Workflow Systems
Using BartPE Quick Ref

1. OVERVIEW

BartPE is a Windows Preboot Environment that essentially allows you to boot Windows 2003 like OS from a CD and have available "most" of Windows 2003 abilities based on Windows 2003 drivers and services. Bart PE is based off of WinPE available from Microsoft for Enterprise customers. The CD supports all Dell PowerEdge and Optiplex RAID and Network drivers. HP should be supported but there are some problems reported with networking. From this Environment you will be able to:

- Look at all the Server's disks no matter with RAID controller is used.
- Connect to the Network.
- Create or Restore Ghost Images either locally or across the network (previously with DOS NDIS2 network boots a max of 2GB images could be saved).
- Open and modify the target Server's Registry.
- Scan for Viruses.
- Scan for Spyware.
- Reset Passwords.

BartPE was created and published by Bart Lagerweij of NU2: http://www.nu2.nu/pebuilder/

2. GETTING BARTPE

There are several ways of creating a bootable BartPE CD (or FlashDrive). You can create your own BartPE CD from scratch by following the instructions from NU2, or download a pre-made CD from TechPlanet.

2.1 Getting BartPE ISO

1) From TechPlanet: **Software > Dell > Server > Downloads > Utilities > Windows 2003 BartPE**.
2) Unzip the file to get the ISO.
3) Use Nero or any other CD writing utility to open and write the ISO to CD.

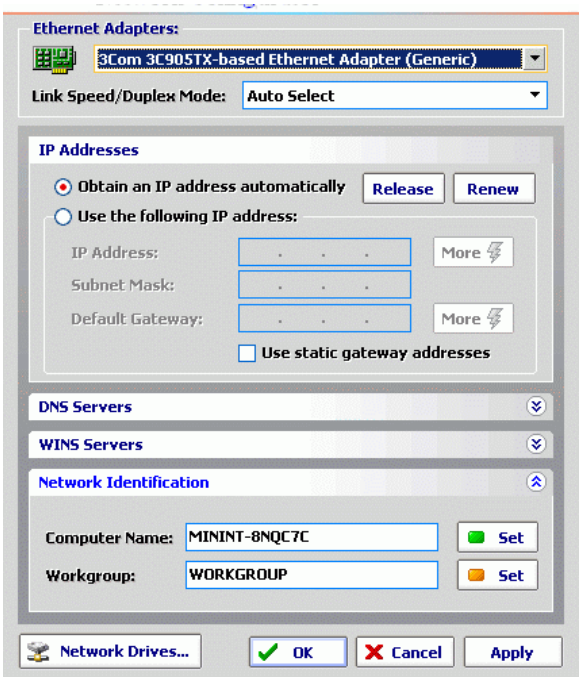
2.2 Booting BartPE

4) Insert the CD and boot the Server. you will automatically load into BartPE ui. The network will also try to automatically start with DHCP. You will see the following:



5) Overriding DHCP with a static IP.

a) Select **Go > System > Network > PE Network Configurator**. Under Ethernet Adapters it should show you the Systems detected NIC. You should see the following:



b) Under *IP Addresses* select **Use the Following IP address**. Enter in the fields as required and hit **Apply** > **OK**

6) Open up a command line by selecting **Go > Run**. Type **CMD** and hit **OK**.

7) Verify the network has started.

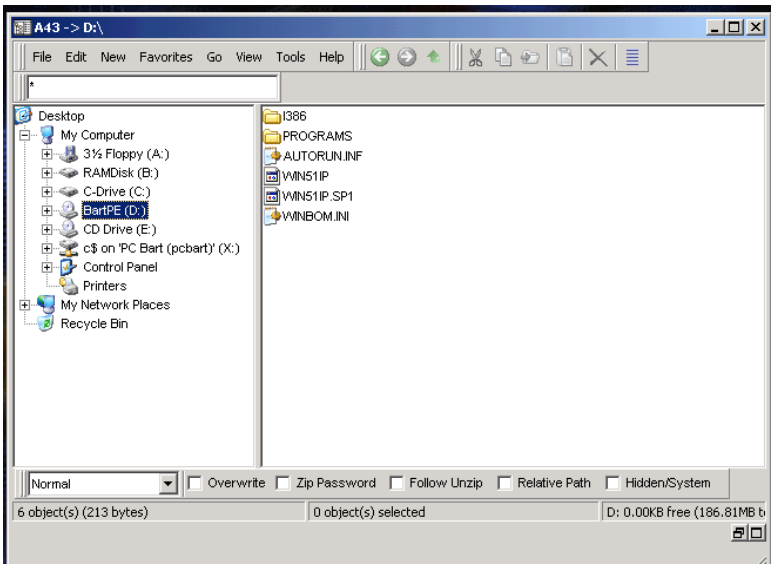
a) From the command line type **IPConfig**. You should see the NIC's IP address.

b) From the command line type **PING** and enter the default gateway's address.

2.3 Looking at files.

Explorer is not supported in BartPE. The file management program installed by default is **A43**.

1) Select **Go > Programs > A43 File Management Utility**. you should see the following.



2) The following drivers will be seen:

A:	Standard Floppy
B:	RAM Disk. This is where BartPE keeps its temporary files.
C:, D:, ...	Server's internal partitions. These "may" be of a different drive lettering scheme as opposed to booting directly from the Server's OS.
X:	BartPE's CD. Note you will not be able to eject the CD until you reboot as this drive is locked for explusive use when booted into Bart.

2.4 Using Ghost

I will assume you will be creating or restoring an image from across the network.

1) Mount a Network Drive.
   a) Gui: Select **Go > System > Network > Map Network Drive**. Mount the drive as normal.
   b) Dos: type: **NET USE * \\ServerName\Share /u:ServerName\Account**. When prompted enter the password.
2) Start Ghost by selecting **Go > Programs > Symantec Ghost > Ghost32** and hit **OK**.
3) Run Ghost as you normally would. Using the mouse appears to be overly sensitive and will tend to send you several menus deep. I would recommend using the cursor keys to move around.
4) To **Restore** and Image:
   a) Select **Local > Disk > From Image**.
   b) **<Shft><Tab>** and hit the **<DownArrow>** and **<Enter>** to select the mapped network drive (typically Z:).
   c) Select the **Appropriate Image** and hit **<Enter>**.
   d) Select the **Target Disk** (which will typically be Drive 1 and hit **<Enter>**.
   e) Modify the **partition sizes** only if needed (not normally needed) and hit **<Enter>**.
   f) Select **<Yes>** to proceed with the restore. Restoring with a Broadcom or IntelPro 1000 will typically start at 2200 MB/min, then work down to anywhere from 1200MB/min to 2100.
   g) When the image is complete select **Reset Computer**. Once the server is out of the BartPE remove the CD.

5) To **Save** an Image. Ghost under BartPE will allow for >2GB images, but the images will be broken into 2GB chunks. For this reason it is a good idea to create an empty folder on the target network share.
   a) Open A43 by selecting **Go > Programs > A43**.
   b) Create a new folder on the Network share. Close A43.
   c) From Ghost select **Local > Disk > To Image**.
   d) Select the Source disk. This will typically be Drive 1 for the Server's OS disk.
   e) **<Shft><Tab>** hit the **<DownArrow>** and select the mapped network drive (typically Z:).
   f) Select your new folder. Hit <Tab> and enter in the image name. The name should be no more then 5 characters since each 2GB chunck will add 3 digit suffix to the name.
   g) Hit **<Alt>'S'** to save and **Yes** to proceed.
   h) Saving with a Broadcom or IntelPro 1000 will typically start at 2200 MB/min, then work down to anywhere from 1200MB/min to 2100.
   i) Select **Quit** > **Yes**.
   j) To restart the Server select **Go > Shutdown > Restart**.

2.5 Checking for Virus's

McAfee under BartPE will allow you to scan and repair infections on the Server's system disks. The virus engine can not be upgraded in the field at this time and is locked to the version that is installed on the CD. At the time of this writing Kodak's BartPE v0.19 virus definition file of date Oct 30, 2006 is being used.

1) Start McAfee by selecting **Go > Programs > McAfee VirusScan GUI Wrapper**.
2) Leave default, or select a folder to scan.
3) Select Scan to begin the scan. Once complete a report will open displaying the scan's results.

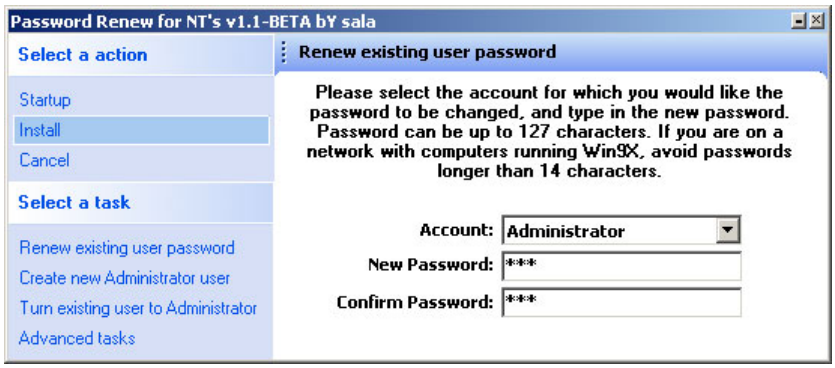
2.6 Editing the Server's Registry

Standard registry editors would modify BartPE's registry instead of the Server's. To modify the Server's hive we use **Registry Editor PE**.

1) Start the editor by selecting **Go > Programs > Registry Editor PE**.
2) Select the System hives.
   a) Select the **Server's Windows** folder and hit **OK**.
   b) Hit Open to the detected **SAM, Security, Software, System** hives.
   c) Hit **Yes** to the remote user profile.
   d) Browse to the "**Documents and Settings\Administrator\NTUser.dat**" and hit **Open**.
   e) Select No to another user profile.
3) once you have finished making registry edits close the editor. The hives should show a successful disconnect.

2.7 Resetting Passwords

Password Renew is a utility that can reset the password to existing accounts, raise the access level of a given account, create new accounts.
Note! Microsoft will from time to time change their hashing for Windows 2003. This has been tested successfully as of Nov, 2007.



1) Start the editor by selecting Go > Programs > Password Renew.
2) Click "**Select a target**" (bottom right of screen) and select the **C:\Windows** directory.
3) Select "Renew an existing password".
4) Select the accounts whose password you wish to reset.
5) Enter and confirm the updated password.
   Note! Computers who have been added to Domains will have a password policy that has been pushed onto the client. The new password must satisfy the Domains password complexity policies.
6) Click **Install** and **OK** to the success prompt.
7) Reboot with the BartPE CD removed.

2.8 Modifying Partitions

This isn't working properly at the time of this writing with v0.32.

3. OTHER TOOLS AND FINDINGS

Thanks to Peter Valck for showing me WinPE and Bart's preboot environment options. If you find any useful plugins that are safe please contact Derek Braendel in TIS.