical components provides the following benefits:

- The Registry components can be located in physically different locations. For example, the SYSTEM.DAT component and other Windows 95 system files might be

located on the PC's hard disk, and the USER.DAT component might be located in the user's logon directory on a network server. With this configuration, users can log on to various PCs on the network and still have their unique network privileges and desktop configuration, allowing the "roving user" network configuration for Windows 95.

- All of the Registry files and the rest of the system files in Windows 95 can be installed on a network server. This configuration enables Windows 95 to be run on a diskless or remote initial program load (RIPL) workstation, or from a floppy disk boot configuration. With this scenario, Windows 95 can be configured to page to a local hard disk but still load all its system files from a server.
- The Registry and all of the system files can be installed on the local hard disk. With this configuration, multiple users can share a single Windows 95 PC. Each user has a separate logon username, separate user profile, separate privileges, and separate desktop configuration.
- The network manager can administer an entire network's user privileges by having a single, global POLICY.POL file. Or the network manager can establish these policies on a server basis or on a per-user basis. In this fashion, a network manager can centrally enforce a "common desktop configuration" for each end-user type. For example, a data-entry Windows 95 PC can be configured so that only two applications—the data entry application and e-mail—can be run. Additionally, the network manager can specify that data-entry users cannot modify this desktop configuration. In spite of this configuration, the Windows 95 PC can fully participate in the network and is fully configurable if a different user with more network privileges logs onto the same PC.
- Separate privileges can be assigned to users and to a PC. For example, if a user who has sharing privileges logs onto a Windows 95 PC that has no sharing (no peer services), the user cannot access the PC's resources. This feature is useful if certain PCs contain sensitive data that should not be "shareable" to the corporate network.

The Registry contains ordered pairs of keys and their associated values that are manipulated via the Win32 Registry APIs. For example, the Registry might have a Wallpaper key with an associated value of WORK.BMP, meaning that the current desktop background is configured to use the "Work" bitmap.

Additionally, a special category of keys known as *dynamic keys* are either pointers to a memory location or a call-back function. Dynamic keys are a new Registry enhancement in Windows 95. They are used by device drivers or Windows 95 subsystems that want to register a dynamic data type, such as a counter, in the Registry. In the case of network cards, the dynamic keys represent data such as data transfer rates, number of framing errors, packets dropped, and so on. In general, dynamic keys are used for data that is updated frequently and is therefore not well suited for storage in the disk-based Registry. Because the dynamic keys exist in memory, their data can be quickly updated and quickly accessed. The data can be accessed by the system performance tools in Windows 95, which call the Registry for the data they are monitoring.

Arbitrary keys and values can be created either programmatically or by using the Registry Editor (REGEDIT) tool. The APIs for managing the Registry are the Win32 Registry APIs, which can be remotely invoked via the Microsoft RPC (DCE-compliant) support built into Windows 95. Windows 95 includes both the client and server portions of Microsoft RPC, making the Registry manageable remotely from another Windows 95 PC.

In this scenario, the network manager's system is the RPC client. It accesses the Registry APIs on the target Windows 95 PC via the RPC server running on the target machine. This RPC access to the Registry is secure, and network managers can limit access to either named privileged users or a group of network managers.

The Registry is also editable using the Registry Editor utility. As shown in Figure 61, the Registry consists of various parallel "trees." The Registry Editor is built upon the RPC support and can edit the local Windows 95 Registry, as well as the Registries on remote Windows 95 PCs. Although the Registry Editor is very powerful, it is fairly rudimentary in design and is intended for use by knowledgeable PC and network support staff or power users. Most end-users will never use the Registry Editor because Registry entries are usually modified via the Control Panel, by applications, or via Plug and Play.

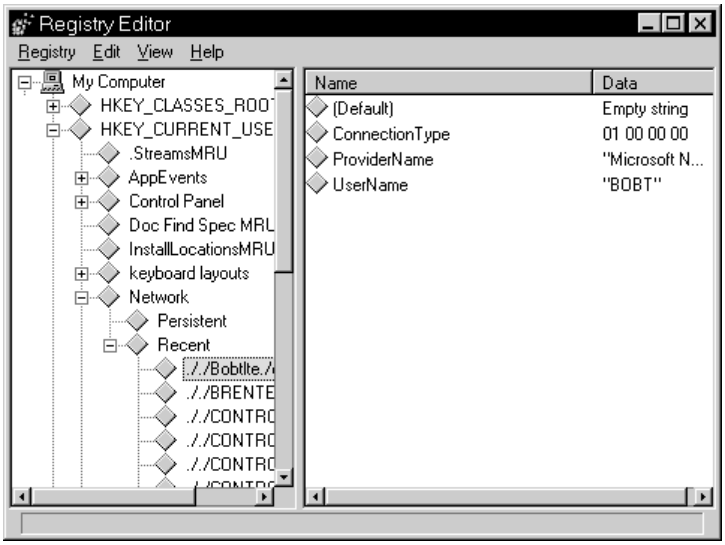

Figure 61. The Registry Editor, showing the settings stored in the Registry, which can be accessed remotely

As Figure 62 illustrates, the Registry is the central datastore that all system management services build upon. Note that all key subsystems are united by the Registry, and "agents" for standard management protocols, such as SNMP, are implemented for Windows 95 using the Registry and Registry services.

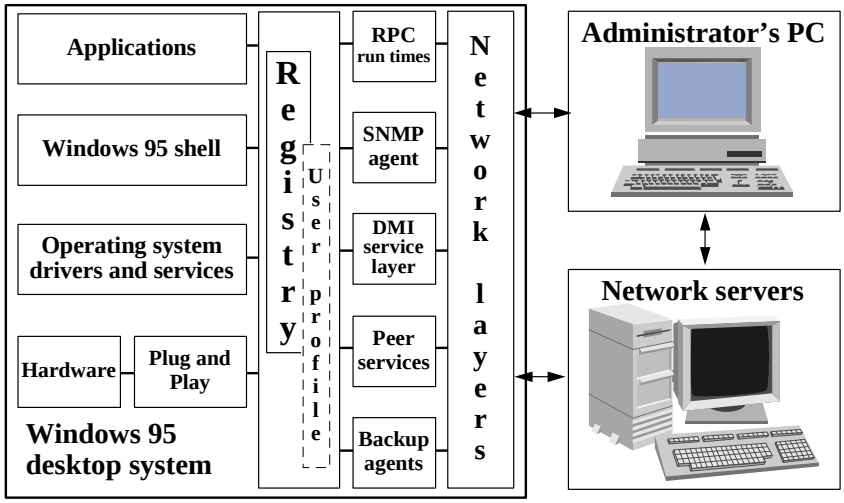

Figure 62. The Windows 95 management architecture, showing the central role of the Registry

User Management

Windows 95 is the first version of Windows to implement functionality for management of user-specific configurations and user-specific privileges. User management under Windows 95 is most evident with the introduction of a user logon dialog box that minimally prompts users for their logon names and passwords each time they reboot a Windows 95 PC. This logon dialog box captures the username and password, which can trigger Windows 95 to dramatically reconfigure the desktop and, as needed, limit access to either network resources or sharing capabilities from this Windows 95 PC. Windows 95 can also pass the username and password through to registered applications and network services that use the Windows 95 logon information as a "master key" for granting or denying access.

The user management capabilities in Windows 95 are built upon the following components:

- User Profiles
- System Policies
- Server-Based Security

User Profiles

In Windows 3.11, settings unique to a user were located in many disparate locations, including AUTOEXEC.BAT, CONFIG.SYS, WIN.INI, SYSTEM.INI, and numerous application-specific .INI files. Because this data was often intertwined with the Windows internal configuration data, providing good user management using Windows 3.11 was very difficult. For example, the simple task of allowing multiple users to work on a single PC was not possible with "out-of-the-box" Windows 3.11. Managing multiple user configurations on a network was even more difficult.

Various tools and products attempted to retroactively address the lack of user management capabilities in Windows 3.11. Out of necessity, many companies wrote their

own user management tools or used third-party products to help manage multiple users on their networks. Very often, this user namespace did not leverage the existing namespace of the corporate network resident on the network servers. In some cases, the user management software was implemented as a replacement Windows shell, with varying degrees of compatibility with existing Windows–based applications and the underlying network client software.

User management in Windows 95 is integral to the system and is implemented in a feature known as User Profiles. User Profiles are part of the Registry, and they contain system, application, and network data that are unique to individual users of a Windows 95 PC. The User Profile characteristics can be set by the user, by the network manager, or by the help-desk staff. In contrast to Windows 3.11, the User Profiles in Windows 95 are contained within a single file named USER.DAT. By keeping all user-specific data in one file, Windows 95 can provide a means to manage the user of the PC separately from the configuration of the Windows 95 operating system and the PC hardware. This separation also allows the user information to be located in a physically different location than that of the system configuration. It also allows the User Profiles to be updated separately from the rest of the Registry. All settings contained within a User Profile are administerable locally or remotely from another Windows 95 PC. Windows 95 enables centralized user management, and the network manager can user the Registry Editor provided with Windows 95 or a variety of third-party tools to automate management of User Profiles.

The settings contained in User Profiles include the following:

- Windows 95 settings, including desktop layout, background, font selection, colors, shortcuts, display resolution, and so on
- Network settings, including network connections, workgroup, preferred server, shared resources, and so on
- Application settings, including menu and toolbar configurations, fonts, window configuration preferences, and so on

User Profiles can effectively be disabled for Windows 95 PCs with only one user, by disabling the option that gives each user a separate desktop in the property sheet for security, shown in Figure 63.

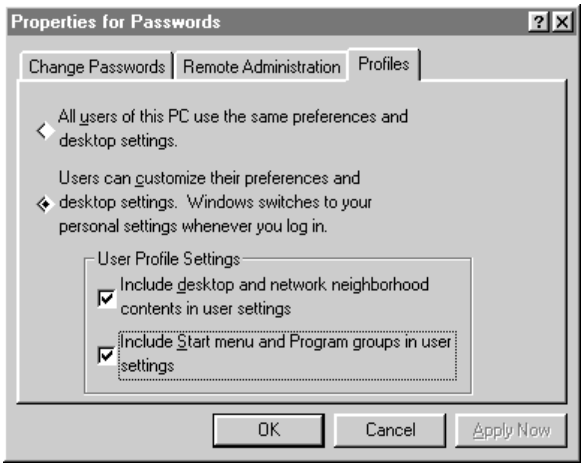

Figure 63. The property sheet for security, showing User Profiles enabled and specifying unique desktops, Taskbar options, and program groups for each user

System Policies

System Policies are designed to give network managers the ability to customize control over Windows 95 for users of differing capabilities or network privilege levels, including control of the user interface, network capabilities, desktop configuration, sharing capabilities, and so on. Like the other two Registry components, System Policies consist of pairs of keys and values. Unlike the other two Registry components, System Policies are designed to override any settings that may exist in User Profiles or Hardware Profile. System Policies are not necessary to enable a Windows 95 system to boot. They are loaded last and are typically downloaded from a location on the network server defined by the network manager.

System Policies can be used to define a “default” setting for the User Profile or the Hardware Profile, as shown in Figure 64. Default settings for both a default user and a default computer may solve the problem of preconfigured PCs for network managers. New PC hardware comes pre-installed with Windows and, in some cases, with the network hardware and software necessary to connect to the corporate network. Many network managers have a network-wide standard Windows 3.11 that they configure by hand on each PC before the PC is allowed on the corporate network. However, if a PC is delivered directly to an end-user, as is often the case, the network manager doesn’t have the opportunity to install the network-wide standard configuration on that PC. Default System Policies can solve this problem. For example, if the network-wide standard Windows configuration consists of a standard set of applications and a standard set of network privileges, such as servers to which connection is allowed, the network manager can preconfigure a default user-based set of System Policies to “enforce” these standards the first time the PC is connected to a network server. Assuming that the user logs on with a valid network logon username, the network privileges made available will be exactly those that the user is entitled to.

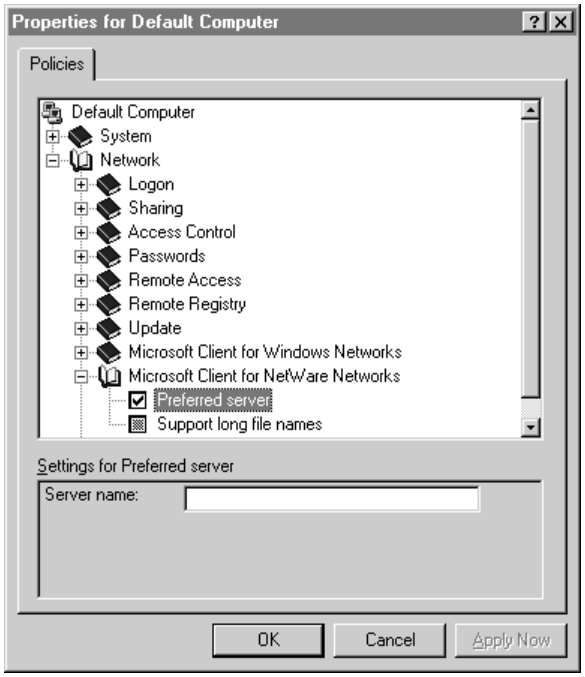

Figure 64. The System Policies properties for a default computer

The range of desktop control offered by System Policies is fairly comprehensive and includes standard network connections and the enabling and disabling of peer sharing capabilities, as well as such controls as password aging. For example, the network manager can define a desktop for a user and then "lock down" this desktop configuration by turning on the attribute that makes the desktop unmodifiable by the user. The network manager can also ensure that the user has access only to approved applications by not allowing the user to run any other programs. This restriction prevents the user from running programs from the command line or from the UI browsers and thus prevents installation of additional software. Another example of the way System Policies might be used is to disable elements of the Control Panel for users who have the habit of reconfiguring their PCs and as a result, are perennially "help-desk intensive."

System Policies for Users

Windows 95 supports a set of System Policies integrated with various system components for controlling the Windows 95 environment on a per-user basis. The following areas and System Policies can be controlled for users:

- **Control Panel.** Within this category of options, network managers can set policies to prevent the user from accessing Control Panel features. Policies include:
    - Restricting access to the Control Panel's Display settings, Network settings, Printers settings, System settings, and Security settings
- **Desktop.** Policies can prevent users from modifying desktop features. Policies include:
    - Specifying a wallpaper and color scheme to be used
- **Network.** The network policies provide restrictions to file and printer sharing. Policies include:
    - Disabling file sharing and printer sharing controls
- **Shell.** The shell (UI) policies can be used to customize folders and other elements of the desktop and to restrict changes to the UI. Policies include:
    - Customizing the user's Programs folder, Desktop items, Startup folder, Network Neighborhood, and Start menu

    Restrictions include:

    - Removing the Run and Find commands from the Start menu
    - Removing folders and the Taskbar from Settings on the Start menu
    - Hiding drives in My Computer and hiding the Network Neighborhood
    - Removing Entire Network from the Network Neighborhood
    - Hiding all items on the desktop
    - Disabling the Shut Down command, which prevents changed settings from being saved at exit
- **System.** These policies restrict the use of Registry editing tools, applications, and MS-DOS–based applications. Policies include:

- Restricting the use of Registry editing tools
- Running only selected Windows–based applications
- Disabling the ability to run an MS-DOS command prompt and single MS-DOS application mode

System Policies for Computers

Windows 95 supports a set of System Policies integrated with various system components for controlling the Windows 95 environment on a per-computer basis. The following areas and System Policies can be controlled for computers:

- **System.** These policy settings relate to the computer configuration. Policies include:
  - Identifying the network path for Windows Setup
  - Enabling User Profile support
  - Identifying items to be run each time the computer starts or to be run only once when the computer first starts
- **Network.** These policy settings relate to the network configuration of the computer. Policies include:
  - Controlling logon settings
  - Disabling file and printer sharing
  - Activating user-level security
  - Controlling password settings
  - Disabling remote dial-up access
  - Controlling remote access to the Registry
  - Defining properties for remote policy updates
  - Defining settings for the Client for Microsoft Networks and the Microsoft Client for NetWare Networks
  - Setting attributes for the SNMP service

Registry Tools

The primary user management tools in Windows 95 are the Registry Editor and the System Policy Editor. For most other types of user administration, network managers use the same user accounts tools on their PC servers that they used before Windows 95.

Registry Editor

The Registry Editor allows network managers to directly read and write values that are contained in the User Profiles and the Hardware Profile in the Registry. Using this tool, network managers can read current settings, modify them, create new keys and values, or delete current keys and values in the Registry.

The Registry Editor can edit remote Registries using the RPC-enabled Win32 Registry APIs built into Windows 95. In the case of a User Profile residing on a network server, the network manager simply connects to the network server and opens the file using normal file I/O—no RPC connection is needed between the Windows 95 client and the network server.

System Policy Editor

The System Policy Editor, shown in Figure 65, generates the System Policies file, POLICY.POL. This tool allows network managers to specify specific network policies or user configurations for Windows 95. The tool is extensible by third parties; the ADF format is a text file that can be extended by network tool vendors or by network managers as needed. The System Policy Editor works via local file I/O and is not RPC-enabled. Because the System Policies file is located centrally on a network server, typically one copy is needed per server. All the network manager needs to do is connect to the network server and edit the System Policies file.

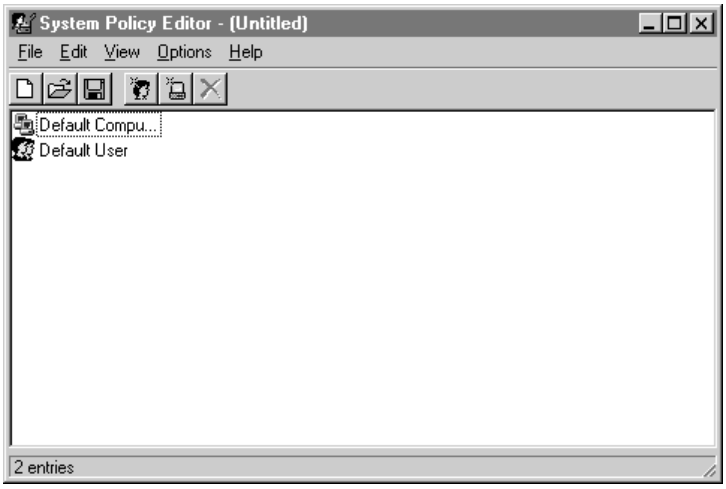

Figure 65. The System Policy Editor, which enables administrators to define policies on a per-user basis

The Role of the Server in Systems Management

In user management, the server plays a central role. All user namespace management is performed on the network server, so the native user-level security mechanism built into the network server is used by Windows 95 for user logon authentication and pass-through security. Windows 95 has no built-in user-level security mechanism of its own. As a consequence, network managers can use the familiar server administration tools to manage user accounts for Windows 95.

The second role of the server in user management in Windows 95 is to contain copies of User Profiles and System Policies. Typically, User Profiles are stored in user directories that are read/write enabled for the user. As changes are made to the local copy of User Profiles, the copy that resides on the server is updated—Windows 95 keeps the local and network image synchronized. System Policies should be stored in a directory that is accessible to all user logons and should be made read only for users to ensure that only network managers can modify the network-wide policies that the System Policies file may define.

System Management

Windows 95 systems have been designed to be managed well, both locally and remotely, using the Registry's remote capabilities. The Registry enables network managers to remotely manage the system software settings of Windows 95, including settings used by device drivers. For example, network managers can remotely change the network frame type in use on all the PCs under their oversight. Prior to Windows 95, this task would, in many cases, be performed by directly editing the NET.CFG or PROTOCOL.INI files.

Plug and Play makes the hardware configuration of Windows 95 PCs much more manageable. It also addresses a paramount problem facing users and help-desk staff: that of proper hardware configuration. One of the more complex hardware/software configuration problems revolves around the use of portable-computer docking stations. Typically, portable-computer users have a "boot configuration" manager to help manage the different devices that need to be installed when the computer is docked or when it is remote. Creating these configurations is very time-consuming and must often be done for each system setup because of conflicts with other device drivers that may be installed. Plug and Play automates docking, as well as the use of PCMCIA cards, and helps with link management when moving from fast links to slower asynchronous links. The Windows 95 system detects events such as docking/undocking, PCMCIA card insertion/removal, and moving between fast/slow media and appropriately loads and unloads device drivers and configures them automatically. Windows 95 also notifies applications that the device is either available or unavailable.

The Windows 95 Tools

Windows 95 includes a variety of tools that allow users or network managers to configure the hardware and software on a Windows 95 PC. These include the following:

- **The Control Panel.** Most key system settings are accessible via the Control Panel, which has traditionally been the only interface available for directly modifying the configuration of hardware and software settings in Windows. The Control Panel in Windows 95, like its Windows 3.1 predecessor, is extensible and provides the best local mechanism for managing all system settings. In Windows 95, all network settings have been consolidated into a single Network tool, rather than being split between several discrete applications as in prior versions of Windows.

- **Context Menus and Property Sheets.** Context menus and property sheets list a number of actions that can be directly applied to system objects. They are displayed by right-clicking the object. For example, the Properties command on the context menu for a directory with sharing enabled allows users to invoke sharing of the directory. The Properties command on the context menu for a server tells whether the server is a NetWare server, a Windows NT server, or a Windows 95 system.

- **Plug and Play.** The current hardware configuration for the system is accessible via the Control Panel's System tool. All hardware device nodes in the hardware tree are shown, with current configuration settings. These settings are updated dynamically whenever a device's configuration changes or if the device is inserted or removed.

- **The Registry Editor.** For network managers or help-desk staff, the Registry Editor allows remote viewing and editing of the full Registry. Data contained in the Registry is represented in its hierarchical tree structure as pairs of keys and values.

- **The System Policy Editor.** System capabilities can be enabled or disabled using the System Policy Editor. For example, sharing can be disabled on a machine basis, or local Control Panel usage can be disabled for non-privileged users.
- **The SNMP agent.** Remote desktop management, including hardware and software inventory and the ability to make remote changes to the system, is possible via the SNMP agent for Windows 95.

Performance Monitoring

Windows 95 includes an enhanced performance monitoring utility that enables network managers and help-desk staff to more quickly troubleshoot performance problems caused by an invalid configuration or some other conflict. The System Monitor, shown in Figure 66, is the replacement for WinMeter in Windows for Workgroups. It provides more detailed information about the system's I/O performance, including file I/O and network I/O performance. Data is gathered on an FSD basis, which means information can be gathered from the FAT file system and any number of network redirectors that may be loaded. The interfaces to the System Monitor are open and are extensible by third parties.

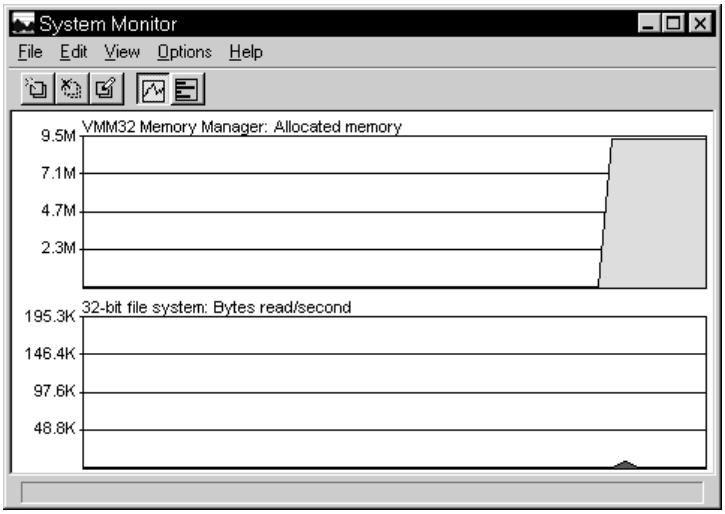

Figure 66. The System Monitor, which allows local and remote monitoring of system performance

For network managers, the key feature of System Monitor is its ability to monitor a remote system. This capability is built upon remote Registry access because performance data is registered with the system using dynamic keys contained within the Registry. For example, a network manager who is attempting to troubleshoot a "slow PC" can discover remotely that the NIC has an unusually high number of dropped frames and can then use the Registry Editor to see how the network card is configured.

Network Management

Windows 95 includes a number of features to facilitate the use of a variety of network management tools. Many of these tools require support in the client to enable their operation. In some cases a formal industry standard exists, and in others, a de facto standard has emerged. Either way, Windows 95 enables some of the key network

management tools by building the necessary “agent” software into the client operating system.

Server-Based Backup

Windows 95 includes agents for the remote backup of the Windows 95 system by a server-based backup system. The following backup agents are included with Windows 95:

- Cheyenne ARCServe agent for backup to NetWare and Windows NT Server servers
- Arcada Backup agent for backup to NetWare and Windows NT Server servers

These agents make it possible to include Windows 95 systems in a scheduled, automatic remote backup scheme managed centrally via the server-based backup system. Their property sheets are shown in Figure 67 and Figure 68.

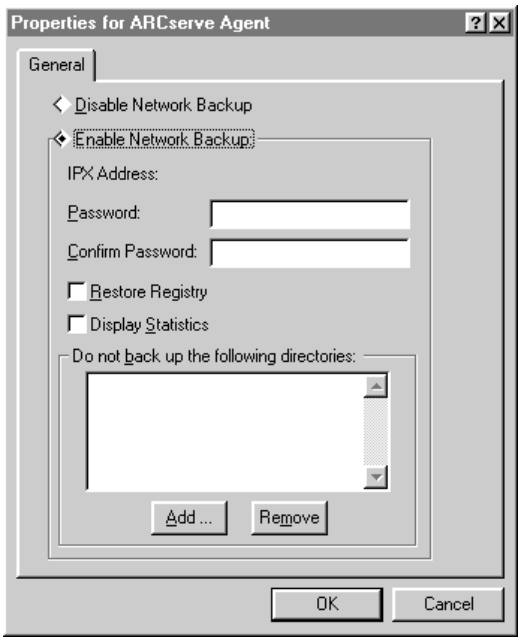

Figure 67. The property sheet for the Cheyenne ARCServe agent

Figure 68. The property sheet for the Arcada Backup agent

Both backup agents include a number of enhancements for Windows 95. For example, both agents include the ability to backup and restore long filenames. (If the native tape format does not include a mechanism for storing long filenames, the agents provide special logic to facilitate saving and restoring the long filenames.) Both agents have also been enhanced to backup and restore the Registry.

Another enhancement for Windows 95 is the ability to secure operation of the backup agent by means of user-level security. By default, remote administration of the Windows 95 PC is enabled only for supervisor-privileged accounts, giving the ability to remotely back up Windows 95 systems only to network managers or help-desk staff. For example, only authorized personnel should be able to back up the hard disk of the CEO's and the corporate controller's PCs.

Network Management Tools

A category of tools is emerging onto the market that all claim to be network management tools. Many of these tools were actually designed to solve a specific problem but have been extended to become more general-purpose network management tools.

SNMP Support

Simple Network Management Protocol (SNMP) consoles are a good example of this trend. They are now being enhanced to monitor components of desktop systems as well as server applications such as database servers. Windows 95 includes an SNMP agent that supports the use of an SNMP console to manage Windows 95 PCs. The SNMP support in Windows 95 includes the following:

- An SNMP Agent
- An extensible MIB handler interface
- MIB-II support via TCP/IP

The SNMP agent provided with Windows 95 is extensible via its MIB handler interface, which enables third parties to include instrumentation of their software or hardware components and allows remote management via the SNMP console.

Because many corporations are beginning to migrate to TCP/IP as a standard protocol, the TCP/IP stack in Windows 95 has been instrumented for SNMP remote management. The MIB-II supports the Internet Engineering Task Force (IETF) Request for Comment (RFC) for the TCP/IP MIB definition. This support enables network managers to centrally monitor the performance of TCP/IP on the network from a central console.

DMI Support

Support for a Desktop Management Task Force (DMTF) DMI Agent will be made available for Windows 95 by Microsoft after the release of Windows 95.

The Windows 95 Tools

Windows 95 includes a number of built-in tools for network management, including NetWatcher (shown in Figure 69). NetWatcher allows local and remote management of users' connections to Windows 95 peer services. The tool shows all current connections to the Windows 95 system, who is connected, and which files and printers are in use. It allows disconnection of users and maintains a log of key system events, such as logon, logoff, system boot and shutdown, and failed attempts to connect.

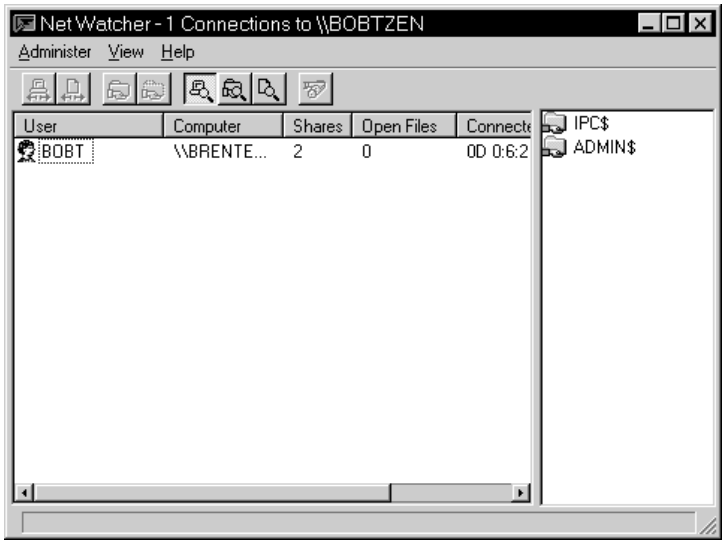

Figure 69. NetWatcher, which supports local and remote monitoring of connections to peer services

Additionally, Windows 95 includes the capability to access a special "administration share" of any capable Windows 95 PC. This share, which allows network managers to reconfigure the hard disks of remote PCs from their desktops, is accessed by displaying the property sheet for the remote PC from the Network Neighborhood. When this feature is activated, a window opens that appears to be a normal browsing window but is actually the remote PC's My Computer view. All files and other resources on the remote PC are then accessible.