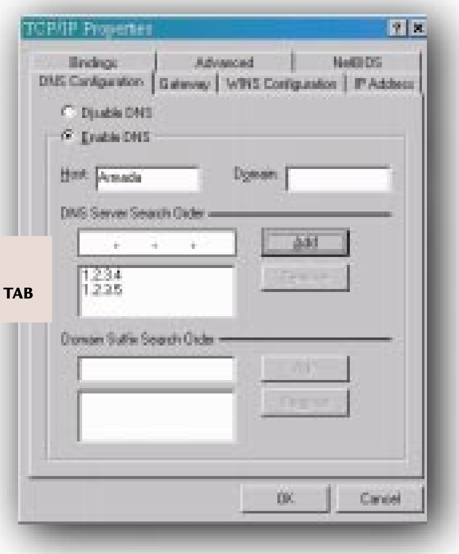
What's in a name?

A good naming scheme, with a DNS server, is the most efficient way to provide automatic addressing and naming services on a Windows network. Bob Walder shows you how to do it.

In a recent issue, we went into some detail on IP addressing and the use of WINS and DHCP to provide automatic addressing and naming services on a Windows network. Since then, I have received several emails asking me to do a follow-up piece on DNS in Microsoft environments — so here goes.

Domain Name System is the cornerstone of the internet, since it provides the means to turn all those long-winded IP numbers into equally long winded-names — but at least they are easy to remember. For instance, how many of you know the IP address of the Novell web server off the top of your head? Try dropping to a DOS prompt and type ping.www.novell .com. After a pause, you should see a reply from 137.65.2.11. If you had typed PING 137.65.2.11 in the first place, you would have got exactly the same result, but marginally quicker. That is because the first thing that happens when you try to PING a domain name is that it must be resolved by a DNS server.

The simplest way to provide name resolution in small networks is to use the HOSTS file. This is a text-based file which can be found on most TCP/IP systems, and which contains a simple list of IP addresses and the names that relate to them [Fig 1]. This file can name common systems both inside and outside an organisation and each address can have several names, usually a "formal" name followed by a number of less formal "nicknames" or aliases. Hence, in our sample HOSTS file, the marketing server can be referred to by its IP address of 10.1.1.2, its full name of dilbert. marketing.acme.co.uk, or by its shortened aliases of Dilbert or Marketing. While the use of HOSTS files is possible in smaller networks, they can have serious drawbacks in larger ones.



○ Disable DNS
● Enable DNS

Host: Armada   Domain:

DNS Server Search Order

1.2.3.4
1.2.3.5

Domain Suffix Search Order

►FIG 2 DNS CONFIGURATION TAB

The main problem is that a copy of the file must exist on each and every TCP/IP client which intends to refer to resources by name rather than IP address. This approach is obviously not very scaleable and presents systems administrators with a potential nightmare in a network with hundreds or thousands of clients. Ensuring that each and every HOSTS file is always up to date as network changes are made is bad enough, but there is also the temptation for users to create their own files with customised naming conventions, making it difficult for "hot desking" colleagues. Of course, it is possible to manage HOSTS files by keeping a master version on one of the central servers, and downloading it to clients automatically on a regular basis, but this approach, too, can have its problems in large distributed networks.

DNS provides for central control over names and IP addresses

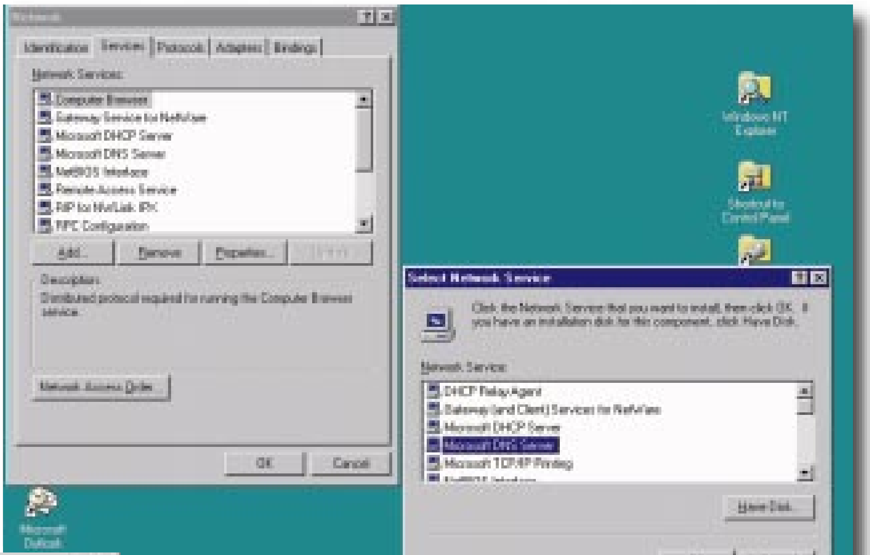
Obviously, such solutions will not scale in large organisations and certainly will not scale to the internet. The problem of internet naming has, to date, been largely satisfied by DNS which allows a computer that is registered to the internet to be uniquely identified by that name wherever it may be located. Because computers work with numbers rather than names, the second major function of DNS is to translate the unique host name into the appropriate IP address required in order to establish communications.

The use of DNS is certainly mandatory in some form if you wish to participate in the internet. However, a good naming scheme coupled with the implementation of DNS servers can also make life considerably easier for users of a large corporate TCP/IP network, even if it is not connected to the internet. DNS provides for central control over names and IP addresses and removes the need for individual HOSTS files — although these can co-exist quite happily where required. It allows control to be applied both in a distributed fashion and where it can be most effective, in local sites and divisions. The domain name protocol is quite complex syntactically, although its operation is straightforward. A

[FIG 1]

```
; Hosts
;
; IP address  name                          alias
;
127.0.0.0     loopback                      Bob
10.1.1.2      dilbert.marketing.acme.co.uk  Dilbert Marketing
10.1.1.3      dogbert.sales.acme.co.uk      Dogbert Sales
10.1.1.5      ratbert.accounts.acme.co.uk   Ratbert Accounts
10.1.1.10     bwalder.acme.co.uk            Bob
192.168.1.52  bgates.microsoft.com          Bill
```

host, given a name, asks the server for a name-to-address translation. If the name server does not possess the means to perform that translation directly, it will pass the request on to a server with a higher authority than itself. This process can be repeated until the request is satisfied, which will always happen unless the requested address was incorrectly specified or there is some unforeseen problem, such as a DNS server being temporarily unavailable. Those of you with internet connections will have one or more entries in the DNS tab in your Network configuration [Fig 2, p299]. This will provide you with everything you need to resolve all those addresses out there on the internet.


Identification | Services | Protocols | Adapters | Bindings

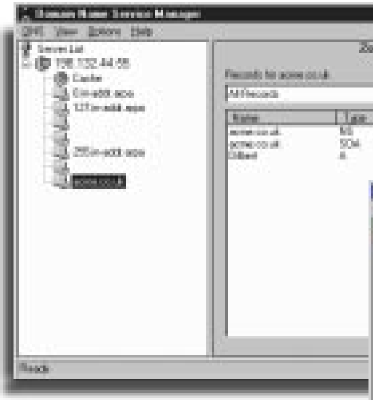
Network Services:
- Computer Browser
- Gateway Service for NetWare
- Microsoft DHCP Server
- Microsoft DNS Server
- NetBIOS Interface
- Remote Access Service
- RIP for NwLink IPX
- RPC Configuration

Description:
Distributed protocol required for running the Computer Browser service.

Select Network Service

Click the Network Service that you want to install, then click OK. If you have an installation disk for this component, click Have Disk.

Network Service:
- DHCP Relay Agent
- Gateway (and Client) Services for NetWare
- Microsoft DHCP Server
- Microsoft DNS Server
- Microsoft TCP/IP Printing

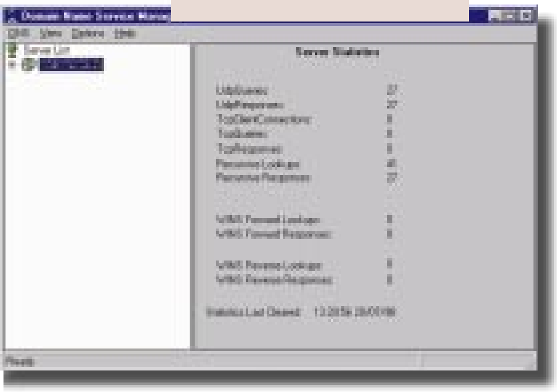

Domain Name Service Manager

Server List
- 198.132.44.58
  - Cache
  - 0.in-addr.arpa
  - 127.in-addr.arpa
  - 255.in-addr.arpa
  - acme.co.uk

Zone Info

Records for acme.co.uk: All Records

Name	Type	Data	
acme.co.uk	NS	compaq_NT40	co.uk.
acme.co.uk	SOA	compaq_NT40	co.uk.
Dilbert	A	10.1.1.2	


Domain Name Service Manager

Server List

Server Statistics

UdpQueries 27
UdpResponses 27
TcpClientConnections 0
TcpQueries 0
TcpResponses 0
Recursive Lookups 41
Recursive Responses 27
WINS Forward Lookups 0
WINS Forward Responses 0
WINS Reverse Lookups 0
WINS Reverse Responses 0
Statistics Last Cleared: 13:28:56 28/09/98

▲FIG 3 Adding the DNS Server
◀FIG 5 Adding Hosts
▼FIG 4 Creating your first DNS server

But what about those within your own organisation? You may have your own internal web server which you want to be known by the memorable name of DILBERT rather than the slightly less memorable address 10.1.1.2.

Luckily, it is easy to add your own DNS server in a Microsoft site, since the appropriate software is included with NT Server 4.0 (prior to this, you had to rely on a rather lacklustre offering in the Resource Kit for 3.51). One nice feature of the Microsoft product is that it hooks neatly into WINS if you already have WINS servers configured.

DNS configuration can be quite complex, unfortunately, so I am going to concentrate on the absolute basics to provide internal naming services.

> ***The use of DNS is mandatory in some form if you wish to participate in the net***

☛ **Call up** the Control Panel on the server and double-click on the Network icon.

☛ **Click Services,** Add, and select the Microsoft DNS Server [Fig 3].

☛ **Supply** the path to the installation files and reboot your server when finished.

☛ **Once the server** has rebooted, go to Start, Programs, Administrative Tools (Common) and the DNS Manager.

☛ **Click on DNS,** New Server and provide the IP address of your new DNS server. The database files are initialised and this address then appears in the Server List in the left-hand pane [Fig 4].

A number of zones are automatically created and can be ignored for now. Your first job is to create a zone to represent your internal network.

☛ **Highlight** the DNS server you have just created and click on DNS and New Zone.

☛ **Click** on Primary and then the Next button.

☛ **Give** the Zone a name (e.g. ACME.CO.UK), tab to the Zone file field and click on the Next button to accept the default file name.

☛ **Click** on the Finish button. The new Zone is created with some default entries.

All that is left is to enter the host names you wish to resolve. Taking our DILBERT example in the Domain ACME.CO.UK, we would simply highlight the Zone ACME.CO.UK and click on New Host.

Enter the host name (DILBERT) and the address (10.1.1.2), and click on Add Host. Your Domain should now look like the right-hand pane [Fig 5]. Now, include the address of your DNS server in the DNS configuration tab of all your clients (first in the list) and you're ready to go.

Refer to my advice on the use of DHCP in an earlier issue to see how you can make that change across all your clients in a matter of seconds. Now if you drop to the DOS prompt and type PING DILBERT.ACME.CO.UK you should receive a reply from device 10.1.1.2 — and away you go.

PCW CONTACTS

Bob Walder *can be contacted via the PCW editorial office (address, p10) or email* **networks@ pcw.co.uk**