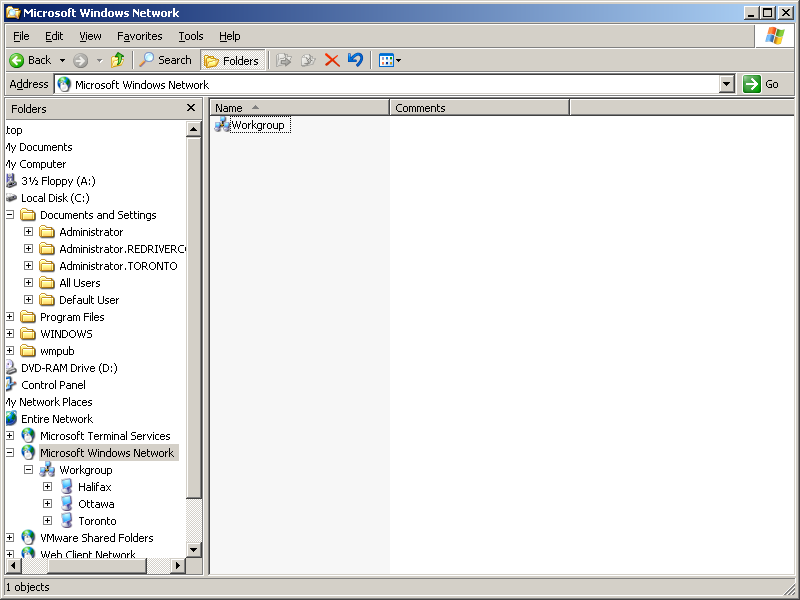
**MCSE 1 Lecture 5**

**Name Resolution**

**Name Resolution**

When you make reference to a computer by its name such as “ping ottawa”, the computer name **ottawa** must be translated into an IP address before the ping command can be executed. NetBIOS was the first form of name resolution. It has since been augmented and in many cases replaced by DNS.



When you open the Windows Explorer and expand My Network Places, the Explorer uses NetBIOS to query the network to find out what domains/workgroups exist. The Explorer must query each domain/workgroup to find out what hosts are in the networks.

In this example, Workgroup contains three hosts Halifax, Ottawa, and Toronto.

Fig. 1 NetBIOS allows Windows Explorer to find other computers

Figure 2 displays the Wireshark capture of the frames that are generated by opening the Windows Explorer as shown in figure 1. The second frame which is highlighted, shows Halifax at 10.1.1.1 is sending a broadcast (10.1.1.255) using the NBNS (NetBIOS Name Service) protocol, to request all hosts to identify themselves if they belong to the same workgroup.

You can see source and destination port is netbios-ns (137).

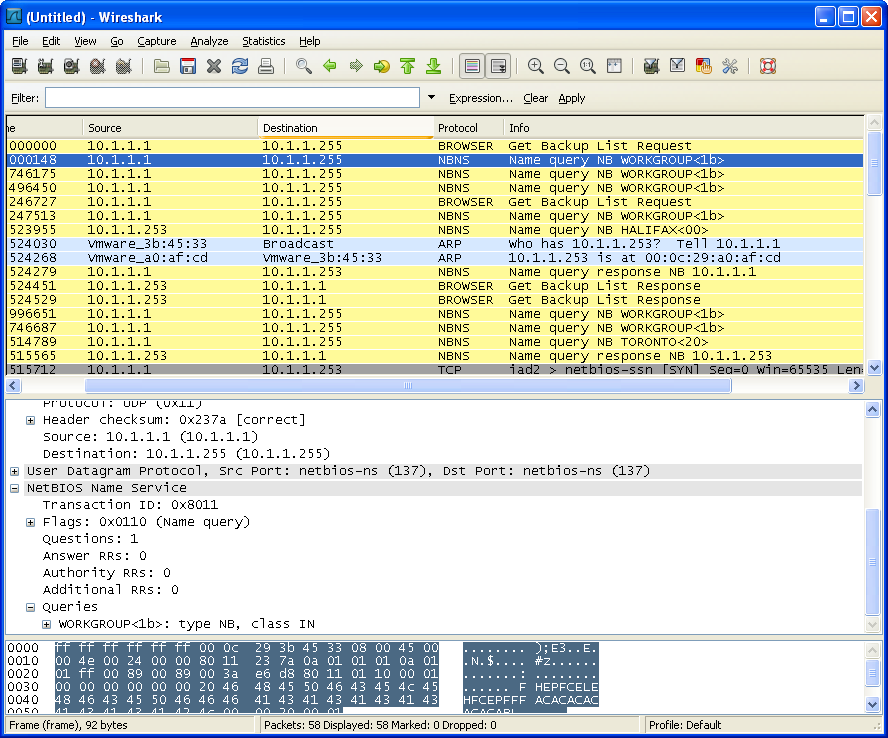


Fig. 2 Wireshark display of the frames generated by opening the Explorer

**NetBIOS names**

Operating systems prior to Win2000 used NetBIOS names for resolving IP addresses. More current operating systems will try to resolve a name with DNS before resorting to NetBIOS.

Many applications still use NetBIOS when communicating with other computers.

Peer-to-peer networks that are not running DNS will use NetBIOS for name resolution.

A NetBIOS name can be up to 15 characters for the name plus 1 byte for the type of service. You can Google “netbios service codes” if you want to see all the possible service numbers and what they mean but, you are not responsible for knowing what the service numbers stand for. Each host can have multiple NetBIOS names because it can offer multiple services as shown below.

ie. Ottawa <00> = workstation service

Ottawa <20> = server service

Ottawa <01> = messaging

Figure 3 shows the NetBIOS names in use for a server called Calgary. Calgary is capable of <00> workstation services, and <20> server services.

You can view the NetBIOS names associated with the local host by typing

**nbtstat -n**

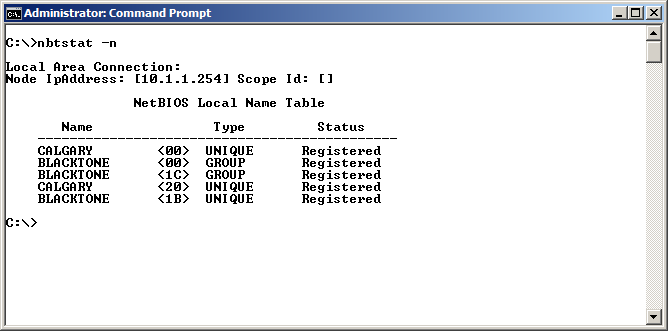
****

Fig. 3 The NetBIOS services provided by Calgary in the Blacktone domain

If the hostname is longer than 15 characters, the hostname will be truncated to 15 characters to form the NetBIOS name. For example, if the hostname is **computer\_services** the NetBIOS name would be the first 15 characters, **computer\_servic**.

Use **ipconfig /all** to view the hostname and DNS suffix. See figure 4

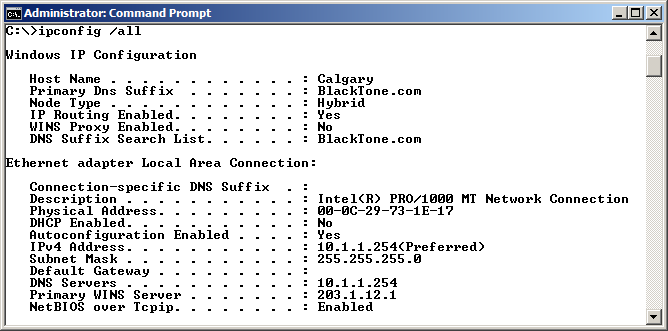


Fig. 4 Viewing the hostname and DNS suffix with ipconfig /all

Another way to find the hostname of a computer is by typing **hostname**.

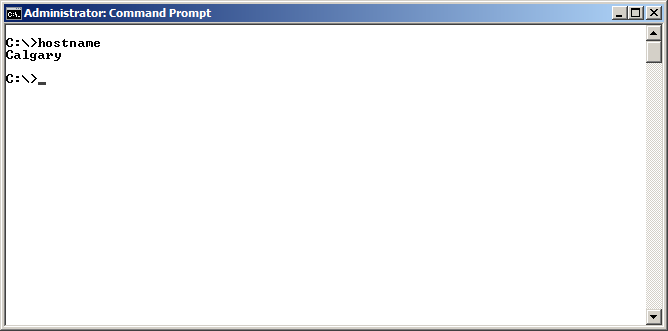


Fig. 5 The hostname command

A third method to reveal the hostname is to click on Start, My Computer and Properties for XP and Computer and Properties for Windows 7/8. See figure 6. Figure 6 can also be reached by going to Control Panel and System.

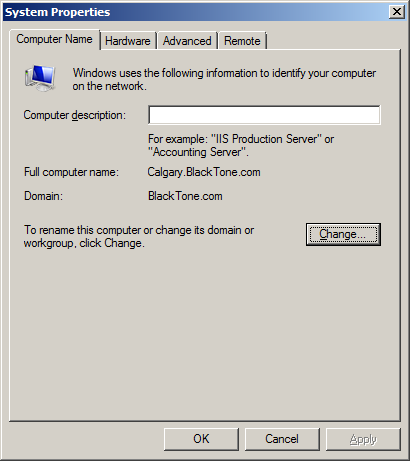


Fig. 6 Finding the hostname through properties of My Computer

If you want to change the name of the computer, click on the **Change** button in figure 6. Figure 7 appears. If you want to see the NetBIOS name, click on the **More** button and figure 8 appears.

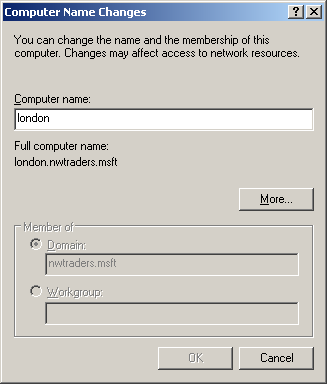


Fig. 7 Changing the hostname

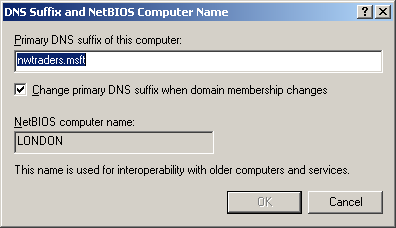


Fig. 8 Viewing the NetBIOS name

**NetBIOS Resolution**

NetBIOS resolution follows the sequence of steps shown below:

**NetBIOS WINS broadcast lmhosts**

**cache server file**

If you type “ping Calgary” NetBIOS will check the NetBIOS cache to see if it already has an IP address mapped to Calgary. You can view what is in the NetBIOS cache by typing **nbtstat –c** as shown in figure 9.

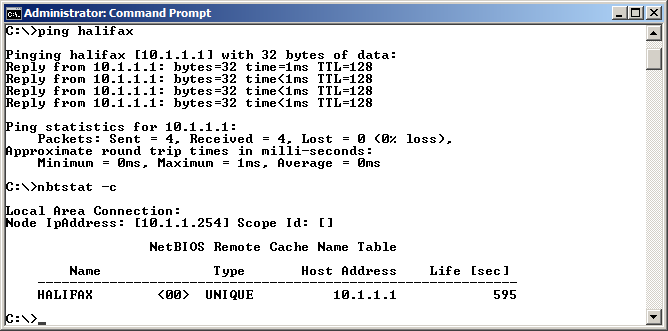


Fig. 9 After pinging Halifax, an entry appears in the NetBIOS cache

In figure 9, NetBIOS manages to resolve the IP address and the ping proceeds to the IP address of Halifax. After the ping has finished, viewing the NetBIOS cache shows that we now have an entry for Halifax. See figure 9.

**Resolved entries stay in cache for 10 minutes.** In figure 9, you can see the entry has 595 seconds left before it will be removed from the NetBIOS cache.

If there is no entry for the targeted host in NetBIOS cache, the computer will try to consult a WINS server to get the IP address of the computer it is targeting by name. If there is no WINS server or the WINS server does not have an entry for the targeted computer name, the host will send a broadcast asking all the computers on the same segment if they are using the targeted computer name.

If one of the computers is using the designated computer name, it will respond by sending its IP address. The address and computer name are then added to the NetBIOS cache so it can be found immediately without going to a WINS server or broadcasting the next time the name is referenced.

If the name still cannot be resolved, NetBIOS will check the **lmhosts** file. The **lmhosts** file contains static entries of frequently contacted hosts.

If the targeted computer name is not in the lmhosts file after the broadcast and WINS server failed to translate the name, the name cannot be resolved.

**LMHOSTS File**

The lmhosts file is used to statically map IP addresses to NetBIOS names. Figure 10 shows the contents of an lmhosts file.

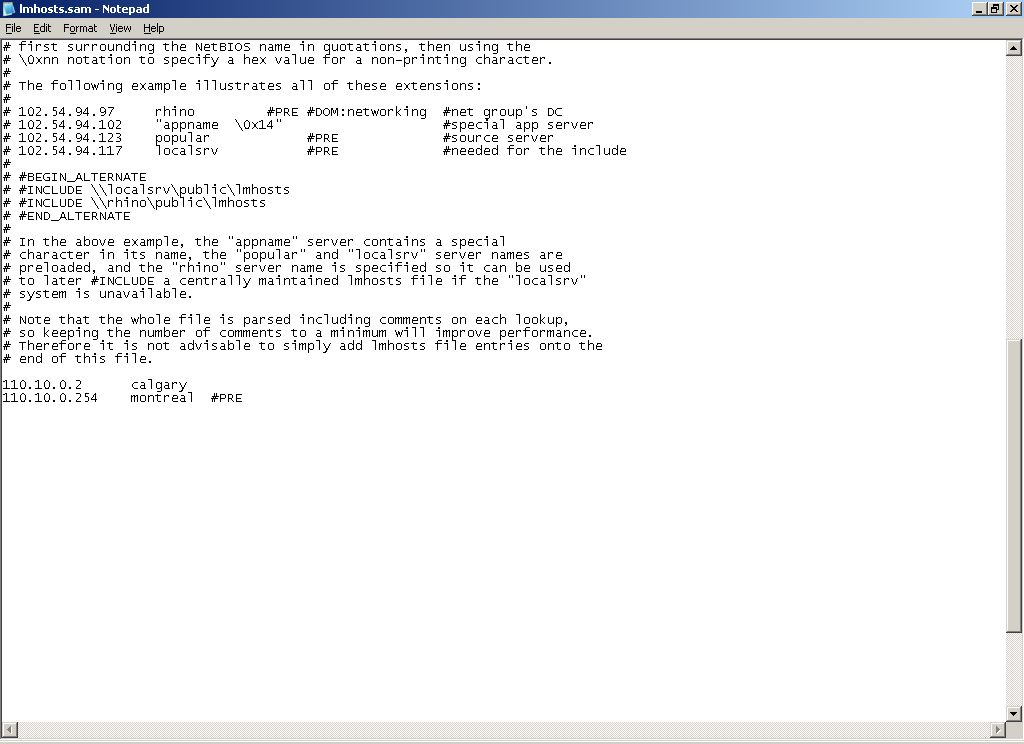


Fig. 10 Contents of the lmhosts file

The # symbol at the beginning of a line tells the operating system to treat this line as a remark statement. There is nothing to execute on this line.

In figure 10, there are two static mappings. One for a computer called Calgary and another for a computer called Montreal.

The file is stored in **%systemroot%\system32\drivers\etc** where **%systemroot%** is the directory the operating system was originally installed in. By default, this is the C:\Windows directory.

This directory contains a sample lmhosts file called **lmhosts.sam**. When you want to use the lmhosts file, add the mappings you require to the lmhosts.sam file and save it as just lmhosts without the extension. The operating system looks for an lmhosts file, not an lmhosts.sam file.

If a mapping in lmhosts is followed by a “**#PRE**”, the entry will be loaded into the NetBIOS cache when each time the computer is started or you can type

**nbtstat –R (not “r”)**,to clear the NetBIOS cache and add any “PRE” entries.“PRE” entries remain in cache until you remove them from the lmhosts file. In figure 10, you can see montreal is proceeded by #PRE. Figure 11 shows how this entry has been loaded into NetBIOS cache.

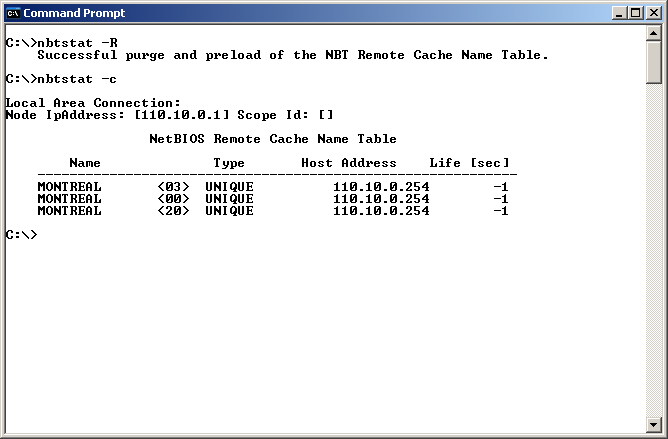


Fig. 11 The #PRE entry for Montreal is added to the NetBIOS cache

Notice the “life” for Montreal is “-1”. This means the entry will not be removed.

If we ping Montreal what would happen?

Check NetBIOS cache. It’s not in NetBIOS cache.

Check the WINS server. No entry in the WINS server.

Send Broadcast. Montreal is on a different network (110.10.0.0). Broadcast fails

Check lmhosts file. Entry for Montreal is found. Host can now send packet to

Montreal’s IP address.

**Turning off NetBIOS**

When NetBIOS issues frames on the network, it is using bandwidth. If an organization is using DNS and has no need for NetBIOS name resolution, NetBIOS can be turned off on the NIC of computers. Figure 12 shows how to configure the NIC so it does not use NetBIOS.

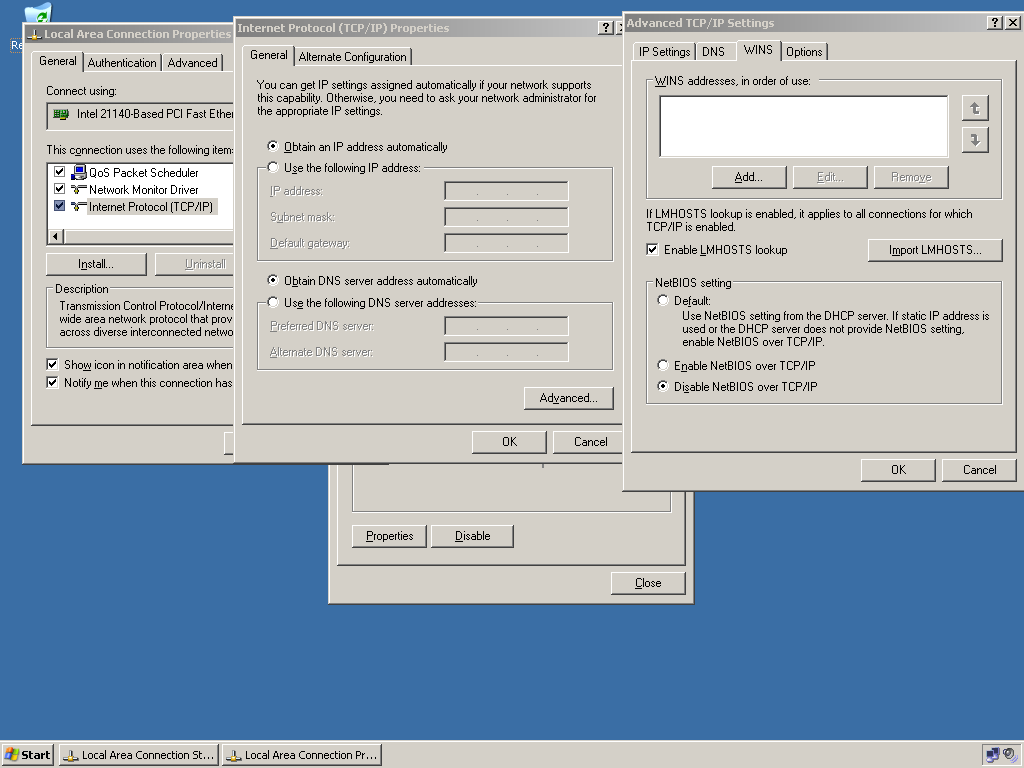


Fig. 12 Disabling NetBIOS on the NIC of the computer

**WINS (Windows Internet Name Service)**

If a NetBIOS client broadcasts to find the IP address of a computer, the process will only work if the targeted computer is on the same segment. Routers do not forward broadcasts to other segments.

If a company’s network is made up of multiple networks, a WINS server will be required to resolve the names of computers found on other segments.

If you configure the IP address of the WINS server on the properties page of the NIC of the client machines, the clients will register with WINS when they turn on. You can see in figure 12, the spot where you can add the WINS server IP address to the properties page of the NIC on the client machines.

You can add the WINS service to a Windows 2003 server by going through the “Manage Your Server” option on the Start menu of a Windows server 2003 server. See figure 13.

You can add the WINS service to a Windows 2008 server by adding the WINS feature in server manager. See figure 14.

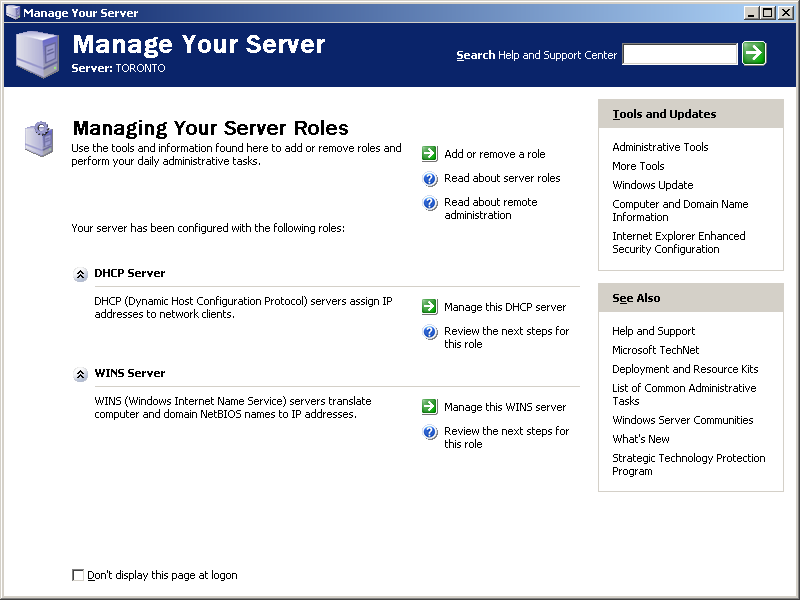


Fig. 13 Use “Manage your server” to install WINS on a server 2003

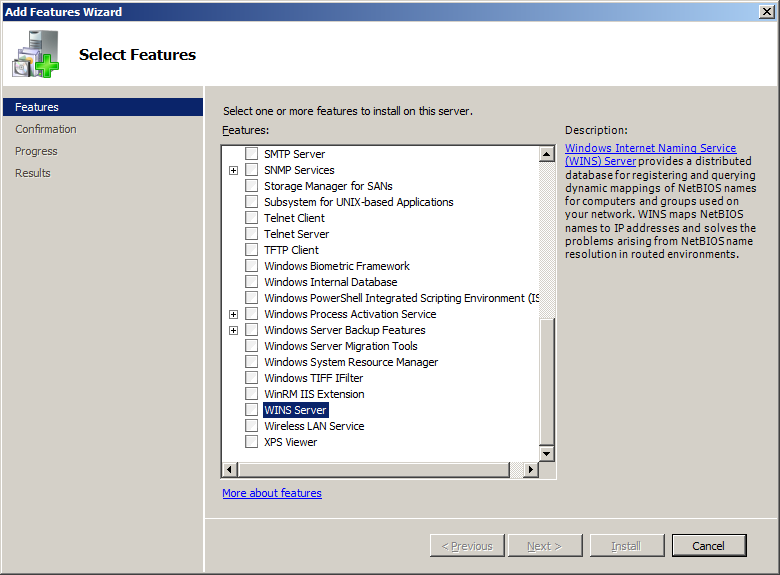


Fig. 14 Use “add a feature” in “server manager” to install WINS on a server 2008 or Server 2012

Registering with WINS means the client contacts the WINS server to tell the server what its name and IP address are. The registration consists of multiple records; one for each service offered by the client. Figure 15 shows the WINS console on the WINS server with records for Calgary, Ottawa, Toronto, and Winnipeg.

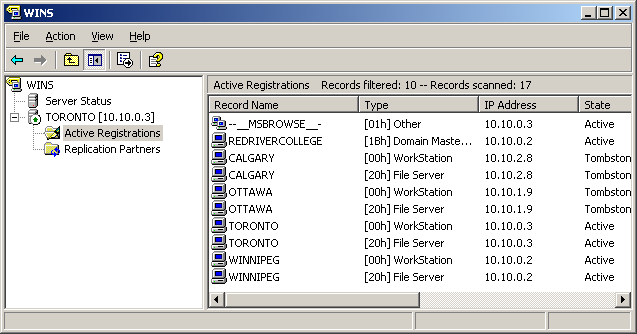
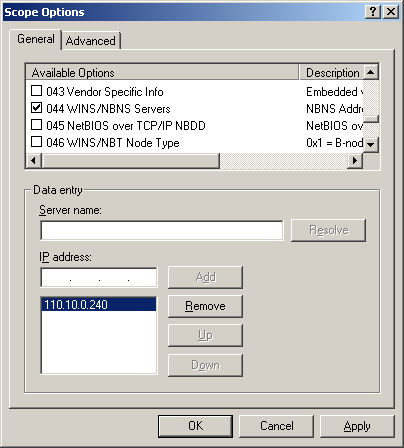


Fig. 15 NetBIOS records on the WINS server



Configuring each client with the IP address of the WINS server is not very efficient. It is better to configure the WINS address as an option in DHCP. Each time a DHCP client turns on, it will be given the IP address of the WINS servers.

Using DHCP to configure the WINS server address is a big time saver as well as allowing the administrator to add other WINS server addresses or change the existing addresses by making a

single change at the DHCP server. Fig. 16 WINS option on the DHCP server

Figure 16 shows how to configure DHCP with the WINS server IP address.