Using NT Shares

BY GUY C. YOST

In the June issue, I examined how NTFS file and directory-level security can be used to protect your network file resources while providing users just enough access to be productive. Simply assigning NTFS permissions to allow access to a directory isn't enough for the user to actually connect to and start using it, however. Directory-level "shares" must be established in order for clients to connect to these central resources.

The steps involved to establish a share are very straightforward; however, before we proceed, there are a few things you should know about how MS networking supports share browsing.

SHARE NETWORKING

First, MS networking traditionally uses the peer-to-peer NetBEUI (pronounced net-booey) protocol to connect network resources between clients and servers. NetBEUI is short for NetBIOS Enhanced User Interface and is an enhanced version of the NetBIOS (Network Basic Input Output System) protocol used by network operating systems, most notably of MS descent. NetBIOS is not routable and is therefore being used less as router-connected networks are becoming the norm. You can use TCP/IP or Novell's IPX/SPX (both routable protocols) to carry NetBIOS requests across LANs, routers and even WANs, but keep in mind that NetBIOS is still being used in an encapsulated form. The reason I mention this is because the most common problem that occurs in setting up an MS network is forgetting that NetBIOS must be enabled over TCP/IP or IPX in order for MS clients to see MS server resources. To ensure NetBIOS is being used with your networking protocol, start Control Panel, bring up the Networking applet, highlight your networking protocol in the list of configured network resources,and click on the Properties button (as shown in Figure 1). You'll see a tab labeled NetBIOS, and on that tab there will be a check-box that allows you to enable NetBIOS over the selected protocol.

Note from Figure 1 that the "Client for Microsoft Networks" must be installed to allow a client to access MS network server resources, and "File and printer sharing for Microsoft Networks" must be enabled to allow the resources of that computer to be accessed by other users on the network. I'm describing very general and standard MS networking set up here, and once the set up is configured, you'll be able to "browse" the network for printers and directories on other computers from Network Neighborhood or the File and Printer Manager utilities.

Note: *In order for TCP/IP to be used in a peer-to-peer MS network environment, you can configure a WINS server to resolve computer names to IP addresses or create computer entries in the C:\WINNT\SYSTEM32\DRIVERS\ETC\LMHOSTS file. There is a sample LMHOST file called LMHOSTS.SAM in the ETC directory to use as a template. After making changes to the file, save it without the SAM extension.*

CREATING THE SHARE

The process of establishing a share is simple, but you should be aware of some parameters and caveats. First, shares can be established using either of the following methods:

Figure 1: Configuring Networking to Support Shares

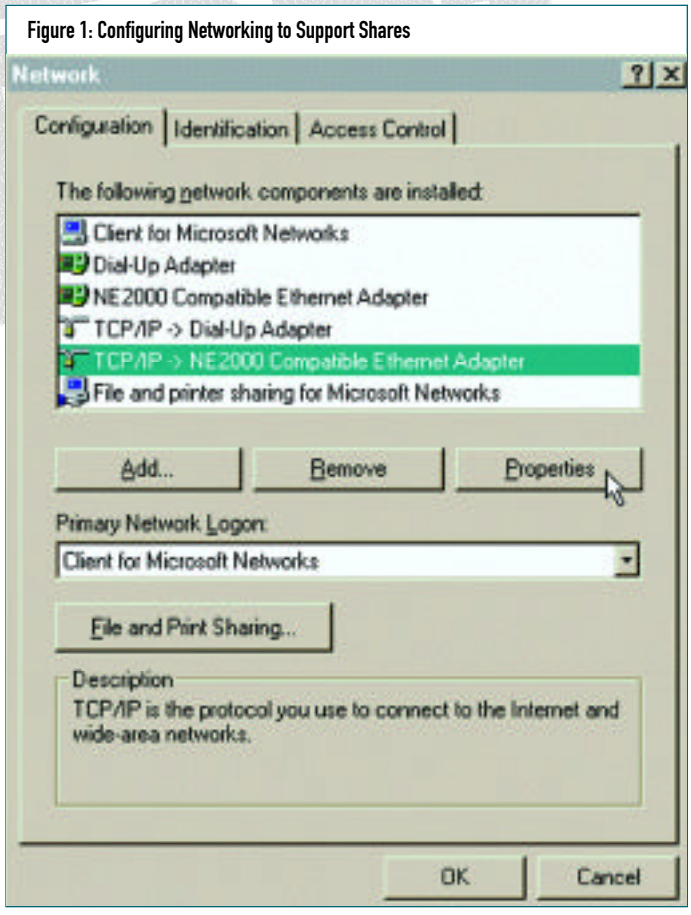


Figure 2: Setting up Directory Shares

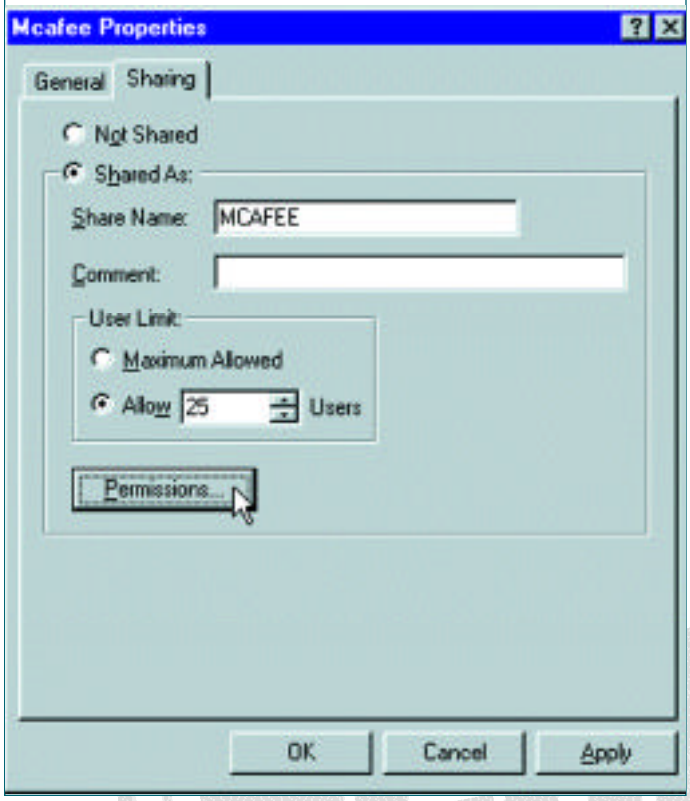
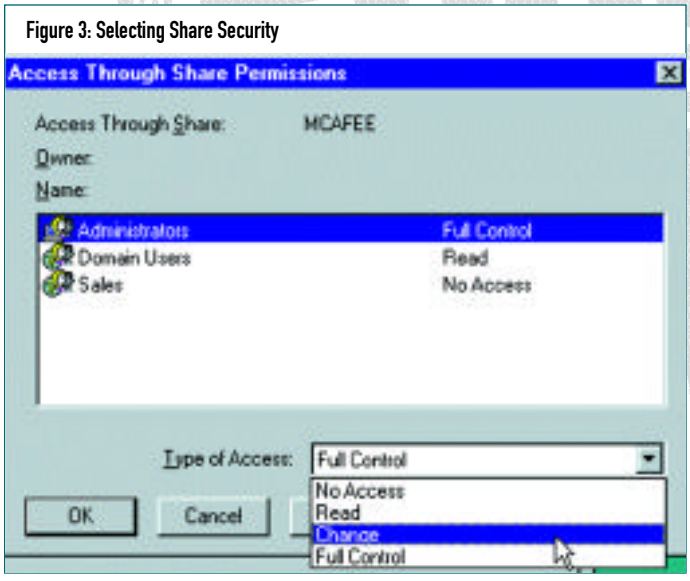


Figure 3: Selecting Share Security

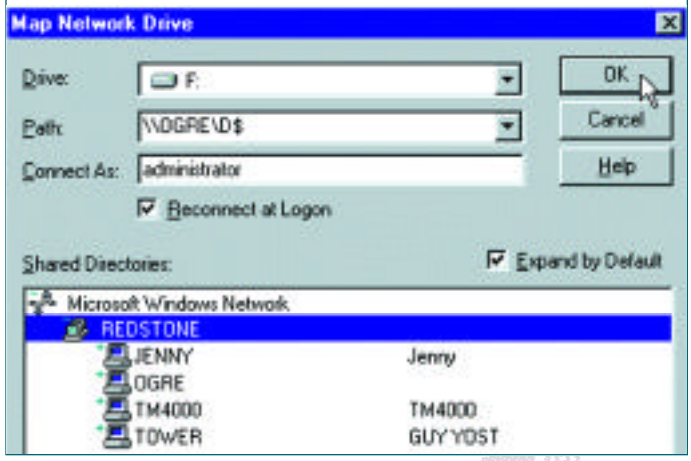


1. Using "My Computer" or Explorer (in 95/98 or NT 4), right click on the drive, directory or program group you want others to access.

2. Select "Sharing" from the drop-down menu to bring up the sharing configuration menu.

3. Using File Manager (in NT3.51/WinFrame/Windows 3.11 or NT 4), highlight the directory and select "Disk" from the main menu. Click on "Share As" from the Disk drop-down menu. In either case you will be presented with a Share Properties screen similar to Figure 2.

Figure 4: Using Administrative Shares



By default, the directory name will be the shared name; however, you can change it for security reasons (so users won't know actual names of directories on the server). Also, be aware that some older 16-bit applications will have trouble accessing shares whose formal path names are more than 20 characters. Note that NT supports built-in metering by allowing you to specify the maximum number of concurrent users that can access the share.

Note: *To remove a share, simply highlight the previously shared directory and select "Not Shared" from the top of the screen shown in Figure 2.*

SHARE SECURITY

Compared to the options available with file-level NFTS permissions, configuring share-level security is much simpler. From Figure 2, click on the Permissions button to bring up Figure 3.

As shown, a share can be accessed using Read, Change or Full Control. Intuitively, Read grants read-only access to the share; Change allows files to be created, deleted and have content updated; while Full Control allows all Change actions as well as administrative control (to change share properties). "No Access" works the same as with NTFS in that it overrides other permissive factors. For example, the Sales group in Figure 3 would not have access to the share even though users in Sales are also members of Domain Users.

The way that NTFS and share-level security work together, however, is not as intuitive. Assume that the NTFS rights to the shared MCAFEE directory are set to Change (RWXD) for the Domain Users group. Yet the share-level access is set to Read. What are Domain Users ultimate access permissions? Read only. In this case, the share-level permissions "block-out" the (WD) permissions, even though they're granted at the NTFS directory level.

In a second example, assume the reverse is true. That is, the share-level access is set to Full Control and NTFS permissions are set to Read only. What are the ultimate rights? Read only, again. This may seem confusing at first — the first example having the share rights prevail and the second example having the NTFS permissions prevail — but it makes sense if you view the share-level permissions as having the ability to filter out NTFS rights but not allow more NTFS rights than what are assigned at the directory level.

ADMINISTRATIVE SHARES

By default,NT has "administrative"shares established at the root directory for each drive on the server. These shares are uniquely

identified by a $ after the drive letter. For example, I can connect to the D: drive on a server called Ogre by specifying the path: \\OGRE\D$ as shown in Figure 4. These shares allow for administrative access (provided you're logged into the NT domain as Administrator and can provide the administrative password) even if a formal user "share" is not yet established.

SUMMARY

Shares are needed for users to access network resources. Ultimately share-access control answers to NTFS permissions at the lowest level, yet share permissions can be used as a type of "filter" by blocking NTFS permissions. The key to using NTFS and share-level access together is understanding that the ultimate permissions a user will experience will be the lesser of the NTFS or share permissions. ts

NaSPA member Guy C. Yost is the owner of Redstone Consulting, an IT management consulting firm in New York. He has authored several books on networking for Que Publishing, including Learning NetWare 4.1, and NetWare 4.1 SmartStart, and contributes to Technical Support magazine as an author, columnist and technical editor. He can be reached at (518) 674-5606 or gyost@logical.net.