



3Com® DynamicAccess® Boot Services (DABS) and Virus Scanning



3Com® DynamicAccess® Boot Services (DABS) and Virus Scanning

Who should read this paper?

This paper is for system administrators who intend to use 3Com® DynamicAccess® boot services (DABS) to conduct centralized virus scanning in a pre-OS environment. This paper explains the advantage of running virus scans in pre-OS environments, gives step-by-step instructions, and provides sample files.

Introduction

Using 3Com DABS to perform centralized virus scanning can reduce the Total Cost of Ownership (TCO) tremendously. Computer viruses can be spread widely over the network and Internet and are more destructive than ever before. Cleaning the viruses and recovering infected systems can cost lots of time and money. It is not feasible in a corporate environment for a system administrator to visit every computer to scan/clean the virus or upgrade the virus scanning software.

3Com DABS provides a virus-scanning solution to reduce TCO. With 3Com DABS, the administrator can conduct the virus scanning centrally, during off-hours, if combined with a Remote Wake-Up (RWU) utility, or scheduled as desired (daily, weekly, monthly, or at specified time).

Pre-OS vs. Login Script

System administrators can embed virus scanning commands into system login scripts, so that when the client PC boots up and logs into the server, the virus scanning commands will be executed. However, if the client PC is infected and encounters difficulties in connecting to the server or cannot even boot locally, login script-driven virus scanning will be ineffective. With 3Com DynamicAccess managed PC boot agent (MBA), or any other PXE boot ROM installed, the client PC can always connect to the server when it boots up, download an executable boot image, which is assigned by the system administrator, and execute it prior to loading the local operating system. The system administrator can embed the virus scanning commands into the boot image, so the client PC can perform the virus scanning even when the PC cannot connect to the server.

Requirements

Client PCs:

- Networked client PCs with 3Com MBA v3.0 or greater, or any other Preboot eXecution Environment (PXE)-compatible boot ROM, installed.
- With MBA, the Boot Method can be set to PXE, BOOTP, or DHCP. In the example below, PXE is selected.
- The client PCs should be compliant with Wired for Management (WfM) v2.0 specifications. For PCs that are not fully WfM 2.0-compliant, they should at least have the wake-on LAN (WOL) ability and have proper power management (APM or ACPI).
- If the PC does not follow PCI specification v2.1 or higher, a WOL cable is needed to connect the network interface card (NIC) and the WOL socket on the PC's motherboard.

Server:

- Microsoft Windows NT 4.0 server with Service Pack 4 or above, or Windows 2000 server.
- A DHCP server (such as Microsoft DHCP Server).
- 3Com DABS—3Com PXE Server, 3Com TFTP Server, 3Com BOOTPTAB Editor, and 3Com Boot Image Editor.
- A DOS-based virus scanning software (such as F-Secure (formerly DataFellows) F-PROT.EXE¹).
- Remote wake-up utility (such as IBM Winwake.exe).

Server Configuration:

1. Install 3Com DABS on the server (please refer to the 3Com DynamicAccess boot services Quick Start Guide for installation information).
2. Configure and start the Microsoft DHCP server. If the DHCP server is running on the same machine as that of 3Com DABS, the option tag 060 of DHCP server needs to be configured.
 - 2.1 On the Windows NT server, click Start → Programs → Administrative Tools → DHCP Manager.
 - 2.2 The “DHCP Manager” window appears. Double click the “Local Machine” displayed on the left panel—DHCP Servers—of the window and select the scope that will be used.

- 2.3 Select from the menu: DHCP Options → Defaults.... The **“DHCP Options: Default Values”** window appears.
- 2.4 Click on the “New...” button. When the **“Add Option Type”** window pops up, type in “ClassID” in the “Name” input box, select “String” as “Data Type,” leave “Array” unchecked, input “60” in the “Identifier” box. (The “Comment” is optional.) Then click “OK.”
- 2.5 From the **“DHCP Options: Default Values”** window, select “060 ClassID” that was just created. From “Option Name” list, type in “PXEClient” as the “Value,” then click “OK.”
- 2.6 Assign the option to the DHCP scope. From the **“DHCP Manager”** window, select from the menu DHCP Options → Scope.... When the **“DHCP Options: Scope”** window appears, select “060 ClassID” from “Unused Options” on the left panel of the window, click on “Add.” “060 ClassID” should be displayed in the “Active Options” list on the right panel of the window. Then click on “OK.”

Note: If the DHCP server is running on a different machine, this PXE option should not be assigned.

3. Start the 3Com PXE Server (the 3Com BOOTP Server may be used in place of the 3Com PXE Server; however, in this document PXE protocol is selected for the example) and the 3Com TFTP server.
 - 3.1 On the Windows NT server, click Start → Settings → Control Panel.
 - 3.2 Double click on the “Services” icon in Control Panel window.
 - 3.3 When the **“Services”** window displays, select “3Com PXE Server” and press “Start.”
 - 3.4 Select “3Com TFTP Server” and then press “Start.”
 - 3.5 If the DHCP server is running on a different server, the 3Com Proxy DHCP Server should be enabled from the 3Com PXE Server. From the **“Control Panel”** window, double click on the “3Com PXE Server” icon, check “Proxy DHCP” from “Options” tab.
4. Create a Virus Scanning Boot Image by using the 3Com Boot Image Editor that comes with DABS.
 - 4.1 Make a DOS-bootable floppy diskette.

- 4.2 Make the DOS-bootable floppy a DOS client of Windows NT. Use the “Network Client Administrator” of Windows NT. Select the network interface card (NIC) being used, or, if the specific NIC is not on the list, select the one most similar. Select “NetBEUI” as the protocol. Please refer to Microsoft Windows NT Server documentation for further information.
- 4.3 Modify the PROTOCOL.INI and SYSTEM.INI file to use universal NDIS 2.0 driver². The PROTOCOL.INI and SYSTEM.INI files are located in the subdirectory \NET of the bootable DOS-client floppy. Modify them following the examples in Appendix D, Sample Network Files. The universal NDIS 2.0 driver (NDIS.DOS file in the example) can be found at Intel’s Web site².
- 4.4 Copy the DOS-based virus scanning utility (F-PROT.EXE¹) onto the floppy. All other relevant files that are needed by F-PROT.EXE, such as virus definition files (.DEF), will not fit into a single 1.44 MB floppy diskette. Leave them on the server, such as C:\Download\AntiVirus\F-PROT\ subdirectory. These files will be added into the boot image later, as shown in section 4.7. The DOS version of F-PROT is a shareware, free of charge for non-commercial use. The latest version of the software can be anonymously downloaded from <ftp://ftp.europe.datafellows.com/anti-virus/free/>.
- 4.5 Label the floppy as VIRUSCAN. The floppy should have the following directory structure and files:

Volume in drive A is VIRUSCAN
Volume Serial Number is 392B-18F1
Directory of A:\

NET	<DIR>	09-18-99	12:00a
AUTOEXEC	BAT	989 04-01-99	1:07a
COMMAND	COM	54,645 05-31-94	6:22a
CONFIG	SYS	128 04-05-99	6:39a
DOSKEY	COM	5,861 05-30-94	9:22p
DRVSPACE	BIN	64,135 07-14-95	12:00a
HIMEM	SYS	33,191 05-11-98	3:01p
IFSHLP	SYS	4,644 08-08-96	3:00p
F-PROT	EXE	278,767 02-29-00	1:05a
ENGLISH	TX0	19,241 02-15-00	9:58a
REBOOT	COM	14 08-13-98	2:14p
SHUTDOWN	COM	44 10-13-99	6:41a
WAIT	EXE	43,962 05-04-99	11:22a
12 file(s)		505,621 bytes	

```

Directory of A:\NET
NDIS          DOS    27,056 09-01-99  4:39a
NDISHLP       SYS    4,468 10-13-96  4:38p
NET           EXE   450,342 10-13-96  4:38p
NET           MSG   74,016 11-11-95  7:57a
PROTMAN       DOS   21,940 10-13-96  4:38p
PROTMAN       EXE   13,782 10-13-96  4:38p
PROTOCOL      INI    523 08-10-98  7:31a
SHARES        PWL    622 04-05-99  6:44a
SYSTEM        INI    471 04-05-99  6:44a
WCSETUP       INF   1,477 10-13-96  4:38p
WFWSYS        CFG    840 10-13-96  4:38p
11 file(s)    595,537 bytes
297,872 bytes free

```

Edit CONFIG.SYS, AUTOEXEC.BAT, PROTOCOL.INI, and SYSTEM.INI files to make sure the floppy boots up, connects to the server, scans all the client PC's hard drives, then logs the reports on the server. See the sample files in Appendix C.

- 4.6 Create the boot image using 3Com Boot Image Editor. Insert the VIRUSCAN diskette into the floppy drive (for example, drive A:) on the Windows NT server, and start the “**3Com Boot Image Editor**.” See Figure 1 below.

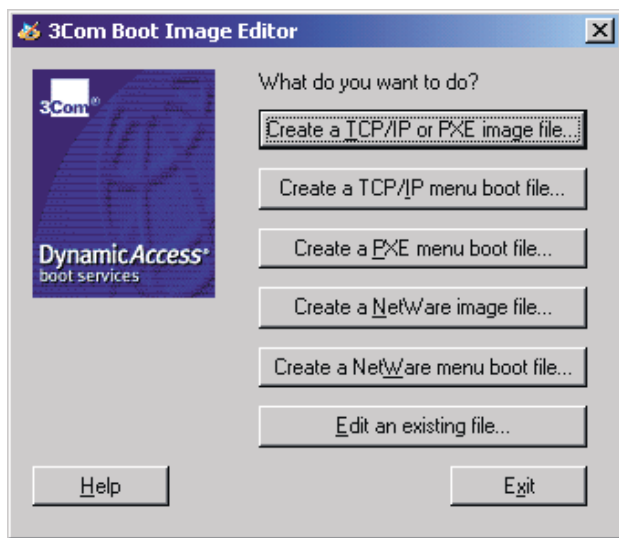


Figure 1: 3Com Boot Image Editor window

- Select “Create a TCP/IP or PXE image file...”
- In the “**Create TCP/IP Image File**” dialogue box (see Figure 2), input the path and file name of the boot image file (for example, C:\TFTPBOOT\VIRUSCAN.IMG).
- Choose the “Source Drive” (usually A:).

- Select “Extended capacity” to “4 MB.”
- Under “Options,” check “Writeable,” and “Pre-OS” boxes.
- Click “Advanced...,” and check “Keep UNDI in memory” in “**Advanced Options**” dialogue box, then click “OK.”
- Click “OK” to create the boot image.

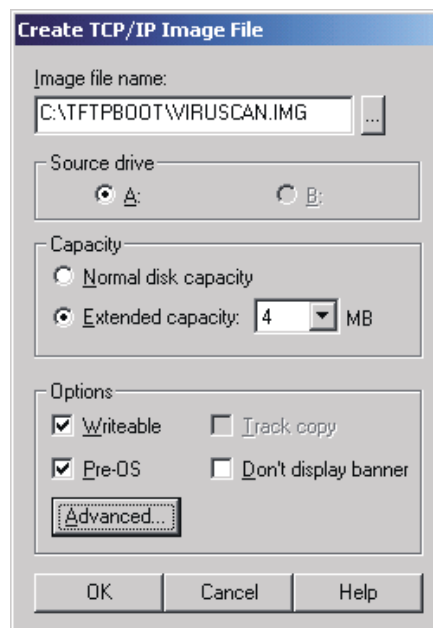


Figure 2: Create TCP/IP Image File

- 4.7 Add the virus definition files into the boot image. From the “**3Com Boot Image Editor**” main menu (Figure 1), select “Editing an existing file...” When the “Open” dialogue box appears, select the boot image file (VIRUSCAN.IMG) that was created in step 4.6 and click “Open.” The “View Image File” window is displayed, as shown in Figure 3.

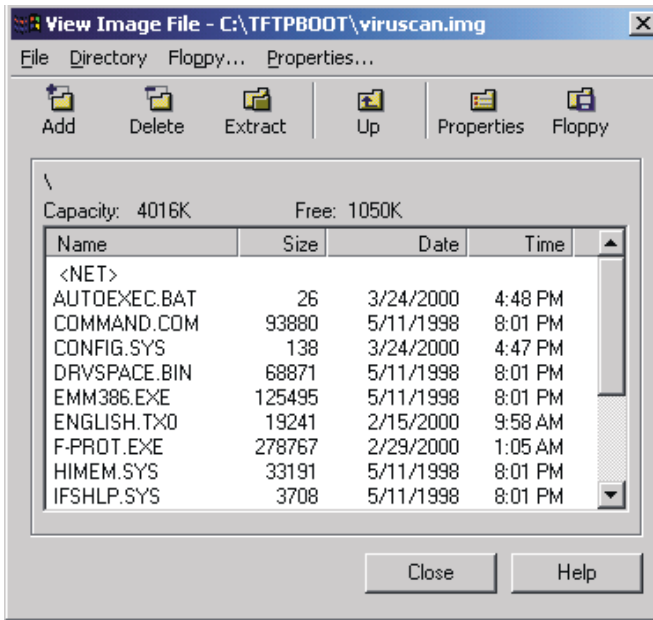



Figure 3: View Image File

Click on  to open an “Add file to image...” window. Go to the directory where the virus definition files are stored, for example, C:\Download\AntiVirus\F-PROT. Select the following files that should be added into the boot image, SIGN.DEF, SIGN2.DEF, MACRO.DEF, AND NONMACRO.DEF, and then click “Open.” Multiple files can be added into the boot image file at once by pressing and holding “Ctrl” key while clicking on the file names to select multiple files.

5. Add the Virus Scanning Boot Image to PXE menu boot file. Start the 3Com Boot Image Editor again and select “Create a PXE menu boot file...” The “**Create Menu File**” window appears (see Figure 4).

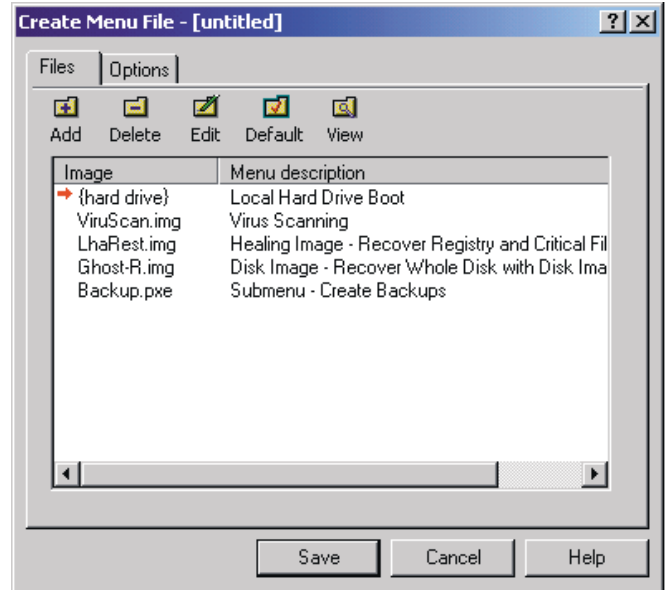



Figure 4: Create Menu File

Click on  to add a boot image into the menu (see Figure 5). Select or input the Image file name and enter descriptive text into “Menu description” input box. More than one boot image and Local Hard Drive Boot can be added into the menu boot file. Repeat until all needed boot images are added to the menu. Click “Save” and give a name to this menu boot file, for example, DABS.pxe.

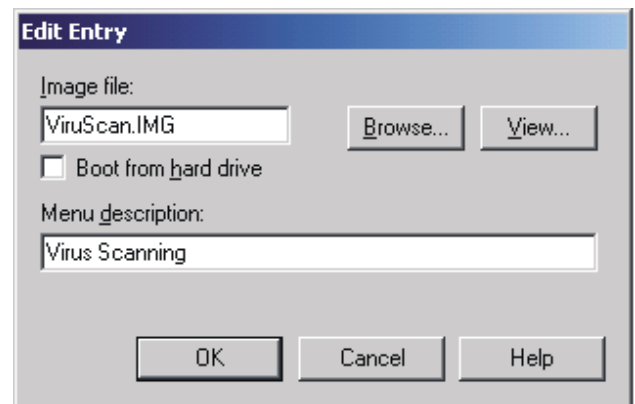


Figure 5: Edit Entry

6. Create/Edit a BOOTPTAB file, including MAC addresses of all client PCs, by using BOOTPTAB Editor that comes with DABS. On the Windows NT server, start the 3Com BOOTPTAB Editor. A window similar to Figure 6 will be displayed.

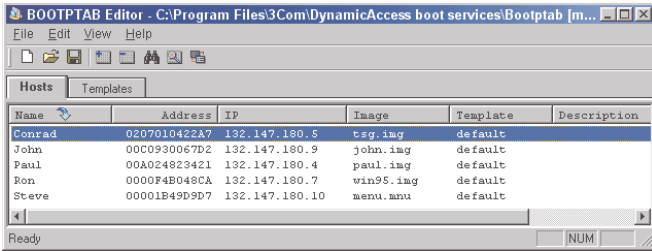



Figure 6: BOOTPTAB Editor

- 6.1 Set the Preferences. Select from Edit → Preferences..., and check “PXE” as the “Application” in “Preferences” window.
- 6.2 Click on the  button to add a host to the BOOTPTAB file. Input the Name and Node (MAC address) of the client, and select a boot Image for the client. (See Figure 7.) Select “default” Template from Options tab, and enter some descriptive text in Description tab (optional).

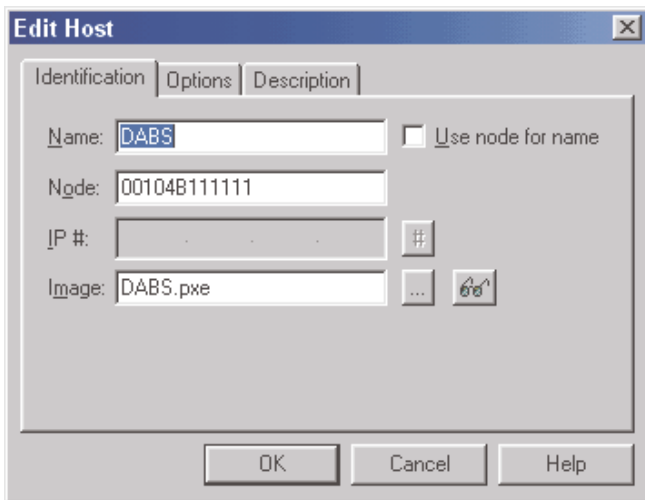


Figure 7: Add Host

- 6.3 Repeat step 6.2 to add all clients to BOOTPTAB file and assign appropriate menu boot files to them.

How to conduct an off-hours centralized virus scanning

1. Create a wakeup list that contains all the MAC addresses (or IP addresses, depending on which RWU utility has been used) of the client machines that are supposed to be scanned.
2. Make the virus-scanning image the default boot entry in the PXE boot menu file by using 3Com Boot Image Editor.
3. Run the RWU utility at any convenient time that the system administrator chooses, or schedule it with a task schedule utility (such as Microsoft Windows Task

Scheduler) at any appropriate time (such as after-hours, or 2:00 a.m.). The RWU utility on the server uses Magic Packets to wake up the client PCs for scanning.

4. The client PCs download a PXE bootstrap file (the PXE menu boot file), in which the virus scanning boot image is set to default.
5. The client PCs download the virus scanning boot image from the server and run the boot image.
6. The commands in the boot image check the client PCs for viruses, log the reports, and finally, shut down the PCs.

Virus scanning can be done by a system administrator without any client intervention at all. If any new virus patterns are introduced, the administrator just needs to upgrade the virus scanning utility or virus patterns, or signature definition files on the server (contained with the boot image file, in this example).

Appendix: Samples Files:

A. Sample BOOTPTAB file

```
# Sample BOOTPTAB file for 3Com BOOTP server, 3Com PXE server and BOOTPTAB Editor.
#
# Blank lines and lines beginning with '#' are ignored.
#
# Each entry in the file contains a name for the entry and a series of
# fields, separated by a colon. Fields are defined by a two-character
# "tag;" some supported tags are explained below:
# More supported tags are available. Please refer to 3Com white paper: BPPatch3.
#
#ha - hardware address
#ip - host IP address
#hd - home directory
#bf - bootfile name
#hn - return host name
#sm - sub-net mask
#tc - template host (points to similar host entry)
#to - time offset (seconds)
#
# Fields within entries may appear in any order. Spaces and tabs in lines
# are ignored. An entry can span more than one line in the file by ending
# continuing lines with a backslash.
```

```
default:hn:hd=\tftpboot\:sm=255.255.0.0:to=3600:
```

```
Conrad:tc=default:ha=0207010422A7:ip=132.147.180.5:bf=tsg.img:
John:tc=default:ha=00C0930067D2:ip=132.147.180.9:bf=john.img:
Paul:tc=default:ha=00A024823421:ip=132.147.180.4:bf=paul.img:
Ron:tc=default:ha=0000F4B048CA:ip=132.147.180.7:bf=win95.img:
Steve:tc=default:ha=00001B49D9D7:ip=132.147.180.110:bf=menu.mnu:
DABS:tc=default:ha=00104B111111:ip=0.0.0.0:bf=DABS.pxe:
```

B. Sample PXE menu boot file

DABS.PXE (Figure 8).

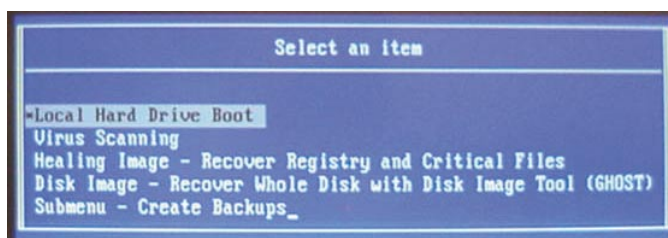


Figure 8: PXE menu boot file—DABS.pxe

C. Sample Virus Scanning Boot Image file

VIRUSCAN.IMG

```
CONFIG.SYS (for VIRUSCAN.IMG)
device=ifshlp.sys
device=himem.sys /testmem:off
device=emm386.exe noems
```

```
dos=high,umb
files=30
buffers=50
lastdrive=z
```

```
AUTOEXEC.BAT (for VIRUSCAN.IMG)
```

```
@echo off
```

```
Rem Load NDIS2 drivers, initialize the network adapter, start network services,
Rem and logon to the server as VirusAdmin (with "noVirus" as the password).
Rem The administrator should create an account on NT server named "VirusAdmin" and
Rem grant accordingly access privileges to this account.
```

```
net initialize
```

```
net start
```

```
net logon VirusAdmin noVirus /savepw:no /yes
```

```
Rem Map a network drive x: to the network share "VirusLog" on the server (McLaren)
```

```
Rem The administrator must create the share and grant appropriate rights to the user
```

```
Rem "VirusAdmin"
```

```
net use x: \\McLaren\VirusLog
```

```
Rem =====
```

```
Rem Syntax of F-PROT:
```

```
Rem F-PROT [drivefileldirectory] [options]
```

```
Rem Options of F-PROT used in the example:
```

```
Rem /HARD Scan all files on all hard drives in the computer.
```

```
Rem /AUTO Do not request the permission before removing each virus.
```

```
Rem This parameter works with /DISINF, /DELETE, or /RENAME
```

```
Rem /DISINF Disinfect whenever possible.
```

```
Rem /RENAME Rename infected COM/EXE files to VOM/VXE. If files with those
```

```
Rem extensions already exist, .VVV is used instead. Infected document
```

```
Rem files are not renamed.
```

```
Rem /DELETE Delete infected files.
```

```
Rem /DISINF /RENAME /DELETE together means: disinfect when possible, otherwise
```

```
Rem attempt to rename infected COM/EXE files to VOM/VXE, but if that
```

```
Rem fails the files are deleted.
```

```
Rem /ARCHIVE Scan inside .ZIP and .ARJ files. Support for .LZH and .RAR
```

```
Rem archives, as well as self-extracting archives may be added later.
```

```
Rem /APPEND Append the report to an existing file (only used with /REPORT).
```

```
Rem /REPORT=X:VirusRpt.log Send the output to a file, in addition to
```

```
Rem displaying it on the screen.
```

```
Rem /WRAP Wrap text so the report fits in 78 columns.
```

```
Rem /NOBREAK Disable ESC and Ctrl_C during scanning.
```

```
Rem =====
```

```
F-PROT /HARD /AUTO /DISINF /RENAME /DELETE /ARCHIVE /APPEND /REPORT=X:VirusRpt.log /WRAP/NOBREAK
```

```
if errorlevel 0 goto success
```

```
if errorlevel 1 goto terminate
```

```
if errorlevel 2 goto selftest
```

```
if errorlevel 3 goto BFvirus
```

```
if errorlevel 4 goto Mvirus
```

```
if errorlevel 5 goto CTRL_C
```

```
if errorlevel 6 goto Single
```

```
if errorlevel 7 goto NoMem
```

```
if errorlevel 8 goto suspicious
```

```
goto end

:success
Echo End of virus scanning. No virus found.
goto end

:terminate
Echo Abnormal termination - unrecoverable error.
Echo This can mean any of the following:
Echo . Internal error in the program.
Echo . DOS version prior to 3.0 was used.
Echo . ENGLISH.TX0, SIGN.DEF or MACRO.DEF corrupted or not present.
goto end

:selftest
Echo Selftest failed - program has been modified.
goto end

:BFvirus
Echo A Boot/File virus infection found.
goto end

:Mvirus
Echo Virus found in memory.
goto end

:CTRL_C
Echo Program terminated with ^C or ESC.
goto end

:Single
Echo A virus was removed.
Echo This code is only meaningful if the program is used to scan just a single file.
goto end

:NoMem
Echo Insufficient memory to run the program.
goto end

:suspicious
Echo At least one suspicious file was found, but no infections.
goto end

:end
Echo.
Echo Virus scanning finished. The system will be shut down.
Rem wait.exe4 is an external utility to wait a specific period of time (in second).
wait 4
Rem shutdown.exe5 is an external utility to shut down the client PC with APM or ACPI.
shutdown
```

D. Sample network files

PROTOCOL.INI

```
[network.setup]
version=0x3110
netcard=ms$ndis,1,MS$ndis,1
transport=ms$ndishlp,MS$NDISHLP
transport=ms$netbeui,MS$NETBEUI
lana0=ms$ndis,1,ms$netbeui
lana1=ms$ndis,1,ms$ndishlp
```

```
[ms$ndis]
drivename=undis$
; INTERRUPT=3
; IOADDRESS=0x300
; DMACHANNEL=none
; DMAMODE=burst
; MAXTRANSMITS=12
; MAXREQUESTS=8
```

```
[protman]
drivename=PROTMAN$
PRIORITY=MS$NDISHLP
```

```
[MS$NDISHLP]
drivename=ndishlp$
BINDINGS=ms$ndis
```

```
[ms$netbeui]
drivename=netbeui$
SESSIONS=10
NCBS=12
BINDINGS=ms$ndis
LANABASE=0
```

SYSTEM.INI

```
[network]
filesharing=no
printsharing=no
autologon=no
computername=Universal
lanroot=a:
username=Superman
workgroup=workgroup
reconnect=no
directhost=no
dospophotkey=N
lmlogon=0
logondomain=NT4test1
preferredredir=full
autostart=full
maxconnections=8
```

```
[network drivers]
```

```
netcard=ndis.dos
transport=ndishlp.sys,*netbeui
devdir=a:
LoadRMDrivers=yes
```

```
[Password Lists]
SUPERMAN=A:\SUPERMAN.PWL
*Shares=A:\Shares.PWL
BOOTROM=A:\BOOTROM.PWL
```

References:

1. F-PROT, <ftp://ftp.europe.datafellows.com/anti-virus/free/>
2. Universal NDIS2 Driver, <http://developer.intel.com/ial/wfm/tools/pxepdk20/index.htm>
3. SHUTDOWN.EXE, <http://www.lanworks.com/download>
4. REBOOT.COM, <http://www.lanworks.com/download>

**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 World Wide 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, and DynamicAccess are registered trademarks of 3Com Corporation. Microsoft, Windows and Windows NT are registered trademarks of Microsoft Corporation. All other trademarks are the property of their respective owners. All other company or product names may be trademarks of their respective companies. All specifications are subject to change without notice.

Printed in U.S.A.

000000-001 5/00