



WHITE PAPER

The When, What, Why, and How of Pre-OS

The When, What, Why, and How of Pre-OS

Contents

When Is Pre-OS?	2
What Can Be Done During Pre-OS?	2
Why Use Pre-OS?	4
Example 1: Workstation Computers	4
Example 2: University Computer Lab	4
How Is a Pre-OS Environment Set Up?	4
Conclusion	5

Acronyms and Abbreviations

BIOS
basic input/output system

DHCP
Dynamic Host Configuration Protocol

DOS
disk operating system

FTP
File Transfer Protocol

IPX
Internet Packet Exchange

NCP
NetWare Core Protocol

NIC
network interface card

OS
operating system

POST
power-on self-test

PXE
Preboot Execution Environment

ROM
read-only memory

RWU
Remote Wake Up

TCO
total cost of ownership

TCP/IP
Transmission Control Protocol/Internet Protocol

TFTP
Trivial File Transfer Protocol

WfM
Wired for Management

The When, What, Why, and How of Pre-OS

By Ron Brejak, Software Engineering Manager, Lanworks Technologies, 3Com Corporation

The issue of the high total cost of ownership (TCO) of PCs in a corporate environment is well understood by the IT community today. The main question now is: What is the best solution for the TCO problem? There are many products available that help address this issue, ranging from simple, low-cost, single-task “tools” to costly, complex, multiple-task client management products.

This paper discusses pre-OS (also referred to as “preboot”), which can be another weapon in the IT manager’s arsenal for tackling the TCO problem. Pre-OS is not a tool that performs specific tasks, but rather a framework that can be used to centrally deploy various client management tools. This paper addresses pre-OS as it pertains to network booting.

When Is Pre-OS?

As the name suggests, pre-OS occurs before the operating system (OS) is loaded. The primary distinctive aspect of pre-OS is the download of a boot image file from a boot server on the network, and the execution of this boot image on the client PC. To do this, the client PC must be equipped with network boot firmware, as described later in this paper.

Figure 1 shows a normal PC boot sequence without pre-OS. Figure 2 shows the PC boot sequence with legacy pre-OS capability. In legacy pre-OS environments, the PC normally reboots when the pre-OS phase is completed.

Figure 3 illustrates the sequence with enhanced pre-OS. In an enhanced pre-OS

environment, one of three actions can follow the pre-OS phase:

- 1 The PC can reboot, as is the case with a legacy pre-OS environment.
- 2 The PC can be shut down. This is useful when using Remote Wake Up (RWU) to perform pre-OS management tasks during off-hours.
- 3 The PC can continue booting using the OS installed on its hard disk, without rebooting. This option is the most distinctive feature of enhanced pre-OS. Products such as 3Com’s DynamicAccess[®] boot services and DynamicAccess managed PC boot agent support this enhanced functionality.

What Can Be Done During Pre-OS?

The boot image file that is downloaded and executed on the client PC determines what actions are performed during the pre-OS phase.

A boot image file is the consolidation of the contents of a regular boot diskette (or diskettes) into one file. Typically boot image files contain two sets of files. The first set are files necessary to boot a PC, such as a small OS. To minimize the size of the boot image file (thus minimizing its download time) and to minimize the amount of memory needed to store the boot image file, the OS used during a pre-OS session is typically a small, light-weight OS. DOS is the OS most commonly used during a pre-OS phase.

The second set of files are those needed to perform the desired tasks. This is where the power of pre-OS is unleashed. Programs, tools, utilities, and batch/script files can be included to perform a desired task on the client PC, as long as they are supported by the OS that is being used. The programs that are executed during the pre-OS phase are often called “pre-OS tasks.” Some of the common

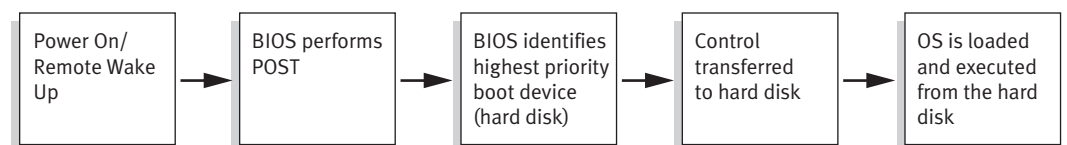


Figure 1. Normal PC Boot Sequence

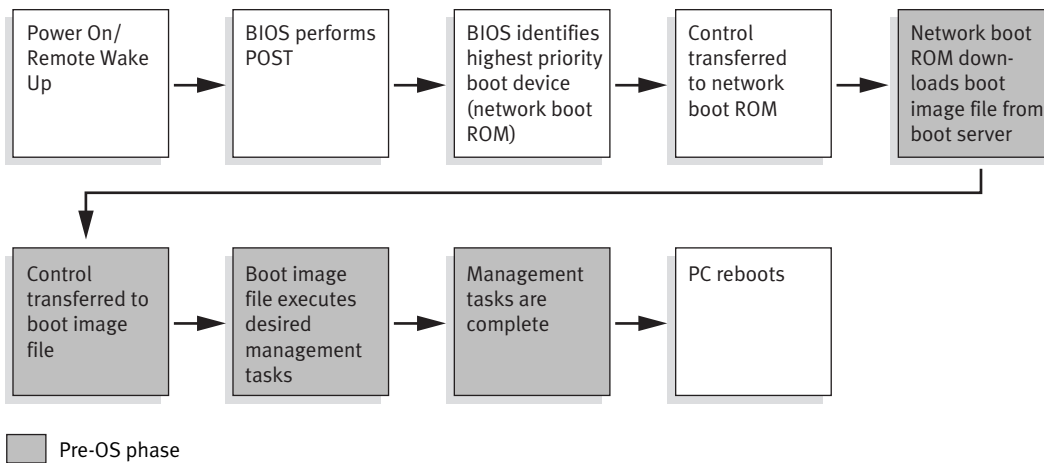


Figure 2. PC Boot Sequence with Legacy Pre-OS

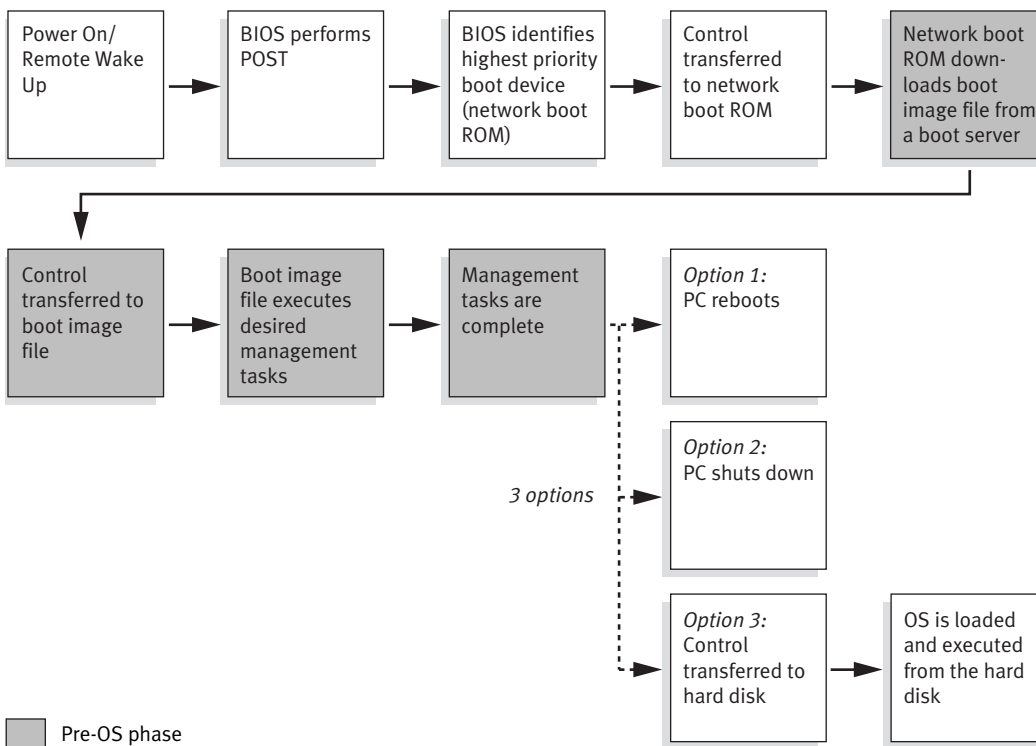


Figure 3. PC Boot Sequence with Enhanced Pre-OS

types of pre-OS tasks that are performed in a pre-OS session are:

- Hard disk imaging. There are many off-the-shelf drive imaging tools available today. They can be used to roll out OS installations and corporate desktops to client PCs.
- Virus scanning, especially of the boot sector.
- System updates, such as updating the client PC's BIOS to the latest version using a flash utility.
- Checking the existence and integrity of critical files.

There are two methods for executing pre-OS tasks:

- 1 Include all the files necessary to perform the pre-OS task in the boot image file. In this case, the files will be loaded into and executed from the client PC's memory.
- 2 Include only the files necessary to connect to and log into a file server where the pre-OS task files are located. Execute the task from the server.

Why Use Pre-OS?

Why bother doing a pre-OS session prior to booting the client PC's local OS? Let's look at two real-world examples where pre-OS would help.

Example 1: Workstation Computers

ACME, Inc. is a mid-sized company that produces gadgets. They have 400 employees, most of whom work in the manufacturing plant. One hundred workstation computers running Windows 98 are in use by various departments.

John is the systems manager. He is conscientious about virus prevention. Windows-based virus scanning software is installed on all computers and scheduled to run on a regular basis.

John has done a good job of preventing viruses from causing damage to ACME's computers. But has he gone far enough? What happens if a boot sector virus is introduced on one of the computers? Boot sector viruses are one of the most common types and are easily spread when floppy disks are exchanged. Also, what if a virus infects some of the Windows OS files so that the computers can't boot Windows? Since the virus scanning software that John is relying on is Windows-based, it doesn't have a chance to run before the Windows OS starts.

This is where pre-OS can help. John can set up a pre-OS environment in which a boot image file containing a DOS-based virus scanning tool is downloaded every time a computer is powered on. The virus scanner would scan for boot sector viruses and automatically eradicate any it found. Then the workstation

would continue to boot Windows normally from the hard disk.

Since this is done in a pre-OS scenario, the boot sector scan would be performed every time a computer is powered on and would require no intervention by the computer user. In addition, John could utilize pre-OS in conjunction with a RWU utility to wake up PCs in the company's off-hours and perform an exhaustive virus scan at a time when it would not disrupt business operations.

Example 2: University Computer Lab

Sue is a lab technician at a college. She is responsible for setting up and maintaining the computer labs that are used for various hands-on computer courses or for students to work on their assignments. The configurations of the various computers are often modified, sometimes intentionally and sometimes unintentionally. Students install software and change OS settings in ways that often cause problems for instructors and classes.

To solve this problem, Sue can set up a pre-OS environment in which, every time a computer is powered on, a pre-OS task is executed that examines the PC, compares it with a predetermined acceptable configuration, corrects or restores it if needed, and then seamlessly boots into the default, standardized desktop for that particular PC.

One minimalist scenario could have Sue's pre-OS tasks doing file comparisons on Windows-based system's critical files, including AUTOEXEC.BAT, CONFIG.SYS, SYSTEM.INI, and WIN.INI, as well as registry files SYSTEM.DAT, USER.DAT, and so on, and restoring them from the network-stored "safe" copies if a difference is detected. A more robust solution might include a workstation rebuild utilizing a third-party hard drive imaging utility that completely restores the PC. This would, again, boot seamlessly and immediately into a predetermined standardized desktop, with a total recovery time of a few minutes.

How Is a Pre-OS Environment Set Up?

The setup of a pre-OS environment varies depending on the network environment.

Three elements are needed to set up a pre-OS environment:

- 1 Client network boot firmware.** Network boot firmware must be available on the client PC. When a PC boots, this firmware will communicate with a network boot server to download the boot image file in the PC's memory and then execute the boot image. The firmware is usually located in an Option ROM on a network interface card (NIC) or integrated into the PC BIOS. There are various network boot protocols, but the specification that has become the industry standard is the Preboot Execution Environment (PXE) specification, which is part of the Wired for Management (WfM) specification. Most enterprise PCs purchased over the last two years typically have PXE firmware already included.
- 2 Network boot services.** Network boot services must be installed on a server that will act as the network boot server. This can be an existing server or a new server that is added to an existing network. When using the PXE network booting method, four services are usually required: Dynamic Host Configuration Protocol (DHCP), PXE, Proxy DHCP (when the PXE service is installed on a boot server separate from the DHCP server), and Trivial File Transfer Protocol (TFTP).

The DHCP service required is the usual one that issues IP addresses to the client PCs. Typically, most TCP/IP-based networks already have a DHCP service running. DHCP services are available with most network operating systems, including Windows NT and Windows 2000.

The Proxy DHCP service is needed to supply the PXE client with the IP address of

the PXE service. The service cannot run on the same server as the DHCP service. The PXE service supplies the PXE client with the filename of the boot image file to be downloaded. The TFTP service is a simple form of FTP. It is used to transfer the boot image file from the network boot server to the PXE client. The Proxy DHCP, PXE, and TFTP services may be available with some network operating systems or they can be purchased from third-party vendors.

- 3 Administrator tools.** Some miscellaneous tools are needed to do various tasks such as boot image file creation. There are products available that contain this functionality.

The components described above all pertain to a TCP/IP network. Pre-OS can also be set up on a NetWare NCP/IPX network. In this case, the client-based network boot firmware will not be PXE; it must support the IPX-based network boot protocols such as 802.2, 802.3, or Ethernet II. Such network boot ROMs are available.

Details on installation and configuration of network boot firmware, services, and tools are specific to vendor products. Refer to vendor documentation for instructions.

Conclusion

Pre-OS is a framework that can be used to centrally deploy various client management tools over a network. It allows DOS-based tools and utilities to be executed prior to the client's ultimate OS being loaded from the local hard disk. Setting up a pre-OS environment and executing client management tools, either on a regular basis with every boot or only when needed, can help reduce system maintenance costs and increase maintenance efficiency. ◻

Related References

3Com DynamicAccess boot services, www.3com.com/bootservices

3Com DynamicAccess managed PC boot agent, www.3com.com/products/dsheets/400350.html

Wired for Management, Preboot Execution Environment, <http://developer.intel.com/ial/wfm/>



3Com Corporation, Corporate Headquarters, 5400 Bayfront Plaza, Santa Clara, CA 95052-8145

To learn more about 3Com solutions, visit www.3com.com. 3Com Corporation is publicly traded on Nasdaq under the symbol COMS.

The information contained in this document represents the current view of 3Com Corporation on the issues discussed as of the date of publication. Because 3Com must respond to changing market conditions, this paper should not be interpreted to be a commitment on the part of 3Com, and 3Com cannot guarantee the accuracy of any information presented after the date of publication. This document is for informational purposes only; 3Com makes no warranties, express or implied, in this document.

Copyright © 2000 3Com Corporation. All rights reserved. 3Com and DynamicAccess are registered trademarks of 3Com Corporation. The 3Com logo is a trademark of 3Com Corporation. Windows and Windows NT are trademarks of Microsoft. IPX and NetWare are trademarks of Novell. All other company and product names may be trademarks of their respective companies.