Overview

Windows XP supports file sharing between computers on a local area network (LAN) which is configured as a "peer-to-peer" network. A peer-to-peer network is one where there is no server to authenticate users and passwords, and each user logs in directly to his/her own computer. Peer-to-peer networks are suitable for smaller companies who have 10 computers or less. As a company's total number of PCs approaches 10, it is necessary to begin planning for the implementation of a server, because a Windows XP computer cannot share files with more than 10 other computers.

In peer-to-peer networks, it is frequent practice to designate one particular machine as the "server", even though it is technically just another PC and does not have a server operating system such as Windows 2003 Server or Windows Small Business Server. This central machine can be used to store files for the entire company, and everyone can open and save files to/from this "server" in order to facilitate backup.

Experience has shown that if certain steps are taken on each machine, file sharing will become much more reliable. The purpose of this paper is to outline the steps required to build and maintain reliable file sharing between PCs on an peer-to-peer network.

System Requirements and Best Practices

1. Every computer on the network MUST have either Windows 2000 Professional or Windows XP Professional. Older systems like Windows 98 and Windows ME will work, but offer absolutely zero file security and will be a constant source of problems. Also, logins on Windows 98/ME are easy to circumvent, which in turn causes problems with file sharing. It is better to upgrade or eliminate all PCs which are still running Windows 98 or ME.

Windows XP Home will not work because XP Home does not offer the type of file and folder security that XP Professional offers. XP Home only offers the ability to share files and folders, without the ability to set protections that allow certain users to access certain folders but not others. XP Home is truly a home operating system and has no place in an office with a file sharing requirement.

2. The central server must have sufficient memory and disk space to serve files for all users. A minimum configuration for the server is 512MB of memory for up to 4 users. For more than 4 users, 1GB of memory is recommended in order for the server to be able to process multiple requests for files simultaneously.

3. The central server must have some kind of unattended backup system, such as a tape drive or an external, removable disk drive. CD-R drives can be used for backup, but they must be manually operated, and experience has shown that the more operator intervention is required, the less likely the backup system is to be effective. Backup to CDs should be consider as an interim solution only.

4. A redundant disk arrangement on a server is highly advisable. It is fairly simple and cost-effective to install a "mirrored disk" configuration on the server using what is called a "RAID card". With this expansion card and two identical disk drives, the system writes the exact same

thing to both disks simultaneously. If one disk fails, the other disk takes over instantly without having to shut down the computer. The failed disk drive can then replaced after hours with no downtime during business hours, and after installation, it re-mirrors and becomes once again identical to the other drive. In most cases a mirrored disk configuration can be added to the main server PC for under $500 including components and installation.

System Setup

In a peer-to-peer network, there is no server to log users in, check their passwords and grant them access to resources on the network. For this reason, there is a greater effort required to maintain the network, but once these procedures are understood, the effort is very manageable. Proper attention spent up-front in setting up the system will make ongoing maintenance much easier and less time-consuming.

1. Every computer must be made part of the same workgroup. It doesn't matter what the name of the workgroup is, but it absolutely must be the same on every computer.
2. "Simple File Sharing" in Windows XP must be turned off. "On" is the default setting, and it forces the user to use a very simplified method of sharing folders that provides no ability to open certain folders to certain individuals only. Windows XP Home provides nothing BUT simple file sharing and that's why it is unsuitable for a business environment.
3. Your software firewall must be configured to allow for file and printer sharing. Usually, when two computers cannot be made to share files, the #1 reason is the presence of a software firewall preventing it. In the Windows XP Firewall, you can check on an Exception that will permit file and printer sharing through the firewall.
4. Between any two computers where file sharing is desired, the logins and passwords must match. For example, let's say that a user logs in as John on PC01 on workgroup WORKGROUP with a password of "sunset". In order for John to be able to access files on any other computer on the network, that computer must also have a login of John with a password of "sunset". (Note: there are ways to work around this, but they are so troublesome and the results so inconsistent that it is easier to just consider this a requirement and learn to live with it.)

   If there is a central file server which serves up files to all the PCs on the network, then that file server must have a matching login for every user who logs into any PC on the network, and the passwords must match. It is this single requirement that makes the management of a peer-to-peer network more work than a server network. Every time a user changes his/her password, that password must be changed on every other computer with which that person shares or obtains files. For this reason it is best to set good passwords, instruct employees to keep them secret from one another, and then simply don't change them unless it's absolutely necessary.

   If an employee leaves the company, it is necessary to remove their login on every machine on the network where their login was set up, and especially on the server.
5. If a particular PC does not need to share its folders with other computers, then that PC does not need to have every login that exists on the network. It needs to have only the login of the person who uses it. However, if it is desired in the future to share one of its folders, then a login should be created on that computer that matches the login of any other user on the network who will access those files.

6. Logins must match exactly. You may know that "John" on one computer is the same as "John Smith" on another, but to Windows those are two separate people. Come up with a standard nomenclature and use it consistently for every login. It is also better if the login is all one word: "Jsmith" or "JohnSmith" or "John" are all better than "John Smith". A blank space in login names causes problems in other applications. Using only first names is fine until you get a second employee with the same first name – then you are forced to change your nomenclature. It is better to avoid first names only.
7. If the logins on two machines are inconsistent, DO NOT merely "rename" one of the logins, as Windows XP will allow you to. Go to the machine where the login does not meet your nomenclature and create a new login that does meet the standard, along with its matching password. Merely renaming an existing account provides inconsistent results.
8. Logins in Windows are NOT case sensitive, so a login of "jsmith" is equivalent to a login of "JSmith". But it is still better to standardize and then be consistent.
9. Every login must have a password. Windows XP does not like logins that have no password, and they will be a source of constant headaches. Many people don't like passwords, but they are absolutely mandatory for consistent file-sharing. Do what you will with passwords, but there must be a non-blank password on every login.
10. If any individual wishes to have a folder or folders that are confidential, that individual must have a different password than everyone else, and the password must be kept secret.
11. Passwords on Windows XP ARE case-sensitive. The best passwords are those which are at least 8 characters and include capitals, lower case letters, numbers and punctuation characters. The password can have a mnemonic such as a phrase represented by the characters, such as Oicu812! (read it.) The best passwords of all are those with a completely random set of characters, numbers and punctuation, such as R23#@bbk. Set the complexity of your passwords according to your need for security from outsiders. If you have a snoopy employee who has hacker tendencies, you may need complex passwords for internal security as well. The greater the need for confidentiality, the better the passwords must be to protect it.
12. In order for a folder to be accessible to others, that folder must be shared. Sharing a folder is as simple as right-clicking on it, clicking on Sharing, and then giving it a share name. In the most general terms, if a folder is shared on any PC using default settings, that folder can be accessed by any other computer with a matching login and password. So, in our example, if John shares a folder on PC01, then that folder is accessible on any other PC on the network as long as it has a login of John with a password that matches John's password on PC01.
13. It is possible to limit sharing of a file to only certain individuals. However, experience has shown that limiting sharing access to a folder as a means of providing security causes a lot of problems. It is much better to set sharing wide-open even for a confidential folder, and then control access through **security** settings on the folder and not through sharing settings.
14. Windows, unfortunately, supports "nested shares". In other words, it allows you to share a folder, and then subsequently share one of its sub-folders. However, sharing a folder means that EVERY subfolder is already available automatically. Nested shares are a mess and create a lot of confusion. It is better to just operate as though once a master folder is shared, ALL of its subfolders are available and do not need to be shared separately.
15. If there is a folder on the server which contains confidential information that should not be made available to all employees, then that folder should be moved OUT OF any master

folder which is already shared. Then the confidential folder is shared separately, and folder security is set for the folder and its contents that limit access to certain logins only. As long as the logins match between PCs, though others may be able to map the folder to a drive, only the authorized user(s) can actually open the folder, view its contents and manipulate its files. This approach is suitable for Quickbooks, Quicken or other financial or HR data. It can also be used to keep Outlook files on the server, although running Outlook on a network. PST file has its own set of challenges. (Specifically, if the network is down, the user will get an error message when running Outlook and the program will not start.)

16. The best way to make shared folders available across a network is through "mapped drives". A mapped drive is simply a shared folder on another computer, mounted to this computer as a particular drive letter such as H: or J: or Z:. If mapped drives are properly set up, they will "remount" themselves every time the computer is started or rebooted.
17. The best way to map drives is through a simple login script that is run on each PC when the user logs in. The script is a program in a text file that tells the computer to mount a particular folder on another computer or the central server, as a particular drive letter. The mapping command is "net use". The syntax is as follows:

    net use \\server\datafolder N:

    This command will cause the shared Data folder on the server to be "mounted" to this PC as the N: drive. Then, any file in the Data folder can be accessed as "N:\filename"
18. It is often customary to share folders that contain company information that employees need access to, and then to allow employees to store other files in their own My Documents folder. Storing of personal files into a company shared folder should be discouraged because file security is a problem and because files so added will increase the backup burden. It is easy to set up a separate folder for each employee, which only he/she has access to, on the server, in a place that can be backed up or not, as preferred.
19. It is also possible to set each machine so that the user's My Documents folder actually resides on the server instead of their local C: drive. Then, anything they save that is not part of the shared company data still gets stored on the server, transparent to the user. This also offers the advantage that if employees swap computers for whatever reason, there are never any files to move from one computer to the other because all files are on the server.

Conclusion

The process of setting up a functional and trouble-free peer-to-peer file sharing configuration sounds like a lot of work, but it really boils down to good habits on the part of the technician in setting it up. These procedures become second nature, and thus experimentation is reduced and the configuration becomes much more likely to work from the start. Once implemented, simple adherence to these rules about login consistency, avoiding nested shares and unnecessary shares, etc. will minimize the amount of maintenance required in order to make file sharing productive and reliable.

On the final page are the Ten Commandments of File Sharing. Remember them and observe them always.

The Ten Commandments of File Sharing

1. **Thall shalt use Windows Professional exclusively and shall eschew and have no portion or share with Home or 9X operating systems.**
2. **Thall shalt abolish Simple File Sharing and never give it a foothold or a portion.**
3. **Thall shalt choose a workgroup name and never stray from it.**
4. **Thall shalt suffer no login to exist without a password.**
5. **Thall shalt make passwords difficult to guess, and share them not among users.**
6. **Thall shalt make the logins match on any two machines which intend to have communion.**
7. **Thall shalt not create nor suffer to exist, any nested share.**
8. **Thall shalt not attempt to secure folders by limiting their share, but shall instead secure them through folder security.**
9. **When an employee departeth, thall shalt strike his name, his login and his password from every computer on which it dwells, and especially from the server.**
10. **Remember your firewall and keep it secure, save for imparting to it the knowledge of file and printer sharing.**