C H A P T E R 9

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 a logical separation of the user of the PC, from the underlying configuration of the PC. This means that the PC and the user configurations and privileges can be managed independently. It also means that if a network manager chooses, a user can be enabled to "rove" on the network, that is logon from virtually any PC on the network and operate in their desktop with the correct settings and network privileges. Additionally it means that a single PC can be shared by multiple users, each with a different desktop configuration and differing network privileges.

Given the proliferation of PCs connected to the corporate network, it's key that the Windows 95 PC also participates in any network wide management schemes. Windows 95 is designed to meet these 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 are enabled that will provide tools for the network manager to keep the PCs and networks running more efficiently and cost effectively.

Key to the management implementation in Windows 95 is that the management interfaces are open. Where a standard exists, Windows 95 implements an enabling technology to embrace the standard. For example, supplying an SNMP agent 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. It is Microsoft's expectation that management software will be available for Windows 95 from a wide range of vendors.

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

- The Registry
- Registry Editor
- User Profiles—user component of the Registry
- Hardware Profile— system component of the Registry
- System Policies— network and system policy component of the Registry
- System Policy Editor
- Remote Administration Security—remote admin authentication scheme
- Remote Procedure Call—mechanism used to remotely administer Windows 95
- NetWatcher
- System Monitor—performance monitor
- SNMP Agent
- DMI Agent
- Tape Backup Agents—ARCServe, 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 the whole of its configuration data. The Windows 95 system configuration, the PC hardware configuration, Win32 applications, and user preferences are all stored in the Registry. For example, any Windows 95 PC hardware configuration change that's 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, we expect that 16-bit applications will continue to create and write to their own various .INI files.

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

- User specific information, these are user profiles contained in the file USER.DAT.
- Hardware or computer-specific settings are contained in the file SYSTEM.DAT.
- System policies are designed to provide an override to any settings contained in the above two components of the Registry. System Policies may contain additional data specific to the network or corporate environment as established by the network manager. This is contained in the file POLICY.POL. 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. By breaking the Registry into these three logical components, Windows 95 gains a number of interesting benefits:

- The Registry components can be located in physically different locations. For example, the SYSTEM.DAT component and other system files in Windows 95 may be located on the PC's hard disk. The USER.DAT portion of the Registry may be located in the user's login directory on a network server. In this configuration, user's are able to logon to various PCs on the network and still have their unique network privileges and desktop configuration, thus 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 diskless or sometimes what is referred to as a remote initial program load (RIPL) workstation, or from a floppy disk boot configuration. In this scenario, it's also possible to configure Windows 95 to page to a local hard disk if desired, but still load all it's system files from a server.

- On a single Windows 95 PC, multiple users can share the system. Each will have a separate user logon name, and separate user profiles. Hence each use will have their own privileges set, and own desktop configurations. In this case, the Registry and all of the system files are installed on the local hard disk.
- Network managers can administer an entire networks users privileges via a single file. By having a global POLICY.POL file, effectively all Windows 95 PCs can have policies set by this one file. Or, these policies can be established on a server basis, or if needed, on a per-user basis. In this fashion a network manager can enforce a "common desktop configuration" for each end user type and have this managed centrally. For example, a data entry desktop can be configured to allow only two applications available to run, the data entry application and email as an example. Additionally this desktop can be configured to not allow any other programs to be run. Finally, the network manager can enforce that the desktop configuration cannot be modified by the end-user. However, this same Windows 95 PC can fully participate in the network and be 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, it's possible to have set no sharing (no peer services) on a Windows 95 PC, and have a user logged on the system that has sharing privilege. In this instance, the sharing is disabled, since the resources on the PC have been set as unshareable. 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." Both keys and values are manipulated via the Win32 Registry APIs. An example, a key in the Registry could be "Wallpaper." The associated value in this example could be "Work.bmp." In this example, this means that the current desktop background is configured as using the "Work" bitmap.

Additionally, there exist a special category of keys known as *dynamic keys*. Dynamic keys are either pointers to a memory location, or a call back function. These addresses are registered by a device driver or a Windows 95 subsystem that would like to register a dynamic data type in the Registry. Typically this data includes counters, or in the case of network cards the dynamic keys represent things like data transfer rates, number of framing errors, packets dropped, and so on. In general, the characteristic of dynamic keys is that its data is being updated frequently, and because of this, is not well suited for storage in the disk based Registry. The dynamic keys exist in memory, and can thus be quickly updated, and quickly accessed. This data can then be accessed by the system performance tools in Windows 95, which call the Registry for the data that they are monitoring. Dynamic keys are a Registry enhancement new for Windows 95.

Arbitrary keys and values can be created programatically, or using the Registry Editor (regedit) tool. The API for managing the Registry are the Win32 Registry API. These APIs 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 our RPC, making the Registry remotely manageable 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, network managers can limit access to either named privileged user accounts, or a group of network managers.

The Registry is also editable using the Registry Editor utility, as shown in Figure 1.

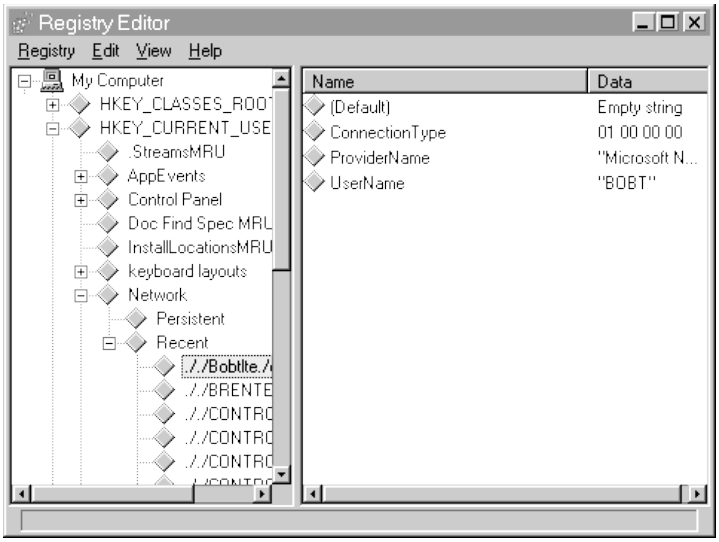

Figure 1. Network Settings are Stored in the Registry, and Can Be Accessed Remotely

Note in the figure that the Registry consists of various parallel "trees." The RegEdit utility is built upon the RPC support, and can edit the local Windows 95 Registry, as well as editing the Registry on a remote Windows 95 PC. The RegEdit tool while very powerful, is fairly rudimentary in its design. The utility is designed to be used by knowledgeable PC and network support staff, or power users. For most end users, Registry entries are modified through either the Control Panel, application settings, or via Plug and Play. That is, typically an end user should not be confronted with a scenario where they must use the Registry Editor tool.

Figure 2 illustrates how the Registry is the central data store that all system management services build upon. Note that all key subsystems are united by the Registry, and "agents" for standard management protocols like SNMP are implemented on Windows 95 using the Registry and Registry services.

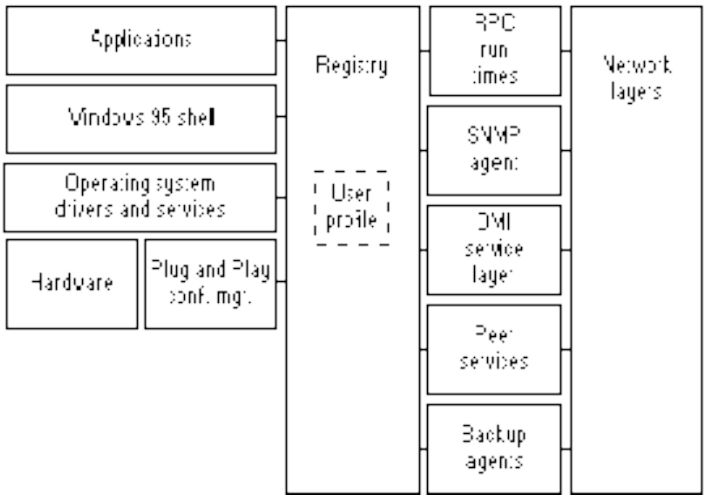

Figure 2. Windows 95 management architecture, showing the central role of the Registry

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 that minimally prompts the user for their logon name and password each time they reboot the Windows 95 PC. This logon dialog captures the username and password that can trigger Windows 95 to dramatically reconfigure the desktop configuration and as needed, limit access to either network resources or sharing capabilities from this Windows 95 PC. Windows 95 can also pass the user logon and password to registered applications and network services that use the logon in Windows 95 as the "Master Key" to enable the user access to these applications and services.

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; AUTOEXEC.BAT, CONFIG.SYS, WIN.INI, SYSTEM.INI and numerous application specific INI files. For example, this data was often intertwined with Windows internal configuration data, thus providing good user management using Windows 3.11 was very difficult to achieve. For example, the simple task of allowing multiple users to use a single PC was not achievable with Windows 3.11 "out of the box." Managing multiple user configurations on a network was even more difficult. Many companies out of necessity wrote their own user management tools, or used third-party tools to help mange multiple users on the network. Very often this user namespace did not leverage the existing namespace on 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 the existing Windows applications and the underlying network client software. All these tools and products attempted to retroactively address Windows 3.11's lack of user management capabilities.

User management in Windows 95 is integral to the system, it is implemented in a feature known as User Profiles. User Profiles are part of the Registry, they contain system, application and network data that are unique to the individual user of a Windows 95 PC. These characteristics can be set by the user, by the network manager or by the PC helpdesk 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. The network manager can user the Registry Editor provided with Windows 95, or a variety of third party tools that will be available to automate management of User Profiles in Windows 95.

In Windows 95, settings contained in User Profiles include:

- **Windows 95 Settings.** Desktop layout, background, font selection, colors, shortcuts, display resolution, and so on.
- **Network Settings.** Network connections, workgroup, preferred server, shared resources, and so on.
- **Application Settings.** Menu and toolbar configurations, fonts, window configuration preferences, and so on.

Finally, User Profiles can effectively be disabled if there is a single user of the Windows 95 PC. In this case the user can disable "each user gets a new desktop" option in the Control Panel.

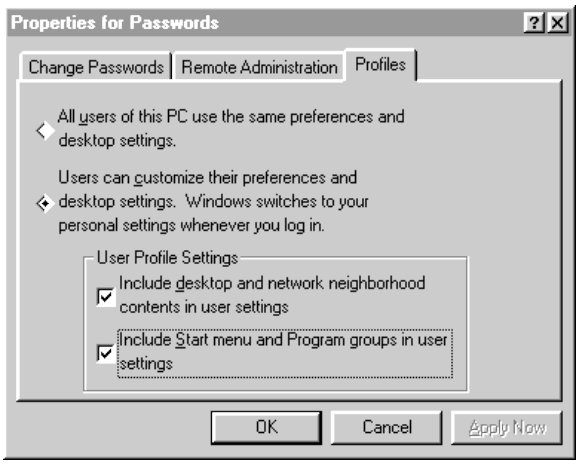

Figure 3. User Profiles enabled specifying unique desktops, taskbar options and program groups for each user

System Policies

In conjunction with User Profiles and the System Settings components of the Registry, System Policies are the final piece of the Registry. Like the other two Registry components, the 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 System Profiles. System Policies are not necessary to enable a Windows 95 system to boot. System Policies are loaded last, and are typically downloaded from a network server. Windows 95 provides a mechanism to allow the network manager to define a network location to find the System Policies file and download to this PC. System Policies are designed to give the network or PC manager the ability to customize

control over Windows 95 for users of differing capabilities or network privilege level. These capabilities include controls of the user interface, network capabilities, desktop configuration, sharing capabilities, and so on.

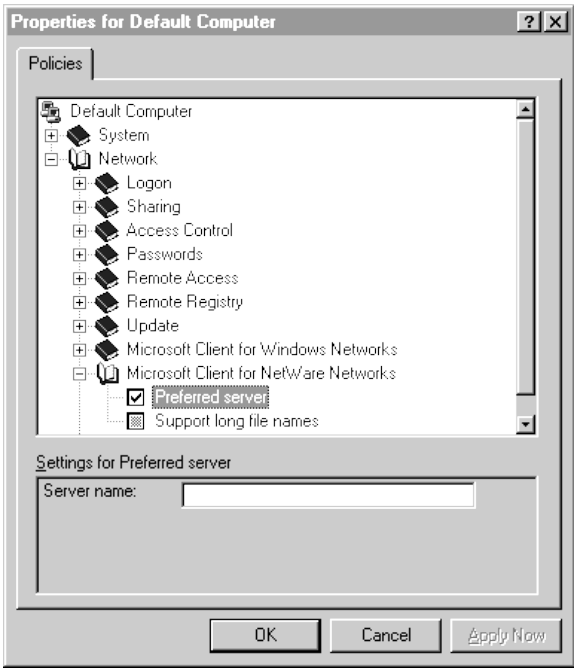

Figure 4. Policy Properties for a Default Computer

System Policies may be used to define a "default" setting for either the User Profile or System Settings. Default settings for both a default user and a default computer may solve the problem of pre-configured PCs for network managers. New PC hardware comes pre-installed with Windows and in some cases network hardware and software necessary to connect to the corporate network out of the box. Many network managers today have network-wide standard Windows 3.11 that normally are pre-configured by hand on each PC before allowing it on the corporate network. However, if PCs are directly fulfilled to end-users, as is often the case, the network manager will not have the opportunity to install the network wide standard configuration on this PC. However, the default System Policies may solve this problem. For example, assuming that the standard Windows configuration consists of a number of corporate standard applications and a standard set of network privileges (for example, servers they are allowed to connect to) then the default settings will "enforce" these standards the first time the PC is connected to a network server. Assuming that the user logs on with a valid network user logon name, then the network privileges that they'll see are

exactly those that they are entitled to today. In this case, the assumption is that the network manager had pre-configured a user based set of system policies.

The range of desktop control offered by System Policies is fairly comprehensive. The network manager can define a desktop for a user, then make the lock down this desktop configuration. This is accomplished by turning on the attribute that the desktop is unmodifiable by the user. Additionally, the network manager can further insure that the user only has access to the applications that they've installed by disallowing the user to run any additional programs. This means that the user cannot run programs from the command line or from the UI browsers, thus preventing them from installing additional software. Some other examples include disabling elements of the Control Panel for users that may have the habit of reconfiguring their PCs and thus are perennially "helpdesk intensive." As noted before, standard network connections, enabling and disabling of peer sharing capabilities and things like password aging, can all be implemented using the System Policies feature.

System Policies for Users in Windows 95

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 areas and system policies that can be controlled for users in Windows 95 include:

- **Control Panel.** Within this category of options, you can set policies to prevent the user from accessing Control Panel features.

  Policies include: Restricting access to Display Control Panel settings, Network Control Panel settings, Printers Control Panel settings, System Control Panel settings, and Security Control Panel settings

- **Desktop.** Policies can prevent users from modifying features for the desktop.

  Policies include: Specifying a wallpaper, and color scheme to use

- **Network.** The network policies provide restrictions to file and printer sharing.

  Policies include: Disabling file sharing and printer sharing controls

- **Shell.** You can use shell (that is, user interface) policies to customize folders on the desktop and to restrict changes to the user interface.

  Policies include: Ability to customize the user's Programs folder, Desktop items, Startup folder, Network Neighborhood, and Start menu. Restrictions include the ability to remove the "Run" command from the Start menu, remove folders from "Settings" item on Start menu, remove "Taskbar" from Settings item on Start menu, remove "Find" command, hide drives in My Computer, hide Network Neighborhood, remove "Entire Network" from Network Neighborhood, hide all items on the desktop, disable the Shut Down command, preventing changed settings from being saved at exit.

- **System.** These system policies restrict the use of Registry editing tools, applications, and MS-DOS-based applications.

  Policies include: Ability to restrict the use of registry editing tools, run only selected Windows–based applications, disable the ability to run an MS-DOS command prompt, disable single MS-DOS application mode.

System Policies for Computers in Windows 95

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 areas and system policies that can be controlled for computers in Windows 95 include:

- **System.** The system policy settings related to the computer configuration.

  Policies include: Identifying the network path for Windows Setup, enabling user profile support, and identifying items to run each time the computer starts up or to be run only once when the computer first starts

- **Network.** The system policy settings related to the network configuration of the computer.

  Policies include: Controlling logon settings, disabling file and/or printer sharing, activating user-level security, controlling password settings, disabling remote dial-in access, controlling remote access to the registry, defining properties for remote policy updates, defining settings for the Microsoft Client for Microsoft Networks and the Microsoft Client for NetWare Networks, and setting attributes for the SNMP service.

Registry Tools

The primary user management tools in Windows 95 are the Registry Editing and System Policies Editing tools. For most other user administration, network managers will use the user accounts tools on their PC servers that they already use today.

Registry Editing Tool

The Registry Editing Tool allows the network manager to directly read and write values that are contained in the User Profiles and System Settings portions of the Registry. Using this tool, it's possible to read current settings, modify them, create new keys and values or delete current keys and values in the Registry. The Registry Editing tool is able to edit remote Registry's, using the RPC-enabled Win32 Registry APIs built into Windows 95.

In the case of the 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. In this case, there is no RPC connection between the Windows 95 client and the network server.

System Policy Editor

The System Policy Tool generates the System Policies file, POLICY.POL. This tool allows the network manager to specify specific network policy 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 other network tool vendors, or network managers as needed. This tool works via local file I/O, and is not RPC enabled. Since the System Policies file is to located centrally on a network server, typically one copy is needed per server. Hence, all the network manager needs to do is connect to the network server, and edit the System Policies file.

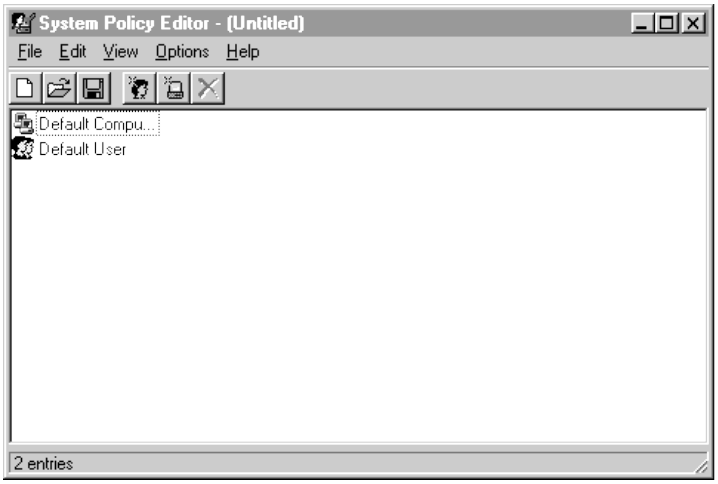

Figure 5. The System Policy Editor in Windows 95 Enables Administrators to Define Policies on a Per-User Basis

Role of the Server in Systems Management

In user management, the server plays a central role. All user "namespace" management is done on the network server. This means for user logon authentication, and pass through security the native user-level security mechanism built into the network server is used by Windows 95. Windows 95 has no built-in user-level security mechanism of it's own. As a consequence, the network managers 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 contained in user directories, and should be read/write enabled for the user. As changes are made to the local Windows 95 copy of the User Profiles, they are updating the image that resides on the server, Windows 95 keeps the local and network image synchronized. System Policies should be located in a directory that is accessible to all user logons, and should be made read only for users. This ensures that only network managers will have the rights to 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 a network manager remote management of the system software settings of Windows 95, including settings used by device drivers. For example, it would be possible for a network manager to remotely change the network frame type in use on all the PCs under their oversight. Currently this is done in many cases by hand directly editing NET.CFG or PROTOCOL.INI files.

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

Windows 95 Tools

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

- **Control Panel.** Traditionally, the only interface available to directly modify the configuration of hardware and software settings in Windows. The Control Panel in Windows 95 like its Windows predecessor is extensible, and provides the best local mechanism for managing all system settings. Most key system settings are accessible via the Control Panel. In Windows 95, all network settings have been consolidated into a single network Control Panel tool, rather than split between several discrete applications as in prior versions of Windows.
- **Context Menus and Property Sheets.** Context menus and property sheets offer a number of actions that can be directly applied to system objects. They are invoked via a right mouse button click. For example, the properties menu item in the context menu for a directory with sharing enabled allows the user to invoke sharing of the directory. Another example, the properties item of a server tells what type of server this is, namely 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. Within the 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.
- **Registry Editor.** For network managers or PC helpdesk, the Registry Editing tool 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.
- **System Policies Editor.** System capabilities can also be enabled or disable System Policies Editor. For example, sharing can be disabled on a machine basis, or local Control Panel usage can be disabled for non-privileged users.
- **DMI Agent.** Remote desktop management will be possible via the DMI agent for Windows 95. This includes both hardware and software inventory, and the ability to make remote changes to the system.

Performance Monitoring

Windows 95 includes an enhanced performance monitoring utility. This gives network managers and PC helpdesk the ability to more quickly troubleshoot performance problems caused by invalid configuration or some other conflict. The System Monitor is the replacement for Windows for Workgroups' WinMeter. It provides more detailed information about the system's I/O performance, which includes file I/O performance and network I/O performance. Data is gathered on an FSD basis, which means it's possible to gather information 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.

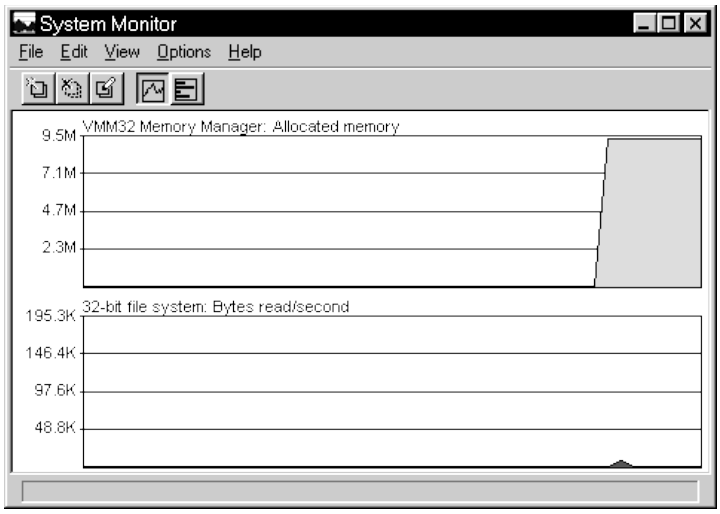

Figure 6. The System Monitor Tool in Windows 95 Allows Local and Remote Monitoring of System Performance

However, for network managers the key feature of System Monitor is its ability to monitor a remotes system. This capability is built upon remote Registry access, since performance data is registered with the system using "dynamic keys" contained within the Registry. For example, if a PC helpdesk person is attempting to troubleshoot a "slow PC," they can discover remotely that the NIC has an unusually high number of dropped frames. They can then move on to use the Registry Editing tool to see how the network card is configured.

Network Management

Windows 95 has included a number of features to facilitate the use of a variety of network management tools. Many of these tools by necessity require support in the client to enable their operation. In some cases a formal industry standard exists, and others, a de facto standard has emerged. In either case, Windows 95 enables some of the key network management tools by including the necessary "agent" software built-in to the client operating system.

Server-based Backup

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

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

By including these agents, it's now possible to include Windows 95 systems in an scheduled automatic remote backup scheme managed centrally via the server based backup system.

Both backup agents include a number of enhancements for Windows 95. For example, both agents will include the ability to backup and restore long filenames, even if the native tape format does not include a mechanism for storing long filenames. In this case, the agent includes special logic to facilitate saving and restoring the long filenames. Both agents also have been enhanced to backup and restore the Registry.

Another enhancement for Windows 95, is securing operation of the backup agent by the user-level security. By default, remote administration of the Windows 95 PC is enabled only for "supervisor" privileged accounts. This means that only network managers or PC helpdesk staff have the ability to remotely backup Windows 95 systems. For example, it's key that only authorized personnel backup the hard disk of the CEO's system, or of the corporate controller's PC.

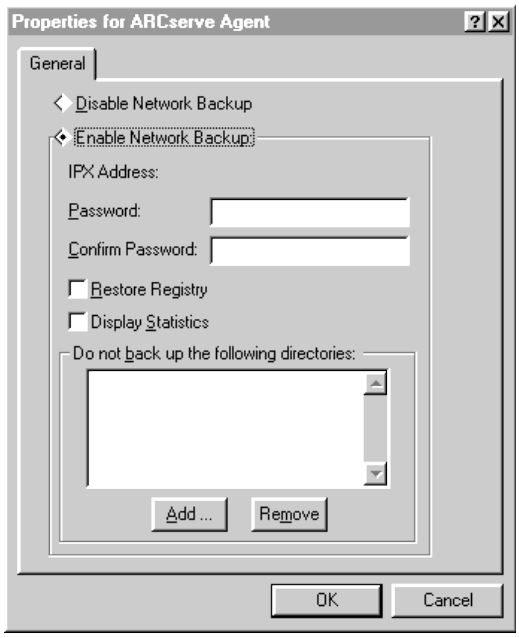

Figure 7. Property Sheet for the Cheyenne ARCserver agent

Figure 8. Property Sheet for the Arcada Backup Exec Agent

Network Management Tools

There is an emerging category of tools in the market that all claim to be network management tools. Many of the tools were actually designed to solve a specific problem, and 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, now being enhanced to monitor components of desktop systems, as well as server applications like database servers. Windows 95 includes an SNMP agent to support the use of an SNMP console to manage Windows 95 PCs. The SNMP support in Windows 95 includes:

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

The SNMP agent provided with Windows 95 is extensible via it's MIB handler interface. This enables third parties to include instrumentation of their software or hardware components and allow remote management via the SNMP console.

Since many corporations are beginning a migration 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 can offer the network manager the capability to centrally monitor the performance of TCP/IP on the network from a central console.

DMI Support

Windows 95 will also include support for the Desktop Management Task Force (DMTF) by supplying a DMI Agent, this however may be included after the availability of Windows 95.

Windows 95 Tools

Windows 95 includes a number of built-in tools for network management, including NetWatcher (shown in Figure 9). 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 or printer is in use. It allows disconnection of the user, and also maintains an event log of key system events, log on, log off, system boot and shutdown, failed attempts to connects, and so on.

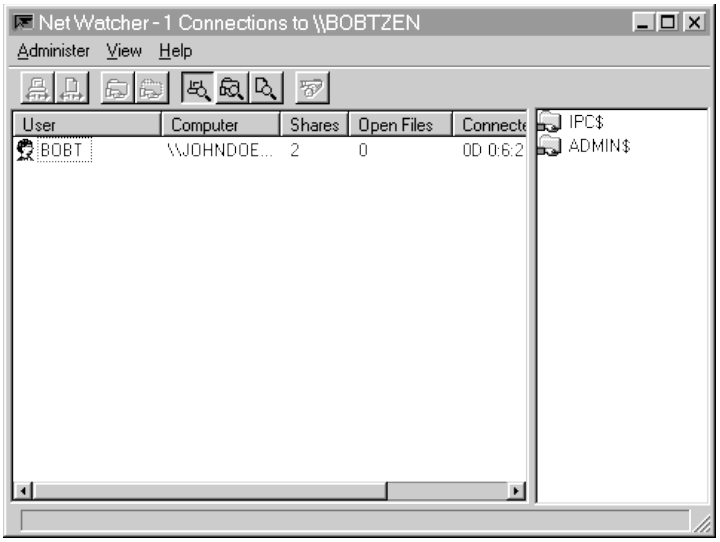

Figure 9. NetWatcher Supports Local and Remote Monitoring of File and Printer Sharing in Windows 95

Administrate File System

Additionally, Windows 95 includes the capability to access a special "administration share" of any capable Windows 95 PC. This allows the network manager to reconfigure the hard disk of a remote PC from his or her desktop. This feature is accessible via the property sheet for the PC from the Network Neighborhood view. Once activated, a window is opened that appears to be a normal browsing window. This is actually the remote machine's My Computer view, and all files and other resources are accessible remotely.

BLANK PAGE

IMPORTANT: This text will appear on screen, but will not print on a PostScript printer.

This page should be the last one in this file; it was inserted by running the InsertBlankPage macro.

Do not type any additional text on this page!