



How to Use 3Com® DynamicAccess® Boot Services to Automate the Distribution of Software to Networked PCs Using Symantec's Norton Ghost



How to Use 3Com® DynamicAccess® Boot Services to Automate the Distribution of Software to Networked PCs Using Symantec's Norton Ghost

Introduction

As hardware prices continue to drop, IT managers are continually looking for less expensive ways to deploy PCs across the enterprise. Once all of the pieces are in place, administrators can perform a complete OS rollout without ever leaving their desk.

Intended Audience

Network Administrators, PC installers, and IT professionals.

Why use DynamicAccess Boot Services?

The use of 3Com® DynamicAccess® Boot Services (DABS) and 3Com Managed PC Boot Agent (MBA) with Symantec's Norton Ghost will help automate the use of Norton Ghost and consequently reduce the Total Cost of Ownership (TCO).

Time saved from the task of manual PC software installation and configuration means more time for IT staff to provide professional, high-level support.

This document will illustrate how to use *DynamicAccess* Boot Services and Managed PC Boot Agent in combination with Symantec's Norton Ghost to automate the distribution of software to networked PCs. Because DABS and MBA enable the client PCs to boot from the boot ROM, the need to visit each desktop with a Ghost boot disk is eliminated. Also, DABS eliminates the need to maintain multiple boot images on floppy disks, as one boot image is maintained on the server.

Introduction to 3Com DynamicAccess Boot Services

DynamicAccess Boot Services is a software package that includes TFTP, BOOTP, PXE services, a Boot Image Editor, and a BOOTPTAB editor that allows you to edit and manage boot image files and BOOTPTAB database files. *DynamicAccess* boot services is fully compatible with 3Com Managed PC Boot Agent, PXE boot ROMs, and Lanworks Bootware ROMs.

Introduction to Symantec's Norton Ghost

Symantec's Norton Ghost 6.0 Enterprise Edition was designed for IT managers in large organizations who expect more from a PC deployment and upgrade solution. Symantec's Norton Ghost 6.0 Enterprise Edition provides the technology for fast, reliable PC imaging and management to further reduce IT costs by providing a means to restore and configure machines that have been cloned. Symantec's Norton Ghost helps you:

- Dramatically reduce IT costs with PC recovery and deployment solutions.
- Restore failed PCs.
- Enjoy a PC cloning solution for disk image management, rollouts, and ongoing PC configuration.

This document will focus on using Symantec's Norton Ghost in conjunction with 3Com's DynamicAccess Boot Services and Managed PC Boot Agent to perform a workstation rollout.

3Com Managed PC Boot Agent and Norton Ghost

With MBA installed, or a PXE boot ROM, a client PC can boot from the network regardless of the contents of their local hard drives. MBA enables new and existing PCs to take advantage of pre-boot management technology to perform operating system and application installations or upgrades, as well as desktop disaster recovery.

Using MBA means that, at boot time, the client can connect to the DHCP/PXE or BOOTP Server and load a boot image file that contains the Ghost DOS Multicast Boot Disk.

What Will Be Needed

- 3Com *DynamicAccess* Boot Services
- Symantec's Norton Ghost Enterprise Edition v6.0
- PXE Boot ROM—3Com Managed PC Boot Agent, for example
- Remote wakeup and shutdown utilities (optional)

Hardware Environment Used in Following Examples

Role	PC	Processor	OS	HD	RAM	NIC
Server	Clone	Pentium II 233	NT Server 4.0 SP5	600 MB	32 MB	3C980
Source	HP Vectra	Pentium II 350	NT Workstation 4.0	10 GB	64 MB	3C905C
Target	Compaq DeskPro	Pentium 133	None	600 MB	32 MB	3C905C

Note: A 3Com OfficeConnect® 100 M hub is being used to network these machines.

A Step-by-Step Guide to Using 3Com DynamicAccess Boot Services with Norton Ghost

Installation of Symantec's Norton Ghost Enterprise 6.0

We installed Symantec's Norton Ghost on the root drive, c:\ghost, of the NT 4.0 Server.

Installation of DABS on the Server

1. Run setup.exe. You will then be presented with a license agreement.
2. After you accept the license, you will be prompted for an install location. Select the default directory, c:\programfiles\3Com\DynamicAccess Boot Services, for installation.
3. During the installation process for DABS, you will be prompted to choose between three options: Administrator, Custom, or Server. Install the Server setup to install all applications, services, utilities, and help documentation.
4. Create a directory on your c:\ drive called tftpboot. Copy the BOOTPTAB file (c:\program files\3Com\DynamicAccess Boot Services\Bootptab) into the c:\tftpboot directory.
5. Configure the PXE Service options to point to the location of the BOOTPTAB file, c:\tftpboot.

Implementation

At the Target machine:

1. We installed 3Com 3C905C NICs on the client PCs.
2. To create the initial image, copy ghost.exe (c:\ghost\ghost.exe) to a floppy and install the Norton Ghost Client on the source machine.

To start Symantec Norton Ghost:

From the DOS prompt, type C:\>ghost.exe.

3. Set up the Packet Driver Interface.
Follow the instructions in the Packet Driver Setup section of the Symantec Norton Ghost Enterprise Implementation Guide. The file is called ngcons.pdf. Ensure all files are installed on the disk. With most network interface card-dependent packet drivers, only one file, the packet driver, will have to be copied onto the disk. For example:

```
C:\> copy ne2000pd.com a:\
```

4. Edit the wattcp.cfg file. Copy wattcp.cfg to the floppy disk. The wattcp.cfg file stores the TCP/IP stack configuration details and specifies the IP address and sub-net mask for the machine.

Sample wattcp.cfg file:

```
IP = 192.168.100.44
```

```
NETMASK = 255.255.255.0
```

For a detailed description of the wattcp.cfg configuration file keywords, see the Norton Ghost Enterprise Implementation Guide, Appendix B, "The wattcp.cfg network configuration file." The file is called ngcons.pdf, and you can find it in the c:\ghost directory.

Creating the Initial Ghost Image

1. Insert a blank floppy disk into the a:\ drive of a Windows 9x or DOS machine.
2. Copy the system files onto the disk. Do one of the following:
 - 2.1. Within Windows 95/98:
 - 2.1.1 Double click the My Computer icon.
 - 2.1.2 Right click the floppy drive, and select Format.
 - 2.1.3 Choose Copy System Files.
 - 2.2 Within a DOS prompt box:
 - 2.2.1 Use the following DOS command to copy the system files to the formatted disk:
C:\> sys c: a:

2.2.2 Use the following DOS command to format and copy the system files to the unformatted disk:

```
C:\> format a: /s
```

2.2.3) Copy ghost.exe onto the boot disk. For example:

```
C:\> copy c:\ghost\ghost.exe a:\
```

3. Use the Norton Ghost Multicast Assist Wizard to create a Ghost Multicast DOS Boot Disk.

The Ghost Boot Disk contains the following files:

command.com	autoexec.bat	config.sys
drvspace.bin	io.sys	msdos.sys
ghost.err	ghost.exe	wattcp.cfg
dis_pkt.dos	el90x.dos	netbind.com
protman.dos	protman.exe	protocol.ini
ghstwalk.exe,	emm386.exe	himem.sys

Note: ghstwalk.exe, emm386.exe and himem.sys were manually added to the boot disk. Ghstwalk.exe was added to the boot disk so that Ghostwalker could be included in the batch file and be used to automate changing the client PC's computer names, passwords, and SIDs.

Using the Boot Image Editor to Make a Boot Image of the Norton DOS Boot Disk.

To eliminate the need to visit each client PC with the Norton Ghost Boot Disk, the Boot Image Editor can be used to create a boot image from the Norton Boot Disk and this single boot image can then be stored and maintained on a server.

To create the boot image:

1. Launch the Boot Image Editor (Start, Programs, DynamicAccess Boot Services, Boot Image Editor).
2. Select "Create a TCP/IP or PXE image file," see Figure .

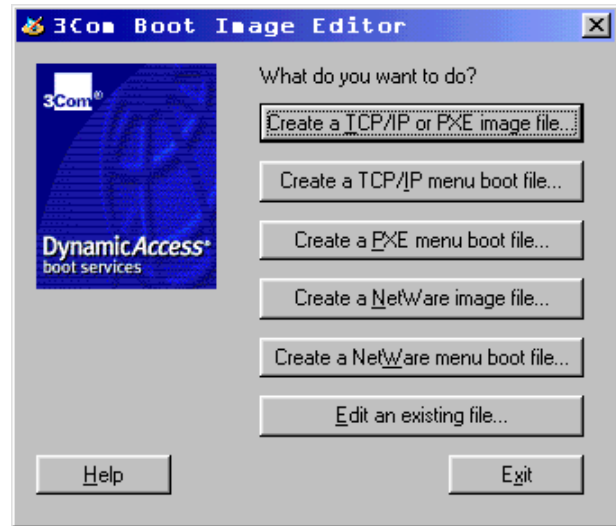


Figure 1: Boot Image Editor

3. Change the path to the tftpboot directory you created in step 3 (c:\tftpboot); see Figure 2.
 - 3.1 Name the image <filename>.sys; see Figure 2.
 - 3.2 Select extended capacity, the image needs to be 2 MB or larger to accommodate the ghostwalker utility; see Figure 2.
 - 3.3 Select Pre-OS Option; see Figure 2.
4. Put the Norton Ghost client boot diskette you created previously in Step 4 into the source drive, a:\.
5. Press "OK" to create the image; see Figure 2.



Figure 2: Create TCP/IP Image File Dialog Box

Creating the Source Ghost Image

4. Start a Multicast Session (Start, Programs, Norton Ghost, Multicast Server).
5. Enter a name in the “Session Name” field; see Figure 3.
6. Select “Dump From Client” to upload and create an image file from the source machine; see Figure 3.
7. Enter the full path of the disk image file in the Image File text box, or use the Browse button to find the destination location.

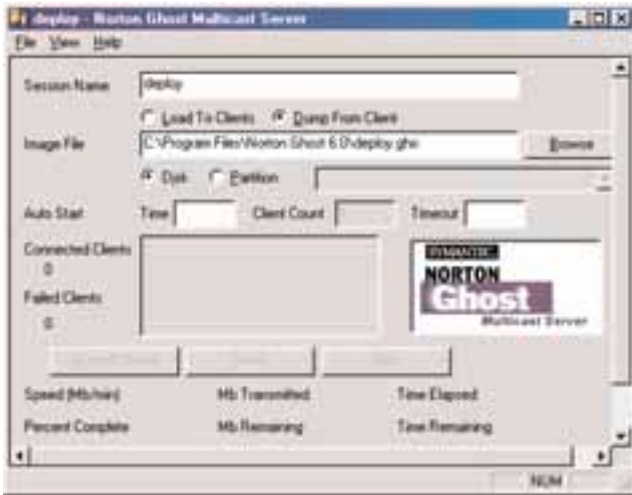


Figure 3: Norton Ghost Multicast Server Dialog Box

8. Click the “Accept Clients” button to accept the client machine(s) into the session. The image from the source machine will then be uploaded to the server.

Automating the Rollout

Now that the initial ghost image has been loaded from the source machine to the server, the rollout of the ghost image to the client PCs can be automated. To automate the rollout:

1. Edit config.sys:

Example of config.sys

REM /testmem:off is used to prevent the ramdrive from being corrupted

```
Device=himem.sys /testmem:off
Device=emm386.exe noems
Dos=high, umb
REM device loads the network drivers
```

```
Device=el90x.dos
Lastdrive=z
```

Edit autoexec.bat:

Example of autoexec.bat

```
@echo off
prompt $p$g
\net\netbind.com
cd \ghost
echo Loading...
```

REM launches the Norton Ghost Multicast Server and waits for the client to connect

```
ghost.exe -clone,mode=load,src=@MCDeploy,
dst=1 -sure -fx
```

REM add Ghostwalker here
REM shuts down the Multicast Server

```
\rmshtdown
```

Note: The Ghostwalker utility can be added to the autoexec.bat (line before \rmshtdown) to automatically change the client's computer name, password, permissions, and SID.

3. To automate the Norton Ghost Multicast Session, create a batch file that starts the multicast server and starts the download. Here is an example of such a batch file “deploy.cmd:”

```
Deploy.cmd
@echo off
@echo starting Norton Ghost multicast server
```

REM launches the Norton Ghost Multicast Server and waits for the client to connect

```
c:\ghost\ghostsrv c:\ghost\deploy.gho DEPLOY -n1 -ls
-fe:\ghost.log -c
@echo All Done
```

For a complete list and explanation of Norton Ghost command-line switches, see the Norton Ghost Enterprise Implementation Guide, Appendix A. The file is called ngcons.pdf, and you can find it in the c:\ghost directory.

4. Follow Boot Method 1, 2, or 3.

Boot Method 1: Using DynamicAccess Boot Services' BOOTP with Symantec's Norton Ghost

At the Server:

5. Run the batch file (e.g. “deploy.cmd”).
6. Start the TFTP service.
7. Start the BOOTP service.

At the client:

1. Turn on the client, either manually or this could be done at the server by remote wakeup if the client has remote wakeup capability.
2. Configure MBA with either the MBACFG.EXE utility found on the MBA Utility Disk or by pressing CTRL+ALT+B on startup. Configure MBA to boot TCP/IP, BOOTP.

At the server:

1. In the BOOTP application window, the client PC's MAC address will be displayed followed by a "not found" comment. This is because the client has not been added to the BOOTPTAB file. To add the client to the BOOTPTAB file:

1.1 Right click the "not found" line; see Figure 4.

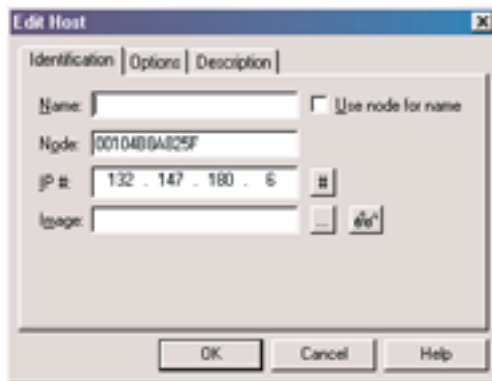


Figure 6: Edit Host Dialog Box to Add BOOTP Client to BOOTPTAB File

Boot Method 2: Using DynamicAccess Boot Services' PXE with Symantec's Norton Ghost

At the Client:

1. Configure MBA with either the MBACFG.EXE utility found on the MBA Utility Disk or by pressing CTRL+ALT+B on startup to boot using the PXE boot method.

At the Server:

2. Use the Boot Image Editor to create a PXE menu boot file.

2.1 Select "Create a PXE menu boot file," see Figure 7.

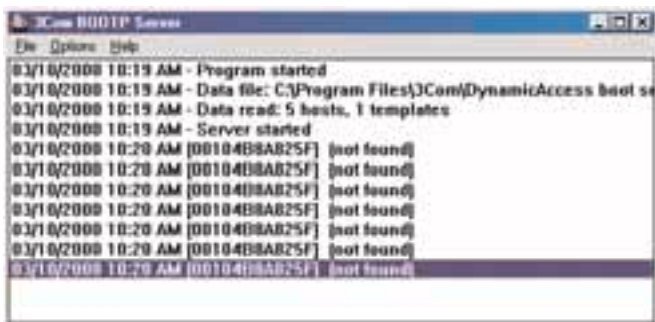


Figure 4: BOOTP Server Application Dialog Box

1.2 Select "edit BOOTPTAB" and the Edit Host dialog box will appear; see Figure 5.

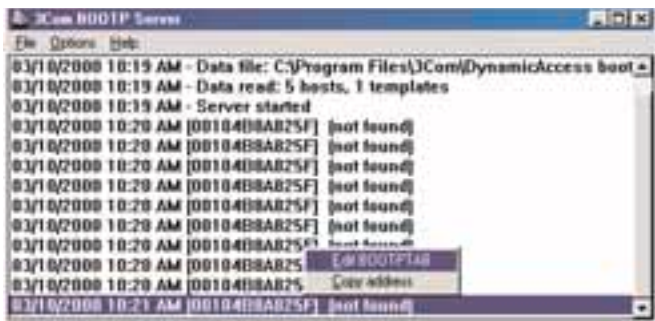


Figure 5: Adding a "not found" Client to the BOOTPTAB File

- 1.3 The client's MAC address is already filled in. Enter a name and an IP address; see Figure 6.
- 1.4 Use the Browse button (...) to find the image <filename>.sys; see Figure 6.

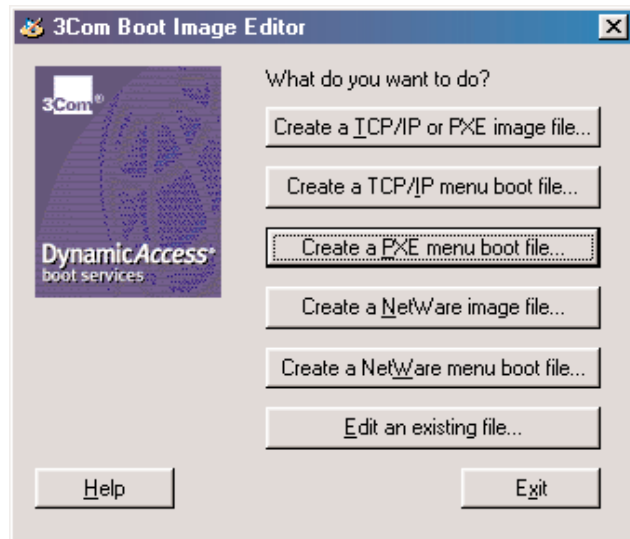


Figure 7: Using Boot Image Editor to Create a PXE Menu Boot File

2.2 Select “Add,” see Figure 8.

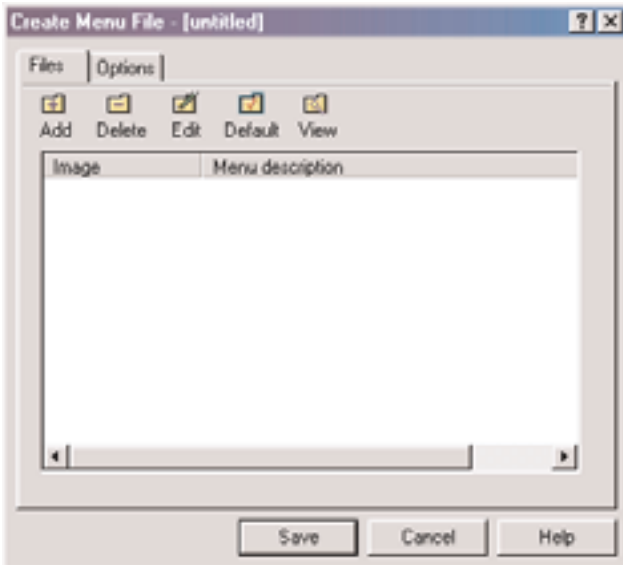


Figure 8: Create Menu File Dialog Box

2.3 Browse for the image file <filename>.sys, press “Open,” see Figure 9.

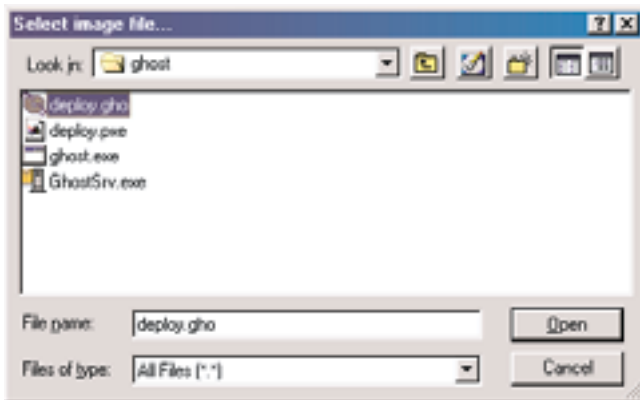


Figure 9: Selecting the Image File

2.4 Enter a menu description if desired, and click on “OK,” see Figure 10.



Figure 10: Edit Entry Dialog Box

2.5 Select “Save,” see Figure 11.

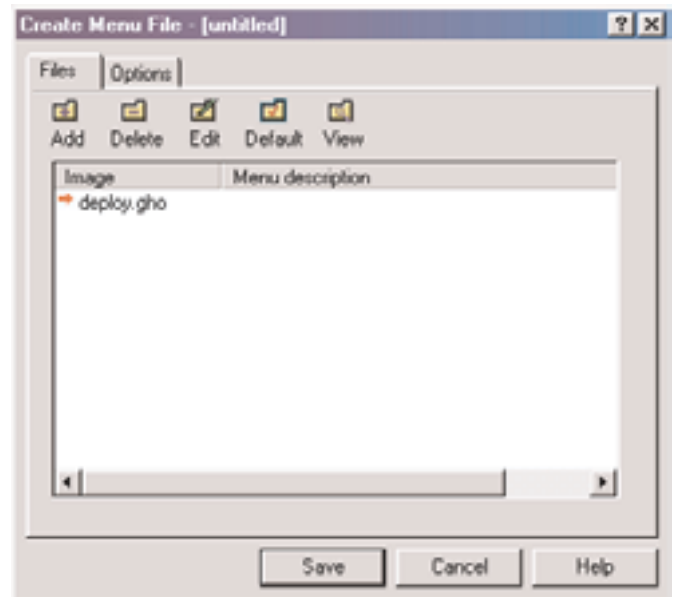


Figure 11: Create Menu File Dialog Box

2.6 Select a file name, <filename>.pxe, click on “Save,” and exit. See figure 12.

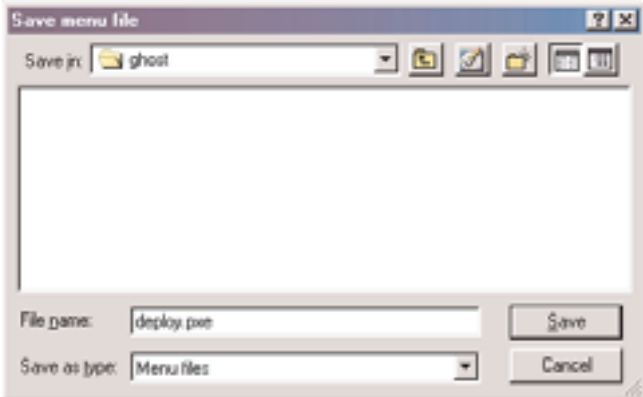


Figure 12: Save Menu File Dialog Box

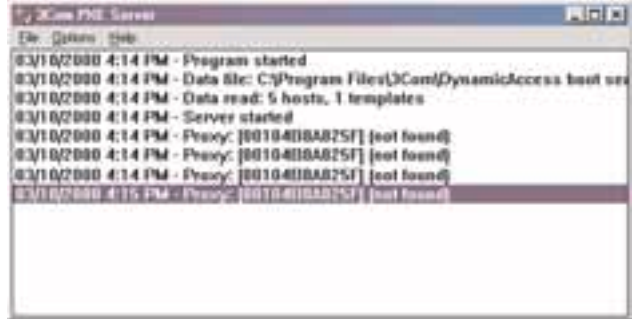


Figure 14: PXE Server Application Dialog Box

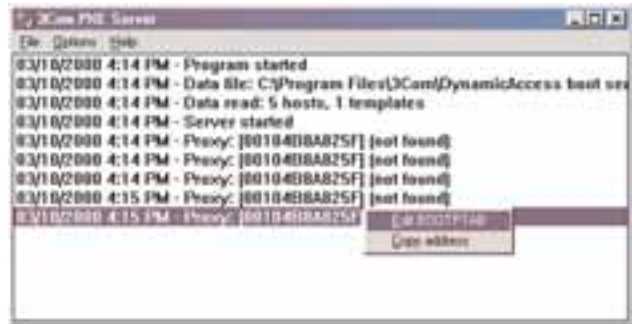


Figure 15: Adding a "Not Found" Entry into the BOOTPTAB File

- If the client has already been entered into the BOOTPTAB file, launch the BOOTPTAB Editor and double click the client. Edit the image file path to point to the <filename>.pxe image you just created. See Figure 13.

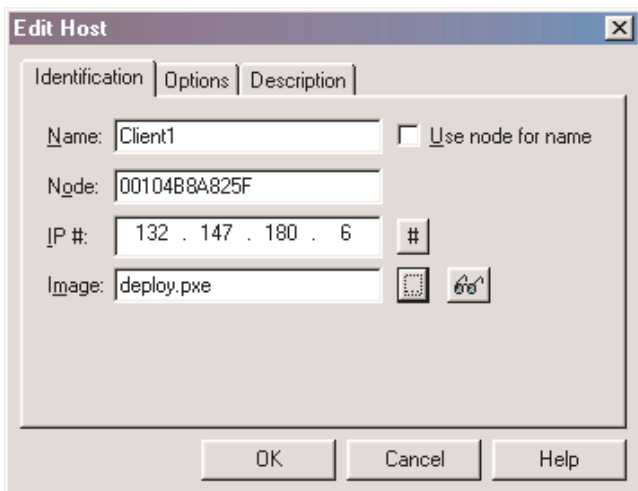


Figure 13: Edit Host in BOOTPTAB Editor to Edit Image Path

- Press "OK" to save the BOOTPTAB File.
- Start the TFTP and PXE services.
- If the client has not been added to the BOOTPTAB File, right click on the "not found" entry in the PXE Server; see Figures 14 and 15.

- Add the client's name and edit the image file path to point to the <filename>.pxe image you just created. See Figures 16 and 13.



Figure 16: Edit Host Dialog Box

- Start the Microsoft DHCP server. If the DHCP server is on a different machine, enable Proxy DHCP when prompted.
- Run your batch file (e.g. "deploy.cmd").
- Start the client either manually or by using a remote wakeup utility.

Boot Method 3: Using DynamicAccess Boot Services and DHCP with Symantec's Norton Ghost

At the Client:

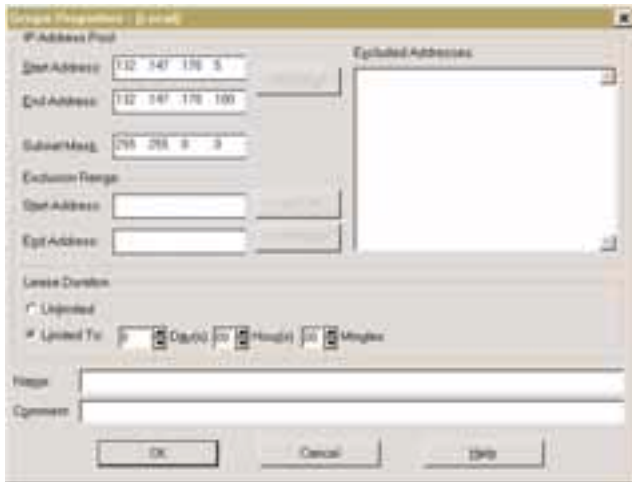
1. Configure MBA with either MBACFG.EXE utility found on the MBA Utility Disk or by pressing CTRL+ALT+B on startup to boot TCP/IP, DHCP.

At the Server

1. Install DHCP Server, assign the server an IP address, and in DHCP Manager, create a scope of IP addresses.

Creating new scope for DHCP server

- Click "Start" on the Windows taskbar and select the "Programs" menu.
- Select "Administrative Tools (Common)" and "DHCP Manager."
- Select the server for which a DHCP scope is to be created in the "DHCP Servers" list box. Select the "Scope" menu and select "Create." (The "Create Scope" dialog box appears.) In the "Start Address" and "End Address" boxes, type the beginning and ending IP addresses for the available range of addresses defined by this scope.



Note: DHCP Manager automatically enters a proposed sub-net mask value in the "Subnet Mask" box based on the values entered in the "Start Address" and "End Address" boxes. Accept the proposed value unless a different value is required.

- (Optional) To exclude IP addresses from the scope range, do one of the following:
 - a. To exclude a range of IP addresses from the DHCP scope address range:

1. In the "Start Address" box of the "Exclusion Range" group, type the first IP address that is part of the excluded range.
 2. In the "End Address" box of the "Exclusion Range" group, type the last IP address that is part of the excluded range.
 3. Click "Add."
- Select the "Limited To" radio-button, and enter the appropriate values in the "Day(s)," "Hour(s)," and "Minutes" text boxes.
 - If you do not want IP addresses in the scope to expire, select the "Unlimited" radio-button.
 - Type a name for the scope in the "Name" box.
 - (Optional) Type a description of the scope in the "Comment" box.
 - Click "OK." (A message appears stating that the scope has not been activated, with an option to activate the scope immediately.)
2. Start the Microsoft DHCP Server and TFTP service.
 3. Run your batch file (e.g. "deploy.cmd").
 4. Start the client either manually or by using a remote wakeup utility.

Conclusion

3Com Managed PC Boot Agent, or any PXE ROM, guarantees that new PCs on the network with no OS and unformatted hard drives will connect to the network. Using DABS and MBA in combination with Symantec's Norton Ghost to perform an automated rollout greatly reduces TCO by compressing new-hire setup, reducing downtime due to PC problems, and accelerating upgrades to the latest PC technologies and applications.

References

Norton Ghost Enterprise Implementation Guide

3Com Managed PC Boot Agent User Guide

3Com DynamicAccess Boot Services User Guide

**3Com Corporation**

P.O. Box 58145
5400 Bayfront Plaza
Santa Clara, CA
95052-8145
Phone: 1 800 NET 3Com
or 1 408 326 5000
Fax: 1 408 326 5001
World Wide Web:
www.3com.com

Asia Pacific Rim

Sydney, Australia
Phone: 61 2 9937 5000
Fax: 61 2 9956 6247
Melbourne, Australia
Phone: 61 3 9866 8022
Fax: 61 3 9866 8219
Beijing, China
Phone: 86 10 68492 568
Fax: 86 10 68492 789
Shanghai, China
Phone: 86 21 6350 1581
Fax: 86 21 6350 1531
Hong Kong
Phone: 852 2501 1111
Fax: 852 2537 1149
India
Phone: 91 11 644 3974
Fax: 91 11 623 3192
Indonesia
Phone: 62 21 572 2088
Fax: 62 21 572 2089
Osaka, Japan
Phone: 81 6 536 3303
Fax: 81 6 536 3304
Tokyo, Japan
Phone: 81 3 3345 7251
Fax: 81 3 3345 7261
Korea
Phone: 82 2 3455 6300
Fax: 82 2 319 4710
Malaysia
Phone: 60 3 715 1333
Fax: 60 3 715 2333
New Zealand
Phone: 64 9 366 9138
Fax: 64 9 366 9139
Philippines
Phone: 632 892 4476
Fax: 632 811 5493
Singapore

Phone: 65 538 9368
Fax: 65 538 9369
Taiwan
Phone: 886 2 2 377 5850
Fax: 886 2 2 377 5860
Thailand
Phone: 662 231 8151 5
Fax: 662 231 8158

3Com Austria

Phone: 43 1 580 17 0
Fax: 43 1 580 17 20

3Com Benelux B.V.

Belgium
Phone: 32 2 725 0202
Fax: 32 2 720 1211
Netherlands
Phone: 31 346 58 62 11
Fax: 31 346 58 62 22

3Com Canada

Calgary
Phone: 1 403 265 3266
Fax: 1 403 265 3268
Edmonton
Phone: 1 403 423 3266
Fax: 1 403 423 2368
Montreal
Phone: 1 514 683 3266
Fax: 1 514 683 5122
Ottawa
Phone: 1 613 566 7055
Fax: 1 613 233 9527
Toronto
Phone: 1 416 498 3266
Fax: 1 416 498 1262
Vancouver
Phone: 1 604 434 3266
Fax: 1 604 434 3264

3Com Eastern Europe/CIS

Bulgaria
Phone: 359 2 962 5222
Fax: 359 2 962 4322
Czech/Slovak Republics
Phone: 420 2 21845 800
Fax: 420 2 21845 811
Hungary
Phone: 36 1 250 8341
Fax: 36 1 250 8347
Poland
Phone: 48 22 6451351
Fax: 48 22 6451352

Russia

Phone: 7 095 258 09 40
Fax: 7 095 258 09 41

3Com France

Phone: 33 1 69 86 68 00
Fax: 33 1 69 07 11 54
Carrier and Client Access
Phone: 33 1 41 97 46 00
Fax: 33 1 49 07 03 43

3Com GmbH

Berlin, Germany
Phone: 49 30 3498790
Fax: 49 30 34987999
Munich, Germany
Phone: 49 89 627320
Fax: 49 89 62732233

3Com Iberia

Portugal
Phone: 351 1 3404505
Fax: 351 1 3404575
Spain
Phone: 34 1 509 69 00
Fax: 34 1 307 79 82

3Com Latin America

U.S. Headquarters
Phone: 1 408 326 2093
Fax: 1 408 764 5730
Miami, Florida
Phone: 1 305 261 3266
Fax: 1 305 261 4901
Argentina
Phone: 54 1 312 3266
Fax: 54 1 314 3329
Brazil
Phone: 55 11 246 5001
Fax: 55 11 246 3444
Chile (also serving Bolivia and Peru)
Phone: 56 2 633 9242
Fax: 56 2 633 8935
Colombia
Phone: 57 1 629 4847
Fax: 57 1 629 4503
Mexico
Phone: 52 5 520 7841/7847
Fax: 52 5 520 7837
Peru
Phone: 51 1 221 5399
Fax: 51 1 221 5499
Venezuela
Phone: 58 2 953 8122
Fax: 58 2 953 9686

3Com Mediterraneo

Milan, Italy
Phone: 39 2 253011
Fax: 39 2 27304244
Rome, Italy
Phone: 39 6 5279941
Fax: 39 6 52799423

3Com Middle East

Phone: 971 4 319533
Fax: 971 4 316766

3Com Nordic AB

Denmark
Phone: 45 48 10 50 00
Fax: 45 48 10 50 50
Finland
Phone: 358 9 435 420 67
Fax: 358 9 455 51 66
Norway
Phone: 47 22 58 47 00
Fax: 47 22 58 47 01
Sweden
Phone: 46 8 587 05 600
Fax: 46 8 587 05 601

3Com Southern Africa

Phone: 27 11 807 4397
Fax: 27 11 803 7405

3Com Switzerland

Phone: 41 844 833 933
Fax: 41 844 833 934

3Com UK Ltd.

Edinburgh
Phone: 44 131 240 2900
Fax: 44 131 240 2903
Ireland
Phone: 353 1 820 7077
Fax: 353 1 820 7101
Manchester
Phone: 44 161 873 7717
Fax: 44 161 873 8053
Marlow
Phone: 44 1628 897000
Fax: 44 1628 897003

To learn more about 3Com products and services, visit our Web site at www.3com.com/. 3Com Corporation is publicly traded on NASDAQ under the symbol COMS.

Copyright © 2000 3Com Corporation. All rights reserved. 3Com, the 3Com logo, DynamicAccess, and OfficeConnect are registered trademarks of 3Com Corporation. DOS, Windows, and Windows NT are registered trademarks of Microsoft Corporation. Other product and brand names may be trademarks or registered trademarks of their respective owners. All specifications are subject to change without notice.

Printed in U.S.A.

000000-001 5/00