Paper Number 5135
Deploying a Standardized PC Operating Environment

Tony Jones
Hewlett-Packard Company
371 Hoes Lane
Piscataway, NJ 08854
908-562-6248
Tony_Jones@hp.com

The HP Professional Services Organization provided assistance to a major telecommunications company in order to implement and deploy a standardized environment across various districts within one of its divisions. The environment is based on Windows 95 clients, Windows NT servers and interoperability with UNIX based workstations and servers. The deployment has led to:

- Better usage of shared resources such as printers and project areas
- Increased productivity
- Reduced support costs

This paper discusses the following topics:

- Standardizing (reducing) PC configurations
- Getting management support and commitment
- Overview session for end-users
- Migration process (Windows 3.X to Windows 95)
- Software distribution via Microsoft System Management Server (SMS)
- Backing up PC data over network
- Detecting/Removing viruses
- Managing TCP/IP information via Dynamic Host Configuration Protocol (DHCP)

Upon completion of the presentation, participants will have a better understanding of how to migrate a PC user community to a more stable, supportable environment.

Architecture Overview

The infrastructure environment consists of HP NetServers functioning as Windows NT servers. The clients consist of Windows 95 based PC's. The baseline operating environment consists of approximately 16 applications (including the Windows 95 operating system). Each user has an account in the Windows NT domain along with access to file storage space on the servers.

The printers are driven by both the NT server and HP-UX based servers. The LPR/LPD protocol is used to talk to JetDirect based printers. Even though the JetDirect interfaces support multiple protocols, standardizing on one protocol allows us to focus attention on ensuring proper router configuration across the network. In addition, LPR/LPD is supported by UNIX and NT. The printers are managed by HP JetAdmin for HP-UX.

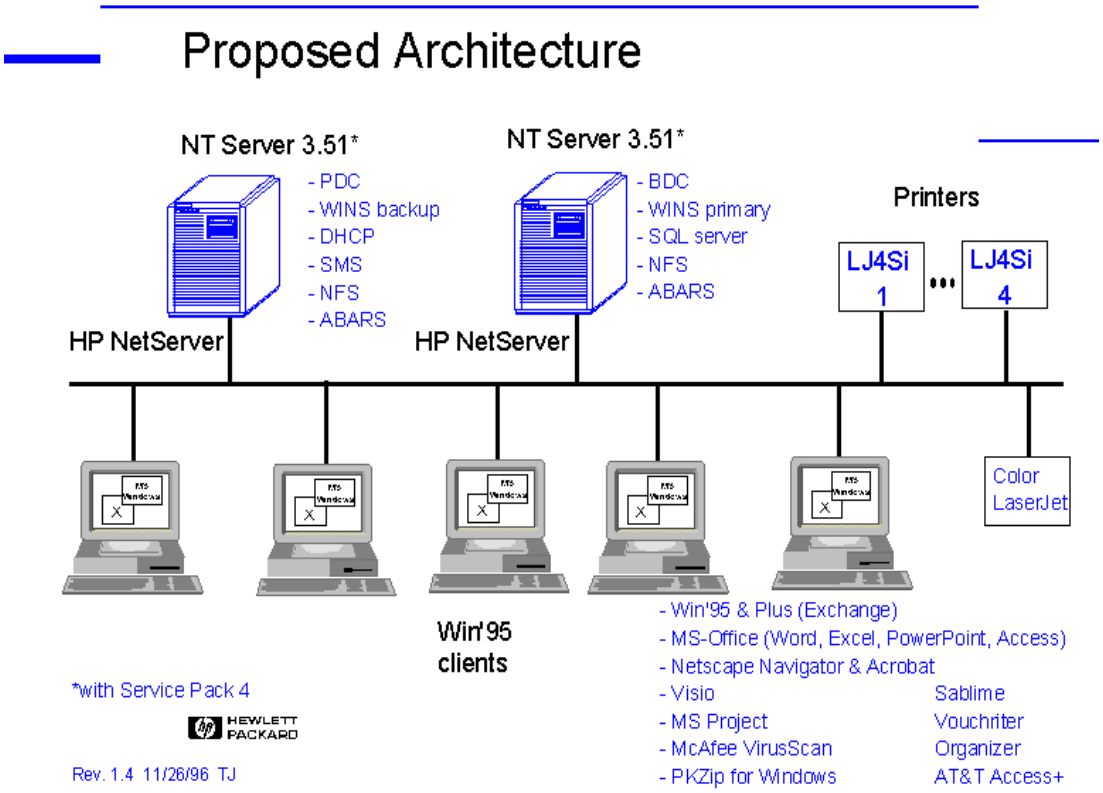

Figure 1. Standardized Architecture

Data directory on local hard drive

Each end-user hard drive has a "data" directory with a subdirectory allocated for each major application. The default data location for each of the baseline applications has been configured to point to the appropriate subdirectory. Therefore, whenever you do a "Save As...", the data file will be placed in the appropriate subdirectory. The user can override this location. The recommendation is that end-

users add a data subdirectory for each new application. This will facilitate backing up user data. The following is a sample directory:

C:\data\	C:\data\
winword\	exchange\
excel\	msproj\
powerpnt\	attmsg\
access\	attplus\
netscape\	vouch\
visio\	your_folder_name\

Standardizing (reducing) PC configurations

The initial phase of the project consisted of setting up the NT server infrastructure and five client PC's. Each of the PC's were set up with the baseline software. This also allowed us to test application interoperability to verify that the PC's would provide a stable environment to the end-users. The different PC hardware configurations represented a cross section of the equipment found in the user community. After testing was completed, we made a hardware configuration recommendation available for new purchases. The benefits to standardizing (reducing) PC configurations include:

- Less hardware permutations to test/troubleshoot/document
- Less types of hardware repair inventory to stock

The software environment consists of a standard data directory (C:\data\...), standard set of printer drivers loaded on each PC, and the "I:" network drive points to user's home directory on the file server.

Getting management support and commitment

Management support and commitment were critical to the success of the project. Without management commitment, end-users would tend to push off the conversion as long as possible. It was also very important for management and the end-user community to be prepared for an initial drop in productivity while users learned the new environment. Even though the user community was "Windows" literate, there were significant differences between the original Windows 3.X and the new Windows 95 environment. The new environment also included NT domain logins, network based printers, and network based file sharing with increased security constraints.

Users were not allowed to purchase (or be reimbursed for) additional software unless their PC had the standard environment.

Management support was also critical in order to set aside a room with five PC's (and LAN connections) for end-user overview sessions. The room and equipment were available throughout the deployment.

Overview session for end-users

End-users were required to sign up and attend an overview session before their PC was migrated to the standard environment. Two overview sessions were run each Monday and we had until the end of the week to convert the PC's. Each overview session had a total of 10 end-users. During the session, two users shared a PC and actually used the standard environment. End-users also received and used their login accounts during the session. An End-user Guide was developed and used as the basis of material covered during the session. We also incorporated suggestions from the end-user community, thus increasing the value of the document as future reference material.

Participation in the overview session established a baseline knowledge level. This was especially useful with respect to handling support related calls.

See Appendix A. for End-user Guide table of contents.

Migration process (Windows 3.X to Windows 95)

The operating environment needed to support different types of clients (Windows 3.1/3.11/95) since it was not possible to convert the entire user base in one quantum jump. Even though the target environment was based on Windows 95, we wanted to take advantage of the new equipment (i.e. disc space) in order to migrate the PC's.

The general procedure to migrate a user to the standardized environment is:

- End-User signs up and attends overview session
- Create User Account and Personal "Share" on NT file server
- Connect PC to NT server via TCP/IP
- Back up PC using Pkzip for Windows (into zip file stored on file server)
- Get PC LAN card MAC address
- Reserve IP address based on MAC address using DHCP
- Create SMS jobs on server to install PC baseline software
- Install baseline software on PC (after clearing hard drive)
- Restore data (from zip file). These directories should end up residing under c:\data. You may also have to move data files up to appropriate directory level (c:\data\winword\msoffice\winword*.doc -> c:\data\winword*.doc)

After each application was installed, it was still necessary to configure default data paths. Each application was configured to have its default data path set to a subdirectory under C:\data. This step was completed during the migration process. The end-users found this to be very convenient because they could focus their attention on creating/modifying the information since the default data location was taken into account as part of the backup/restore plan.

One of the main goals was to provide a comprehensive user environment. For example, PKZip for Windows was chosen because one executable could be used for Windows 3.X, Windows 95, and Windows NT. It supported long file names, zip file spanning across multiple floppies, and had a consistent interface across the different clients found during the migration. Including PKZip in the baseline also allowed end-users to compress or expand (unzip) their own files, since many of the files encountered on a day to day basis (including internet files) are in "zip" format.

Note: Only data files from the user's backup were restored as part of the migration process. Users were responsible for re-installing any applications that were not part of the baseline.

Software distribution via Microsoft System Management Server (SMS)

Microsoft SMS includes the following features: software distribution, hardware/software inventory, and PC remote control. The PC's were configured to check for new software every 4 hours. All baseline software was installed via the SMS package command manager client . SMS also provided the foundation to install upgrades based on current versions of software loaded on end-user PC's.

Users no longer had to find CD's or floppies to install applications. In addition, baseline software was tested before end-users installed it on the PC's. This also allowed the support team to become familiar with the applications in order to answer questions.

We also used SMS to generate a report that listed converted PC's. This was very useful to show progress made during the migration.

Backing up PC data over network

We included an icon on the desktop called "backitup". When an end-user double clicked on the icon, it would copy any new or updated files found under the c:\data subdirectory to the i:\data subdirectory (on the server). It was the end-user's responsibility to back up their own files. Restoring files was as simple as opening the I: drive and copying files back onto the C: drive. The various servers were backed up over the network to a centralized system on a weekly basis.

There was no need to back up executables because the baseline environment could always be re-installed on the PC in case of disaster.

Detecting/Removing viruses

McAfee VirusScan is part of the standardized environment and was also used during the migration process to clean up any infected files. During the migration process (backing up hard drive and restoring user data files), viruses were found on some of the users' hard drives.

We also found that some end-users developed a false sense of security when they found virus detection software on their PC. Many of the new PC's came with an older version of the McAfee VirusScan utility. This software needed to be kept up to date more than any other application because new types of viruses were always being developed. The most often encountered viruses were MS-Word macro viruses.

Managing TCP/IP information via Dynamic Host Configuration Protocol (DHCP)

DHCP allowed us to centrally manage TCP/IP related information used by the PC's. Instead of having to manually configure this information on each PC, we were able to configure the DHCP subsystem to pass the information down to a PC when it booted up on the network. This also allows for future changes to the network with less dependency on informing the end-users.

The TCP/IP related parameters passed to the PC's included:

- IP address
- Subnet mask
- Default gateway
- DNS server addresses including search order
- Domain and organization information

- Microsoft WINS server address
- Address resolution method

The PC LAN card MAC address was used to reserve a unique IP address (per PC). Since each of the original users had IP addresses assigned to them (as part of getting their PC on the network), we wanted to pass the same designated IP addresses down to each their PC's when they booted up. By downloading the same IP address to the PC's, we were able to maintain the original IP address list (hosts table) used before we introduced DHCP.

Note: In order to support DHCP across routers, the routers must support or be upgraded to support RFC 1542 (BOOTP relay agent). Without this support, the PC's and the NT servers must be on the same subnet.

Appendix A. End-User Guide Table of Contents