

**New Hampshire Wing Headquarters Building
Local Area Network
Lt Col Skip Guild (NH Wing/IT)
23 April 2005**

The Local Area Network (LAN) installed in CAP Headquarters (Concord) is currently configured as indicated in Figure 1. The Digital Subscriber Link (DSL) connection to the Internet is brought into the Headquarters building and connects to the DSL Modem in the basement. The Modem is connected to a collocated Router which splits the signal from one Modem to up to [] wall outlets spread around the building (indicated by the red squares in the figure). Members with wired LAN connectors on their PCs can bring their PCs (and CAT5 LAN cable) to Headquarters and connect to the Internet simply by plugging their cable into any available cable outlet. One of the LAN outlets is connected to a WiFi Wireless Access Port which can share access to the LAN by multiple PCs using 802.11b or 802.11g wireless transceivers in or attached to your PCs. The PCs do not normally share their own disk drives or attached printers with other users on the LAN. Wired and Wireless PCs must be configured to get their local IP Address from the Domain Name Server (located physically in the Router). The Wireless Access Point also implements Wireless Encryption Protocol (WEP) with a Shared Password to protect the LAN from non-CAP members trying to access the LAN from outside the building. Detail on configuring PCs for Wireless connections is described in an instruction sheet at Headquarters.

For security purposes, all the servers and PCs in the building (including the mobile PCs which may be able to access the Wireless Access Point from a short distance outside the building) are protected by a firewall in the Router and are not accessible from the Wide Area Network.

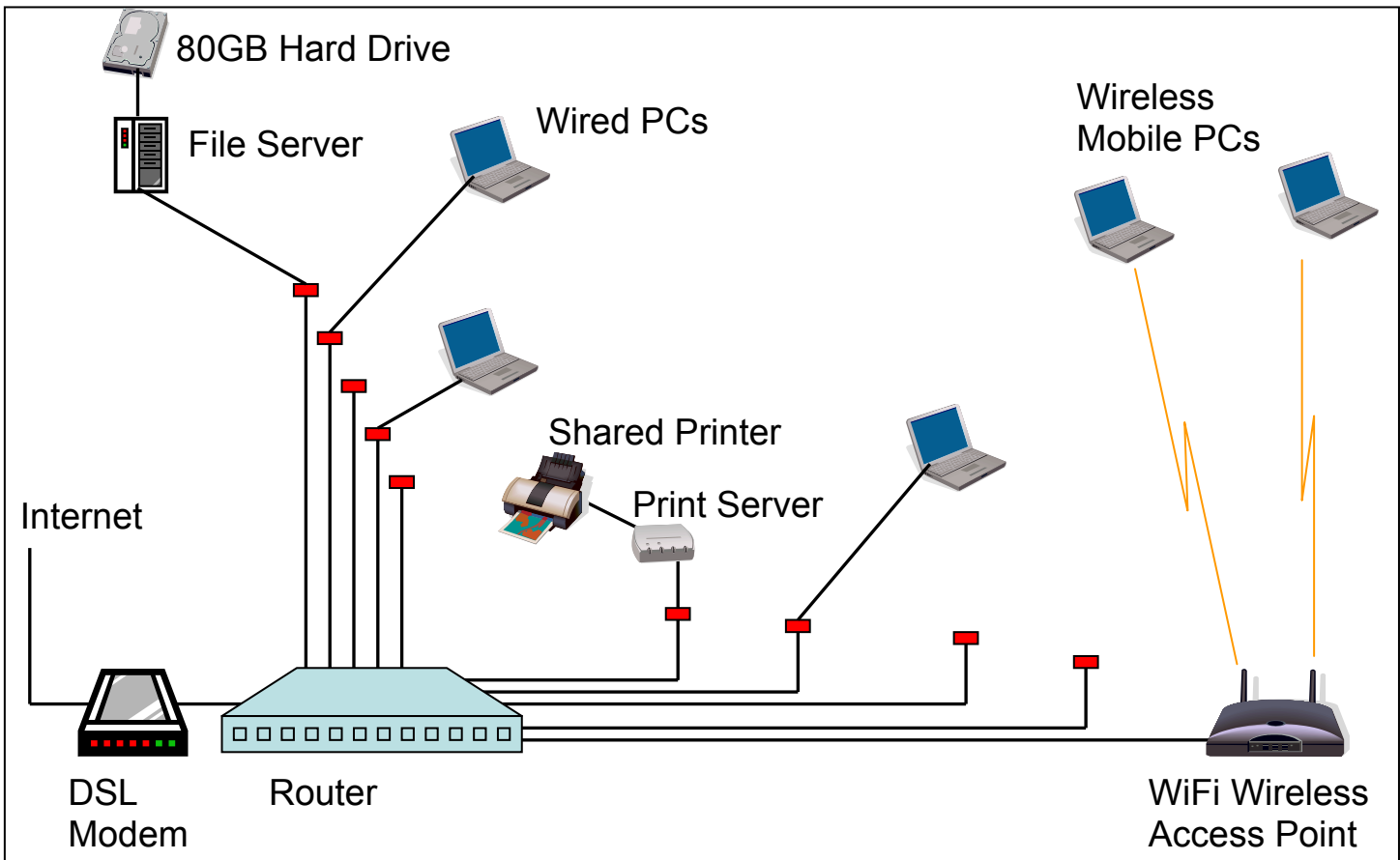


Figure 1 . LAN Topology
Page 1 of 8

The Internet Protocol (IP) Address Assignments for the devices on the local network are:

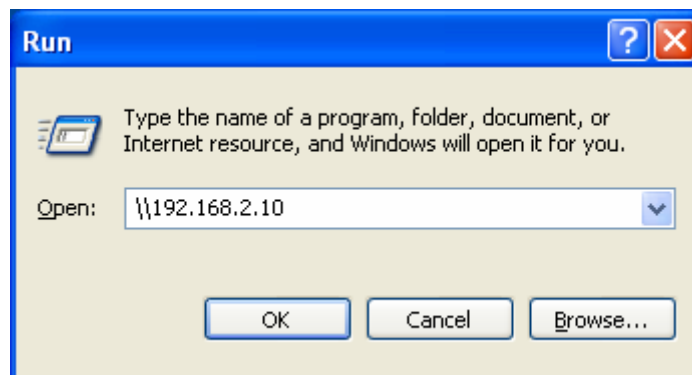
Device	IP Address
Wired LAN Router (DNS)	192.168.2.1
Wireless LAN Router (WAP)	192.168.2.2 **
File Server	192.168.2.10
Print Server	192.168.2.50
PCs	192.168.2.100-255 (Dynamic)

** IP address still assigned dynamically but will be...

FILE SERVER

A shared File Server has been added to the LAN. It is currently located in the main room on the table against the south wall closest to Concord Airport entrance. The file server and attached external 80GB hard drive will eventually be relocated to the basement to get it out of the way. The server and hard drive is accessible to all the PCs in the building over the LAN. Access to the server is limited to PCs on the local area network by the building's firewall.

The first time you try to access the file server, you need to connect to it from the Start Menu by clicking on Start ... Run and entering the IP Address of the server as illustrated here:



and then click on "OK". This should open a Windows Explorer window (Figure 2) showing the folder contents of the file server.

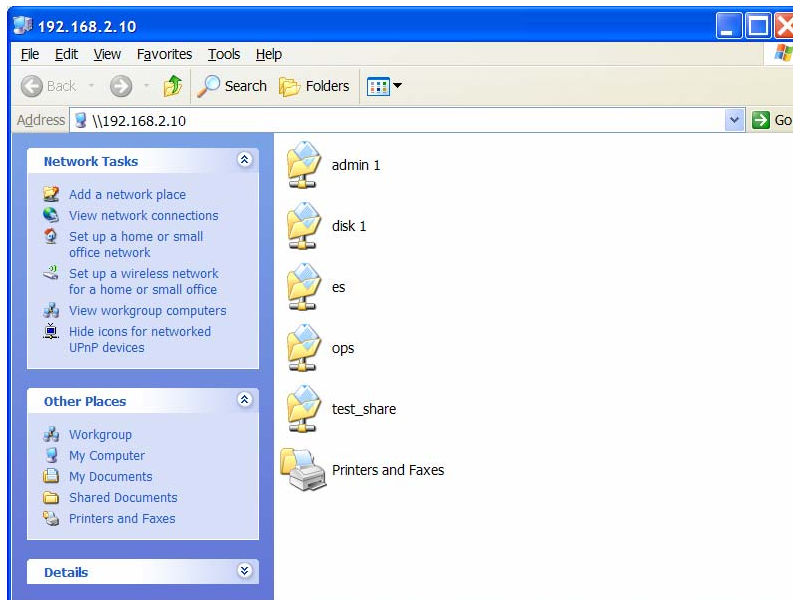


Figure 2. Sample File Server Folders

If you cannot access the server, you may have to modify your PC configuration to access the LAN. If no one in the building can access the server, the server may have to be reset. This server can be reset by pressing the power button on the front of the unit and after a few seconds turning it back on. The server takes about a minute to reboot.

Depending on what you want to do with the folders you see on the server hard drive, you can right click on them and permanently map them to drive letters (e.g., Z: or M:) for ease of access in the future, or simply create a shortcut to the server on your desktop by selecting the computer icon in the Address window (Figure 2) and Drag and Drop the icon to your desk top. This will create a shortcut on your desktop with a name set to the IP Address of the server as shown in. You can select and rename the icon to a more user friendly name like the server's real name, HQ Server. You will not be able to access the server from home as the local area network is protected by a firewall, but the next time you visit HQ all you have to do to access the folders is double click on the HQ Server icon (or open the drive letter you created).

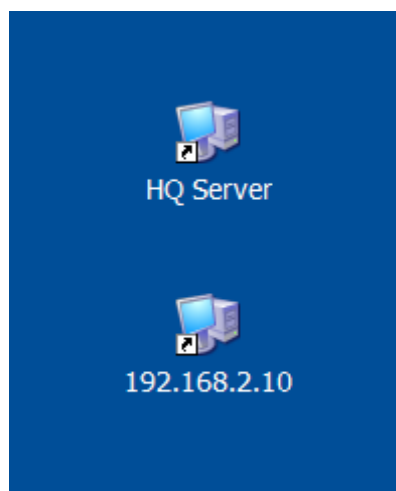


Figure 3. File Server Icons

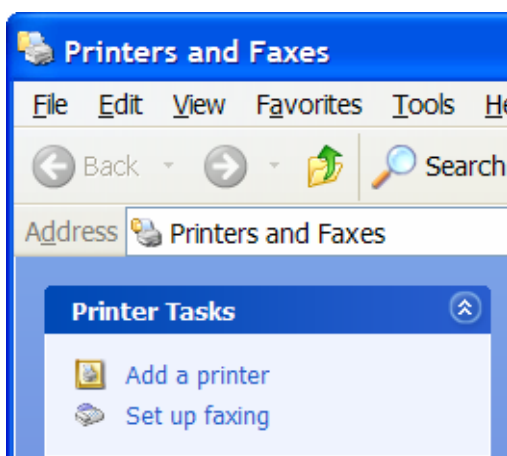
The sample folders shown here are only temporary and will be renamed and configured per the needs and requirements of each directorship. Samples of how the server can be used will be explained later.

PRINT SERVER

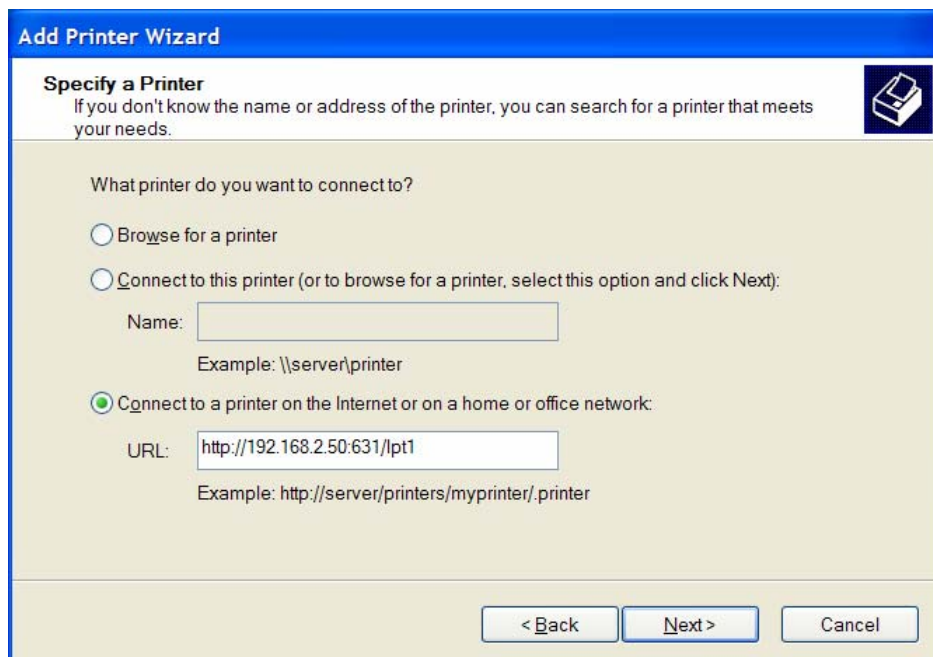
The second recent enhancement to the HQ LAN is the addition of a print server with attached shared printer. We are currently using the Canon i70 portable printer but this may be replaced with a more suitable printer later. The print server is configured via administrator software to support a specified printer. You cannot simply swap printers attached to the server and expect the new printer to be available on the LAN.

The advantage of having a shared printer is that anyone connected to the local network can print to this printer without having to have it physically connected to your computer. Anyone on the wired or wireless LAN can simultaneously share the use of this printer. Like the File Server, access to the printer is restricted by the building firewall to computers connected to the local network in the building.

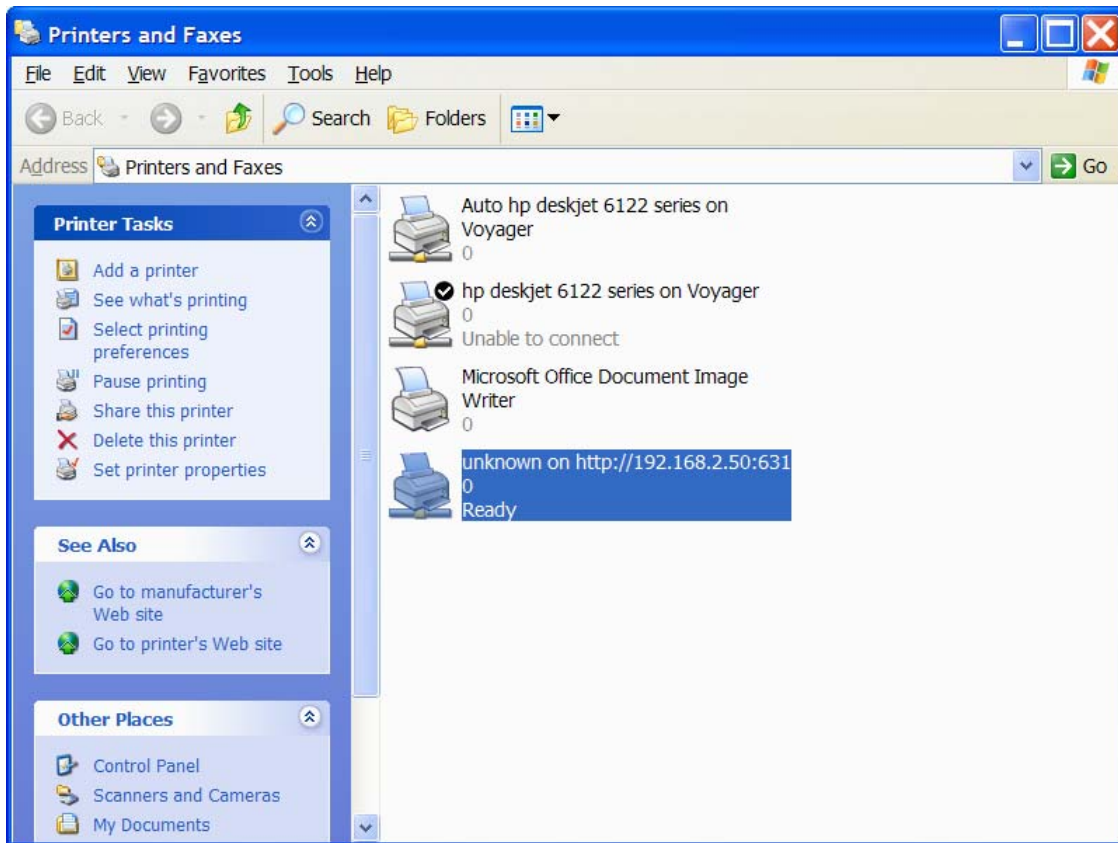
Again setting up your computer to use the shared printer is a one-time process you only need to do the first time you connect to it. From your Start menu, open the Printers and Faxes window



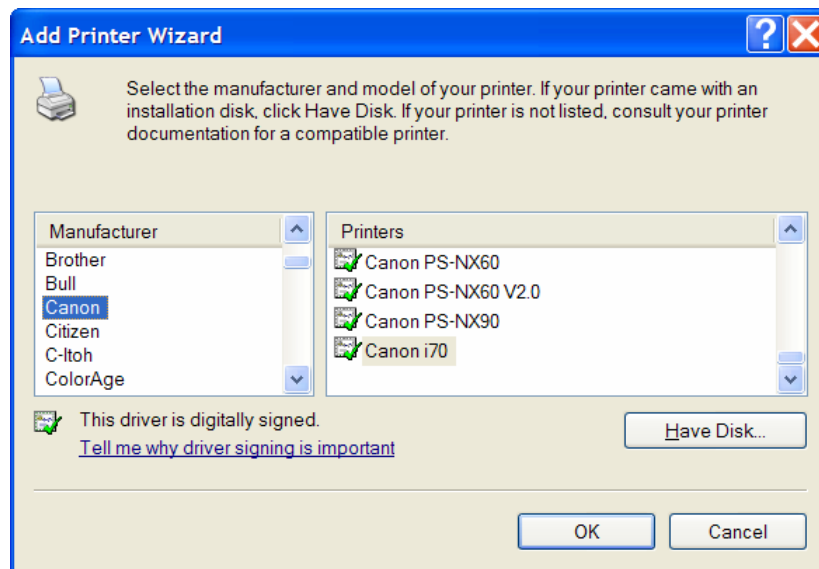
and click on Add a Printer. This will open the Add Printer Wizard. :



Enter the URL for the print server, **http://192.168.2.50:631/lpt1** in the URL window and click on Next. Follow the prompts and a new printer port will be created on your printer selection screen. You can select it and make it the default printer for as long as you are at HQ, or manually select this printer each time you print:

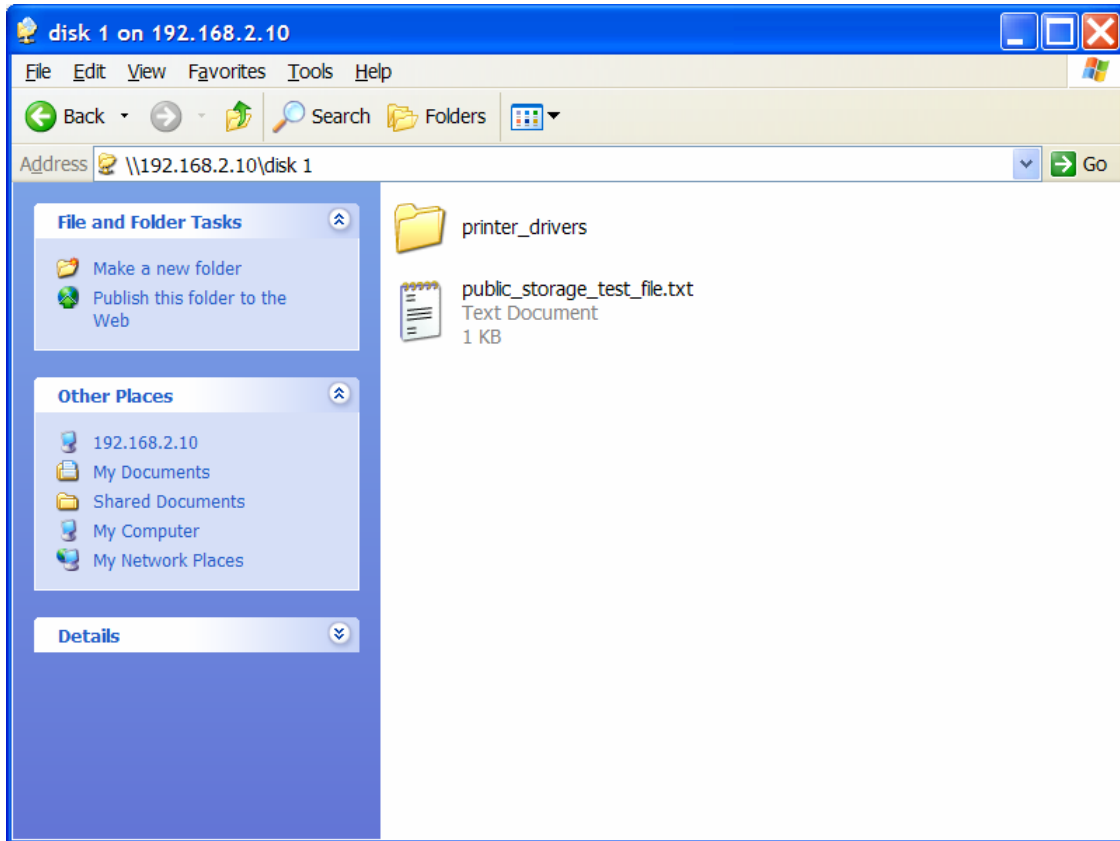


If your system does not have the printer installation files already installed for this printer on your computer, you will be prompted to specify the printer in the Add Printer Wizard.



Select Canon as the Manufacturer and Canon i70 as the printer. If this is not a selectable option on your computer, click on Have Disk, and navigate to the NH Wing shared file server (above if you haven't done so

before now), “disk 1” folder, then navigate from the “printer_drivers” folder down the applicable subfolders until you can select the install or setup file file.



FILE SERVER SETUP

The file server can be set up a number of ways. One way is to use it as a general-purpose shared asset with everyone sharing files stored on the server with no protection against someone else changing or erasing important files. The “disk 1” folder (Figure 2) is currently set up this way. Anyone can access this folder by double clicking on it and it will open a Windows Explorer folder as shown in Figure 3.

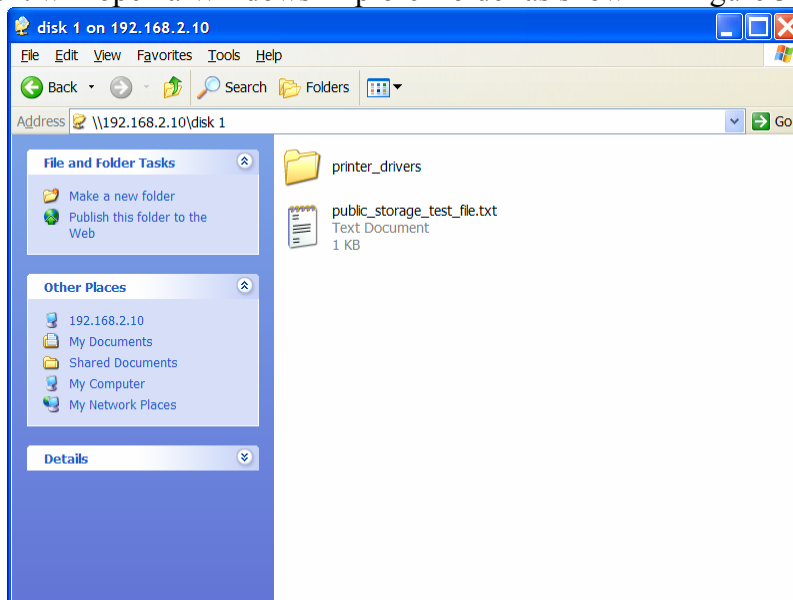


Figure 3. Disk 1 Folder

If you try to open other folders on the File Server today, you will find they are user name and password protected. They are accessible with varying levels of protection to groups of users defined by the Administrator on the server. This is the preferred way to use a file server in our environment. The Administrator will establish user names and individual passwords for every user. Each user will then be assigned by the Administrator as a member of one or more defined Groups. Each Group will in turn be given defined access rights (read-write-delete, read-only, or none) by the Administrator to one or more shared folders.

In the sample environment I set up, there is a user I've named "**ops_user**" with password "**operations**". This user has been assigned to one user Group I've named "**ops**". Several other users could be members of this Group, and this member could be assigned to multiple Groups. I have assigned members of the **ops** group certain access privileges. Any member of this group has "read-write-delete" privileges to the **ops** shared folder. This, by the way, is an example of a bad name for the shared folder. There is no predefined relationship between user names, names of user Groups, and the names of shared folders. For example, user bongo could be a member of the bongo group with access to the bongo folder which would be very confusing.

Continuing the example, I have also given members of the **ops** group "read-only" access to the **es** shared folder, and no access at all to the other folders (except Disk 1, of course).

Another member with user name "**es_user**" and password "**emergency**" is a member only of the **es** group. This group has been given read-write-delete privileges to the **es** shared folder, but only read-only privileges to the **ops** shared folder.

The result is that members of the "ops" group have total control over the "ops" shared folder and the members of the "es" Group have total control over the "es" shared folder. However each member can only read files in the other Group's folder. They cannot create, delete, or modify files or folders in the other group's folder. Note members of both groups cannot even open the files in the **admin 1** folder.

If this kind of file protection is desired for the server, the File Server Administrator would have to create shared folders, groups, and user names with individual passwords for every user. He/She would then individually assign each user to one or more groups as needed. Collectively we need to determine what shared folders are needed and who should "own" each folder. The owner then determines which groups should have read-write-delete privileges to his folder, which groups should only be allowed to read the files in his folder. The other groups have no access to his files. Figure 4 is a sample of what *could* be done with the server.

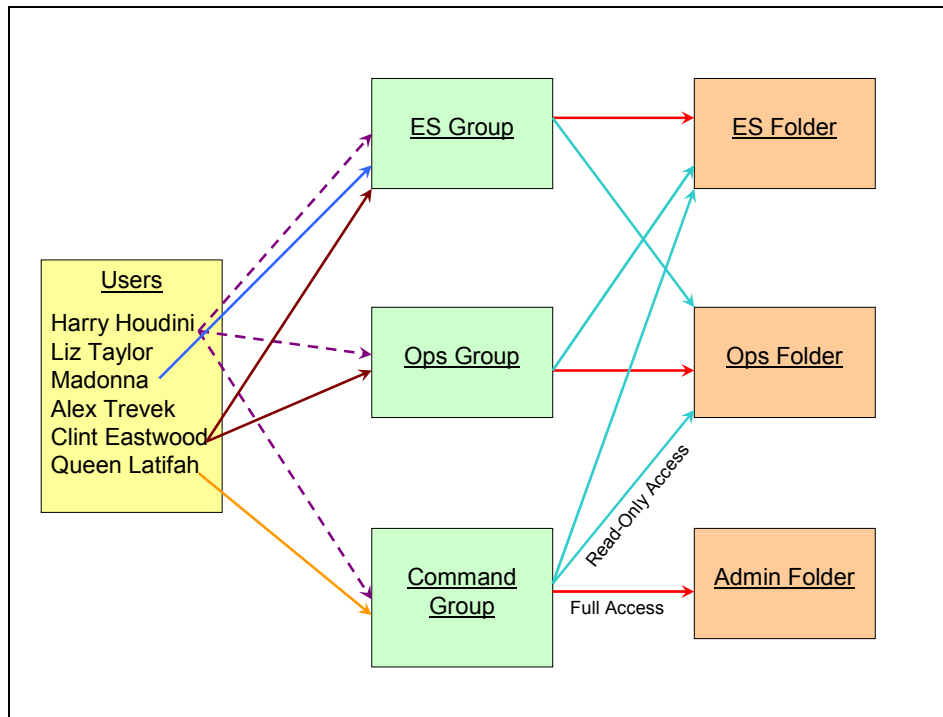


Figure 4. Sample Access Setup

Resulting access rights:

User	Folder	Access Rights
Harry Houdini	ES	Read-Write-Delete
	Ops	Read-Write-Delete
	Admin	Read-Write-Delete
Madonna	ES	Read-Write-Delete
	Ops	Read
	Admin	
Clint Eastwood	ES	Read-Write-Delete
	Ops	Read-Write-Delete
	Admin	
Queen Latifah	ES	Read
	Ops	Read
	Admin	Read-Write-Delete