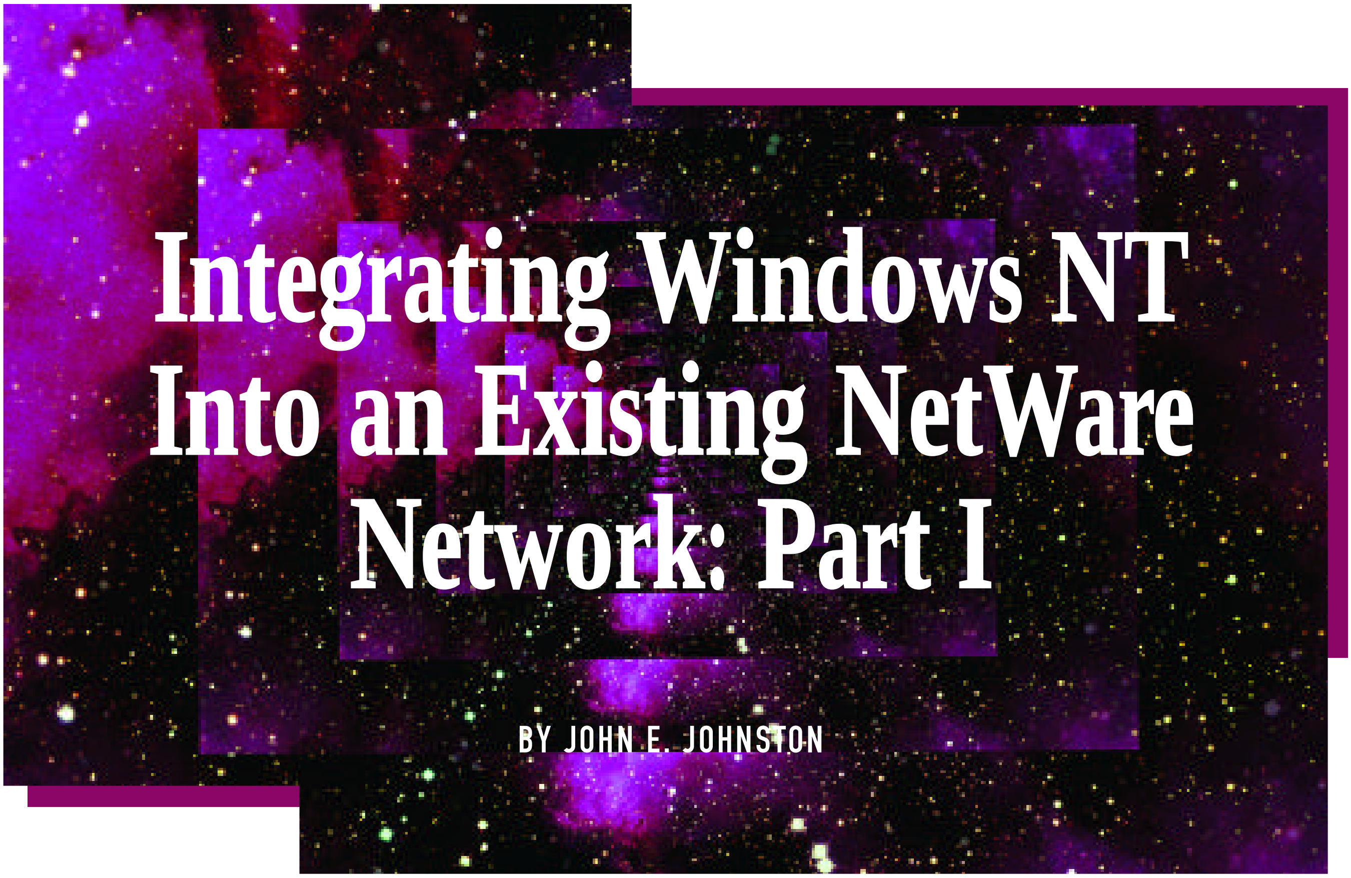


Integrating Windows NT Into an Existing NetWare Network: Part I

BY JOHN E. JOHNSTON

It is very easy to set up a Windows NT network. However, with this ease of implementation comes a price. In fact, it is so simple to get a Windows NT network up and running that without realizing it, you could easily set up an extremely unmanageable, poorly performing network.

I should know; I've been there and am now in the process of straightening it out. Here's my story: I manage a group of network technicians in charge of a 1,400-node LAN/10-site WAN. My company was primarily a NetWare shop until we decided to implement the Microsoft Exchange Email system. Exchange requires the use of a Windows NT network, so we built one. We installed NT 4.0 on a file server, making it a PDC (Primary Domain Controller), which was a good thing. We also installed another NT 4 Server as a BDC (Backup Domain Controller), which also turned out to be a good thing. Knowing that the NT network would grow rapidly, we decided to dedicate the PDC and BDC machines as domain controllers (i.e., no other applications are run on these two machines). Next, we installed Exchange on yet another NT Server. It took us one day to install these three servers.

Then, we began installing the Outlook 97 mail client on our workstations. This included the preparation of the client workstations on which we installed the Novell IntranetWare Client for Windows 95 along with the Microsoft Client for Windows. We reasoned that by implementing both the NetWare and Windows Networking clients we could get the most performance and flexibility out of both networks by implementing the native clients for each network. I still stand behind that reasoning, and this strategy has worked well for us. Dual clients do increase the complexity of any network, but, in many instances, this added complexity is worth the price.

While we were adding the Microsoft networking client to our Windows 95 workstations, we made our first implementation mistake: We implemented the TCP/IP protocol on each workstation (a good thing) but assigned hard coded addresses to each (a bad thing). We now administer 1,400 TCP/IP addresses manually and are in the process of implementing a DHCP server to solve this problem.

As expected, as soon as we announced that we were implementing Exchange, the requests for access to the mail system became overwhelming. We now have approximately 400 users on the Exchange system. After implementing the first 200 clients, we found that performance degraded on the entire LAN. That's when we uncovered our second implementation mistake; we chose to enable the default protocols on the NT Servers and on the Windows 95 clients that included NetBEUI. The NetBEUI traffic was consuming large chunks of our LAN bandwidth.

We are currently in the process of web enabling several of our legacy applications. Web browsers rely on the WinSock API. WinSock applications need DNS name resolution, so to implement web-enabled applications on a LAN you need a local DNS. Rather than playing catch up now by implementing a DNS into our existing network, we should have implemented the DNS when we first installed the PDC and BDC. That was mistake number three.

The fourth (and final…I hope) mistake was our lack of a WINS server. The first time we tried to implement Exchange at one of our remote sites we discovered that we needed a WINS server. It would have been much simpler to implement this server when the Domain was first created rather than shoehorning it in later.

On a positive note, we did do several things right, including implementing a single NT domain. The security, complexity, and cost of implementing multiple domains are not for faint-hearted or frugal network managers. Our single domain has served us well in our LAN environment and for our WAN sites. We also implemented rock-solid backups on the NT side of our network. We run full backups of all of our NT Servers nightly using ARCServe for NT. We utilize the ARCServe Exchange add-on product to backup our Exchange mailboxes. ARCServe is also used to backup our NetWare file servers.

Well, enough of my story. My goal in writing this series is to pass on some knowledge I learned at the school of hard knocks. I will show you how to implement the components that we are using to clean up our mess. Keep in mind that my group's objective is to provide the best possible performance and flexibility of both the NetWare and NT networks, which run independently over our wires. Not unlike most departments, my group also faces budgetary issues. We attempt to provide the best service to our end users while keeping costs under control. We chose not to implement the NT Gateway Services for NetWare (GSNW) because of its performance hit and we also chose not to implement NDS for NT because of its cost and complexity.

This series is written for network administrators who currently have NetWare installed and deployed throughout their organization and who now need to deploy Windows NT resources to their end users. Microsoft networking concepts and components can be quite difficult to understand, especially for entrenched NetWare administrators. Microsoft uses a completely different method (compared to Novell) to provide networking services. This series will help bridge the differences between the two networks and show you how to integrate a Windows NT network into your existing NetWare environment.

> This series is written for network administrators who currently have NetWare installed and deployed throughout their organization and who now need to deploy Windows NT resources to their end users.

Some of the topics that will be covered in this series include:

- **Thinking NT:** Here we will examine the various components of a Windows NT network, including Domains, machine names, user names, shares, and the Universal Naming Convention (UNC).

- **Implementing Networking Components With NT 4.0:** The full-scale implementation of a Windows NT network requires several support components. These components make your network easier to administrate and troubleshoot. In this section I will demonstrate how to set up the following network support components using Windows NT Server 4.0:

  • Domain Name System (DNS)
  • DHCP
  • WINS

- **Client Considerations:** This section will show you how to configure Windows 95 and Windows NT Workstations to access both your NetWare and NT networks.

- **The NET Command:** The NET command is an invaluable tool in setting up, troubleshooting, and administering your network. We will explore the NET command in detail.

- **Windows NT Workstation Profiles:** Dealing with Windows NT Workstation profiles can be a frustrating endeavor. This section will show you how these profiles work and how you can tame the profile beast.

- **Printing:** I will conclude this series with a discussion on printing. I will explore how you can share both NetWare and NT networked printers.

THINKING NT

Before you attempt to implement a Windows NT network, you must shift your thinking to the Microsoft way of networking. Failing to become acquainted with the way Microsoft "thinks" will result in frustration and a poor implementation. For all of you NetWare administrators, you must keep this point in mind when learning the basics of Microsoft networking: Microsoft networking was derived from a peer-to-peer base while NetWare was developed using a client/server model.

Domains

If you are implementing a corporate network you should implement the Microsoft Domain model. Domains allow you to control security centrally. So, what exactly is a domain? A domain is a collection of Windows NT Servers and Windows NT Workstations that are centrally managed. Now we are beginning to see how the peer-to-peer roots of Microsoft networking come into play. Domains allow you to exploit the strengths and resources of all of the NT-based machines connected to the network. This includes NT Workstations residing on employees' desks. Compare this to NetWare. NetWare will allow you to centrally control file servers; the computing power residing on the employees' desks is not controlled and exploited by the network.

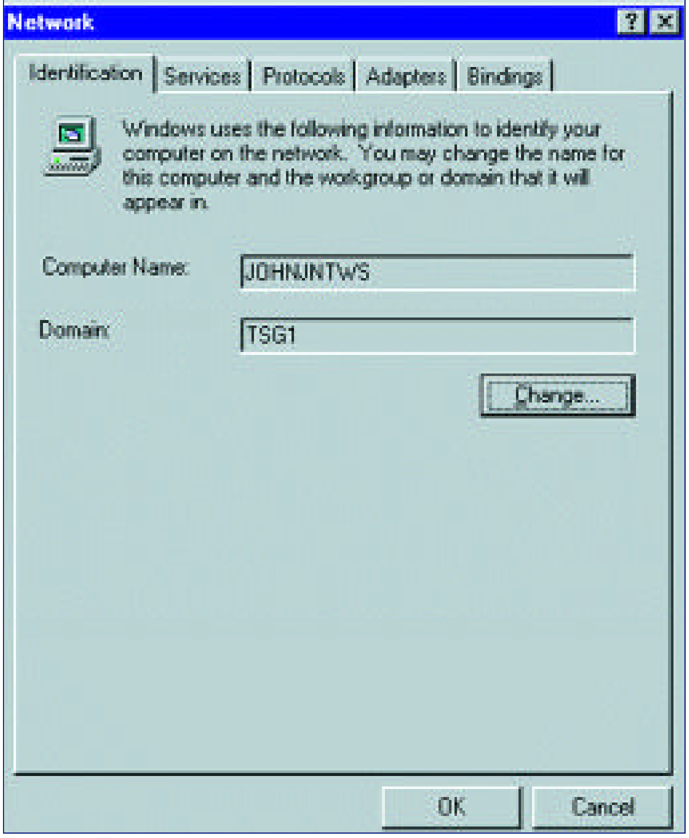
Note: *Windows 95 workstations are not part of the Windows NT domain. This is one of the confusing aspects of Microsoft networking and the Windows NT domain. The domain acts like a workgroup for Windows 95 and DOS-based workstations.*

Each domain requires a PDC and a BDC. These computers hold (and replicate) the security database. For more information on NT Domains, please refer to the following ***Technical Support*** articles: **NT Insights** "Understanding NT Domains" in the November 1997 issue and **NT Insight**s "NT Domains and Wide Area Networking" in the December 1997 issue.

Machine Names

Each machine that participates in an NT network must have a machine name. Machine names can be up to 15 characters in

Figure 1: All Machines in an NT Network Must be Named

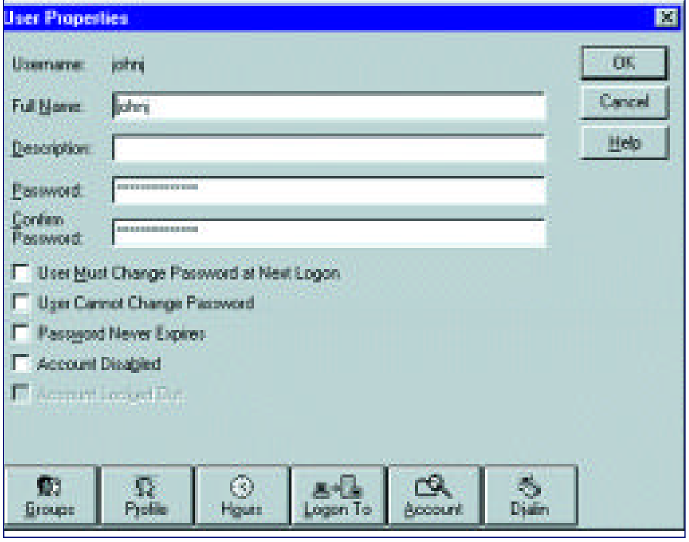


Windows uses the following information to identify your computer on the network. You may change the name for this computer and the workgroup or domain that it will appear in.

Computer Name: JOHNJNTWS

Domain: TSG1

Figure 2: User Manager for Domains



Username: johnj

Full Name: johnj

Description:

Password: **************

Confirm Password: **************

□ User Must Change Password at Next Logon

□ User Cannot Change Password

□ Password Never Expires

□ Account Disabled

□ Account Locked Out

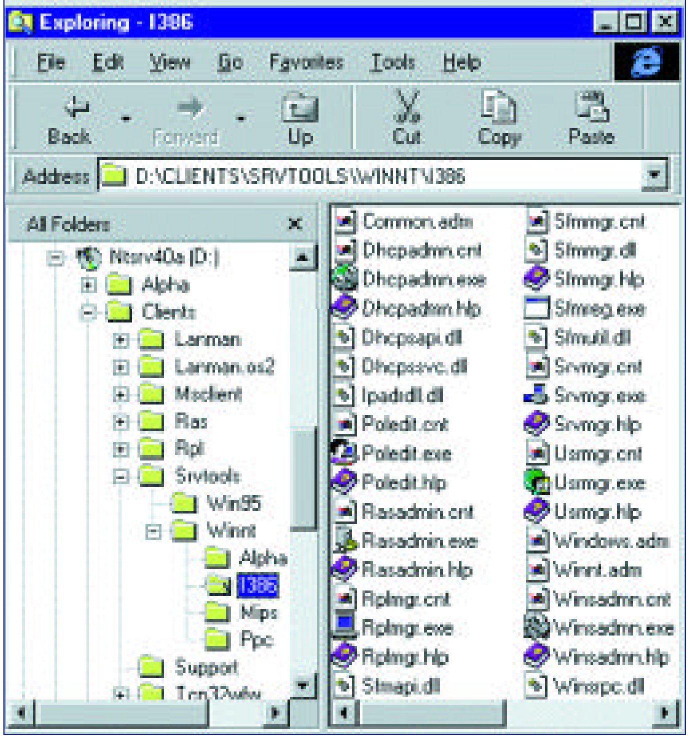
length. It is common practice to use corporate inventory numbers for these machine names. Machine names are specified in the Network applet from within the Control Panel. Figure 1 shows the machine name for a Windows NT 4.0 Workstation.

User Names

Just as with a NetWare network, all users in an NT network must be assigned a user name. This is done in the "User Manager for Domains" tool. Figure 2 shows a sample User Manager screen shot.

When implementing an NT network, you will become very familiar with the User Manager for Domains utility. This utility is only available under Windows NT Server. You may notice that Windows NT Workstation has a scaled down version that is simply called "User Manager." This version of User Manager can only administer local accounts on that workstation. As a network administrator, you should install the User Manager for Domains on your Windows NT Workstation. This saves you the trouble of having to go to your domain controller(s) to administer domain user accounts. To install User Manager for Domains on a Windows NT Workstation, perform the following:

Figure 3: Copying the NT Ser ver Tools to a Windows NT Workstation

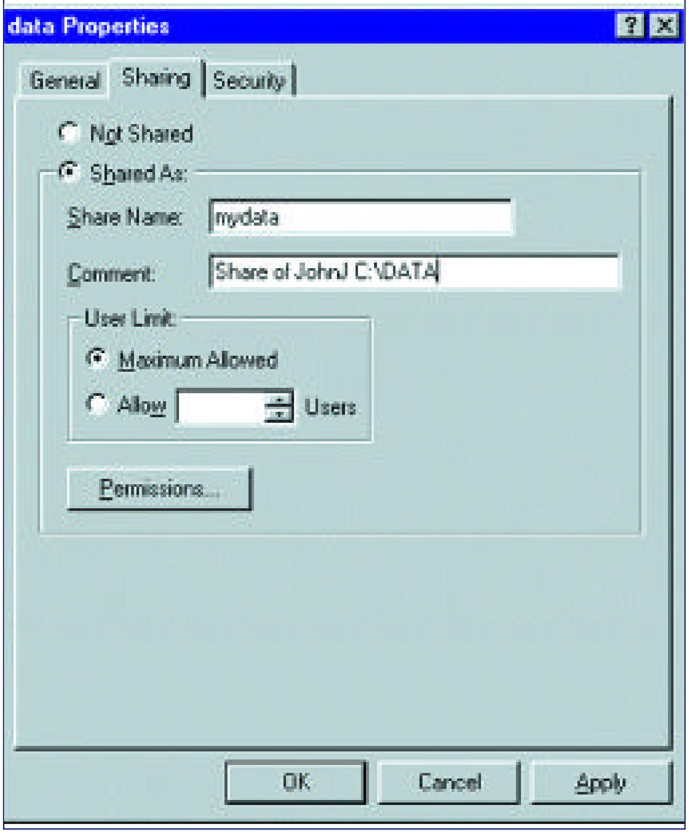


Address: D:\CLIENTS\SRVTOOLS\WINNT\I386

> **Before you attempt to implement a Windows NT network, you must shift your thinking to the Microsoft way of networking. Failing to become acquainted with the way Microsoft "thinks" will result in frustration and a poor implementation.**

1. Insert the Windows NT Server CD-ROM in your NT Workstation CD-ROM drive.
2. Using the NT Explorer, browse to the \CLIENTS\SRV TOOLS\WINNT\ platform, as shown in Figure 3.
3. Copy the files in this directory to a directory on your local hard drive.
4. Create a shortcut for the Usrmgr.exe file.
5. While you're at it, you should create shortcuts for the other utilities in the directory as well.

Figure 4: Creating a New Share Using the NT Explorer



○ Not Shared
● Shared As:
Share Name: mydata
Comment: Share of JohnJ C:\DATA
User Limit:
● Maximum Allowed
○ Allow Users

Share Names

Share names have no corresponding NetWare counterpart that you can use to help you grasp the concept. Share names are names that allow you and your users to share computer resources over the network. NT Server resources, such as printers, CD-ROM drives, and/or directories can be shared with your end users. Your end users can also "share out" the resources on their NT Workstation computers.

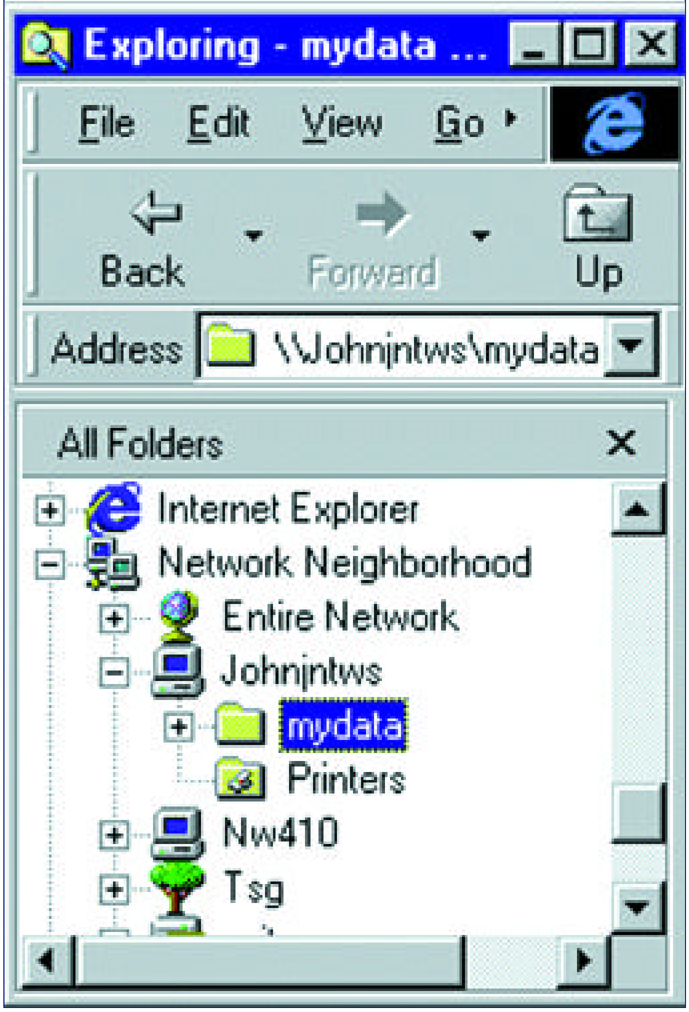
Most NetWare administrator cringe at the thought of end users sharing out the resources on their workstations, and for good reason. Left unchecked, the misuse of shares can leave your users' programs and data at the mercy of inside and outside hackers. There are ways to tighten NT network security, but this is a topic for a future series.

The best way to understand a share name is to see one being created and used. Let's say that an end user wants to share the C:\DATA directory on his NT Workstation's hard drive. The following steps are required to accomplish this:

1. From the NT Explorer, browse to and highlight the C:\DATA.
2. Click on the right mouse button, and then click on "Sharing."
3. Click on the "Share as" button.
4. Using Figure 4 as an example, in the "Share Name" field, enter the name you would like to use as the share name and then click on OK.

Shares can also be created using the "NET SHARE" command prompt command. A future article will explore this command in detail.

Figure 5: Browsing the Network Neighborhood to our Newly Created Share



Address: \\Johnjntws\mydata

From another NT Workstation or server, you will be able to see the share just created. Figure 5 shows a screen shot of the NT Explorer browsing to the new share just created. You may also utilize the "NET USE" command prompt command to provide access to shares. The "NET USE" command will be discussed in Part II of this series.

The Universal Naming Convention

Notice the name " \\Johnjntws\mydata" that is contained in the "Address" field of Figure 5. This is known as a universal naming convention (UNC) name. UNCs are used extensively in NT networks. Again, looking at Figure 5, the first two slashes indicate that the name to follow is a machine name. In this example, Johnjntws is the name of an NT Workstation machine. The \mydata part of the UNC specifies a share name, not a directory name.

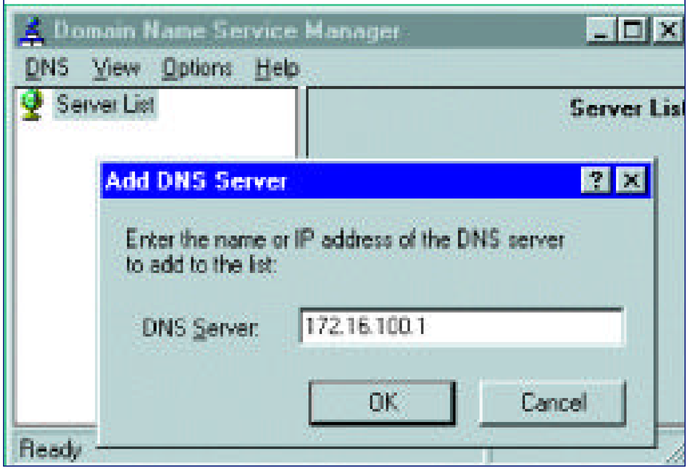
IMPLEMENTING NETWORKING COMPONENTS WITH NT 4.0

You will find that implementing network components, such as the DNS and WINS under Windows NT Server, is relatively simple to do. Nevertheless, it is always nice to have a step-by-step guide to help you get started. In this section I will show you how to implement the DNS, DHCP, and WINS components under Windows NT 4.0.

Implementing a DNS with Windows NT 4.0 Server

Sooner or later, you will need a DNS for your network. As more and more applications become web-enabled, it's just

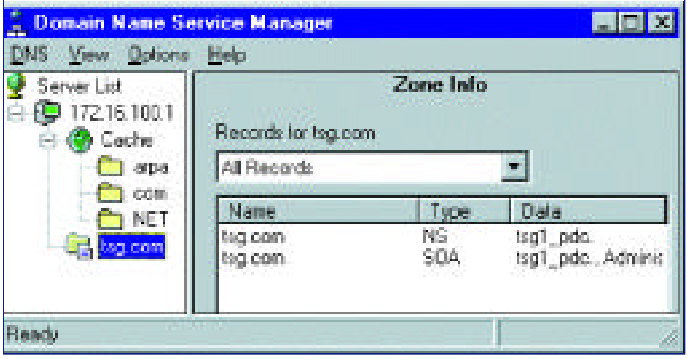
Figure 6: Entering the IP Address of the DNS Server



Enter the name or IP address of the DNS server to add to the list:

DNS Server: 172.16.100.1

Figure 7: DNS Manager Showing New Domain



Records for tsg.com

All Records

Name	Type	Data
tsg.com	NS	tsg1_pdc.
tsg.com	SOA	tsg1_pdc., Adminis

a matter of time before you find yourself implementing a DNS. Windows NT 4.0 includes the DNS function. The actual implementation of the Windows NT DNS function is relatively simple to perform. In the following example, we will set up a small domain named TSG.COM. This domain uses a class B network number of 172.16.0.0. This domain contains a PDC named TSGPDC.TSG.COM that resided at address 172.16.100.1 and an FTP server named FTP.TSG.COM at address 172.16.100.101. The actual DNS service will reside on the PDC machine.

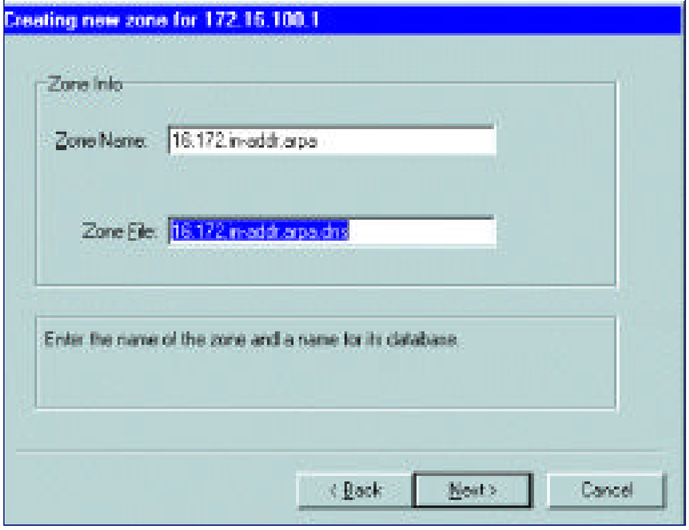
We must first install the DNS service on the PDC. To do this, perform the following steps:

1. Click on Start > Settings > Control Panel.
2. Double-click on the Network icon.
3. Click on Services > Add.
4. Choose the Microsoft DNS Server, and then click on OK. Files will then be copied from your Windows NT Server CD-ROM.
5. After the service has been added, you will be prompted to restart your server.

After your server restarts, you are ready to configure the DNS service:

1. Click on Start > Programs > Administrative Tools (Common) > DNS Manager.
2. Click on DNS > New Server.
3. Enter the IP address of the local PC as shown in Figure 6 and then click on OK.

Figure 8: Creating the Reverse Lookup Zone



Zone Name: 16.172.in-addr.arpa

Zone File: 16.172.in-addr.arpa.dns

Enter the name of the zone and a name for its database.

It is now time to create a new domain (also known as a zone). From the DSN Manager, perform the following:

1. Click on DNS > New Zone.
2. Click on Primary, and then click on Next.
3. Fill in the name of the zone (in this case TSG.COM).
4. After entering the zone name, press the TAB key. After doing this, the "Zone file" field will be filled in for you.
5. Click on Next, and then click on Finish.

When completed, you should see a screen similar to Figure 7.

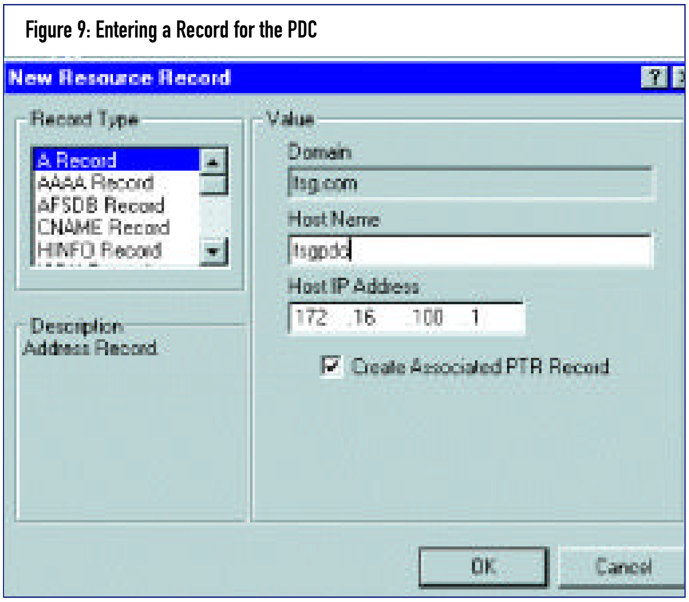
We must now create a special zone for reverse DNS lookups. This takes a bit of explanation. Our domain, TSG1.COM, resides in a class B IP network (172.16.0.0). The reverse DNS lookup zone must be created and named 16.172. Notice the reverse numbering of the IP address. To create the reverse lookup zone, perform the following from the DNS Manager utility:

1. Click on the server 172.16.100.101 to highlight it.
2. Click on DNS.
3. Click on New Zone.
4. Click on Primary, and then click on Next.
5. Enter 16.172.in-addr.arpa in the Zone Name Field, and then press the TAB key. You should see a panel similar to Figure 8.
6. Click on Next, and then Finish.

We are now ready to add records for the PDC machine (the DNS is also installed on this machine) and the FTP server that is located at address 172.16.100.101.

1. Right click on TSG.COM and select New Record.
2. Make sure the "A Record" entry is highlighted in the Record Type box.
3. Enter the name and IP address as shown in Figure 9.
4. Click on OK to create the A record for TSGPDC.TSG.COM. Since the "Create Associated PTR Record" was selected (see Figure 9) the reverse lookup record was also created for us.

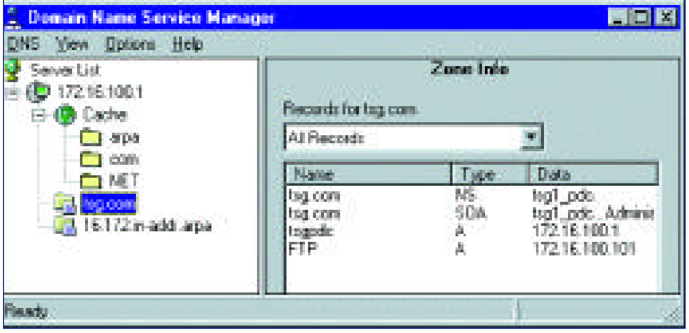
Figure 9: Entering a Record for the PDC



A Record
AAAA Record
AFSDB Record
CNAME Record
HINFO Record

Domain: tsg.com
Host Name: tsgpdc
Host IP Address: 172 .16 .100 .1
Description: Address Record
☑ Create Associated PTR Record

Figure 10: DNS Configuration After Adding the PDC and FTP Machines

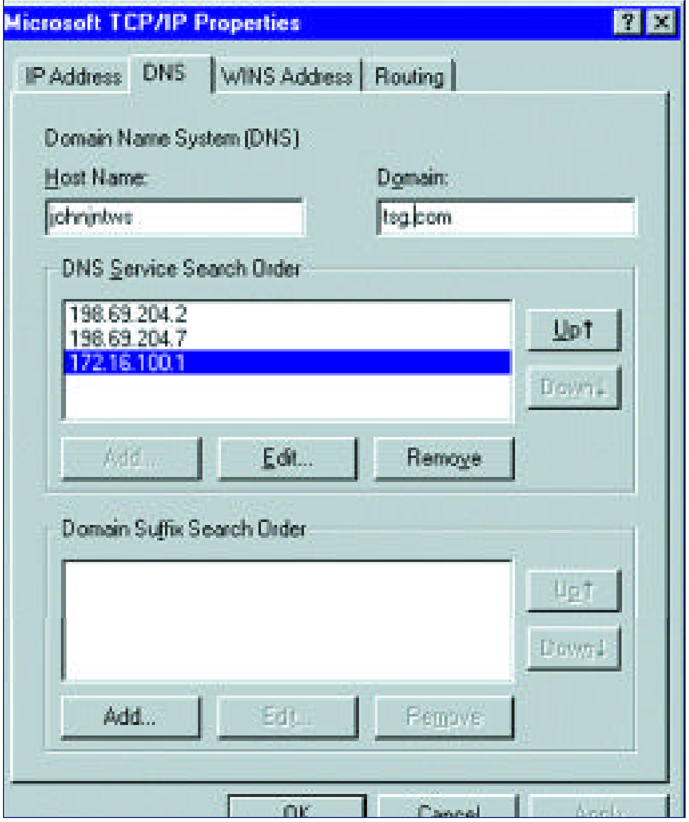


Server List
172.16.100.1
Cache
arpa
com
NET
tsg.com
16.172.in-addr.arpa

Records for tsg.com
All Records

Name	Type	Data
tsg.com	NS	tsg1_pdc
tsg.com	SOA	tsg1_pdc., Admini
tsgpdc	A	172.16.100.1
FTP	A	172.16.100.101

Figure 11: Adding the DNS to the Client Network Configuration



Domain Name System (DNS)
Host Name: johnjntws
Domain: tsg.com

DNS Service Search Order
198.69.204.2
198.69.204.7
172.16.100.1

Domain Suffix Search Order

Follow the above process to add other machines to your DNS. In this example, a record for the FTP server was added, resulting in the configuration shown in Figure 10.

Now we need to point our workstations to the newly created DNS. To do this, modify the TCP/IP protocol form the Network icon, as shown in Figure 11. After adding the local DNS to your workstation, reboot and test by pinging the DNS names just created.

CONCLUSION

There are many more options available in the Windows NT Server DNS service that were not covered in this article. You should spend some time getting acquainted with the DNS service before implementing it in a production environment. Part II will demonstrate how to install and configure DHCP under Windows NT Server 4.0. ts

NaSPA member John E. Johnston is manager of technical support and communications for a major hospital in Pennsylvania. He designs and maintains cross-platform local and wide area networks utilizing NetWare, OS/2, DOS, and Windows.