**Lab 5 Name \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**MCSE NetBIOS Name Resolution**

**Objective:**

In this lab you will:

- work with the NetBIOS cache

- observe how broadcasts are used for local NetBIOS resolution

- investigate the role of a WINS server when resolving names

- configure the lmhosts file to statically configure NetBIOS names

**Procedure:**

\_x\_\_ Start Ottawa (Windows 7), Hamilton (Windows 8) and Calgary (Server 2008 R2). Log into the Administrator’s account on each computer.

**Calgary:**

\_\_x\_ Put Calgary on VMNet 2 so it can communicate with Ottawa and Hamilton.

\_x\_\_ Configure the NIC for 10.1.1.10/16. The preferred DNS server will be Calgary, 10.1.1.10. There is no gateway.

\_x\_\_ Turn off IPv6.

\_x\_\_ Make sure you can ping by IP address between Ottawa, Hamilton and Calgary.

\_x\_\_ Start Wireshark on Hamilton.

**Hamilton:**

\_x\_\_ Make sure you are on the start screen. Type **CMD**.

\_x\_\_ Right-click on the CMD box in the upper-left corner and select **Run as Administrator** in the menu bar at the bottom of the screen.

If you do not run cmd as the administrator, the **arp –d** command will fail.

\_\_x\_ Check the ARP cache by typing **arp –a**. Clear the ARP cache by typing **arp –d \***. Display the arp cache again. (There is a multicast address of 224.0.0.22. Just ignore it. This is an IGMPv3 packet.)

**1. Capture the DOS window on Hamilton showing the output from the 3 commands; arp –a, arp –d \*, and arp –a again. The ARP cache should be empty when the last command is executed.**

\_x\_\_ On Hamilton, ping the IP address of Ottawa.

\_\_x\_ When the pings have finished, stop the Wireshark capture.

The window should look like figure 1.

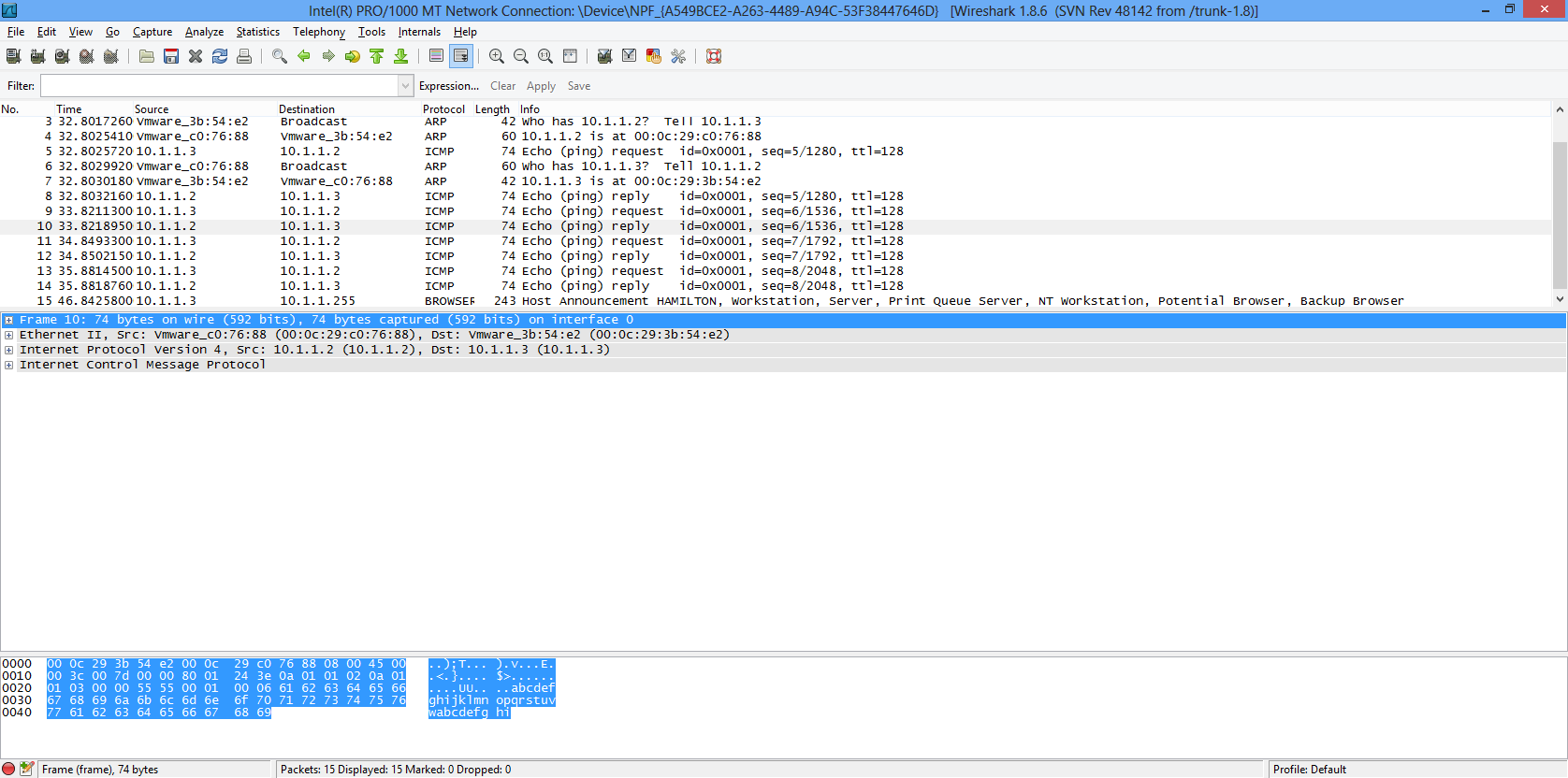


Fig. 1 The wireshark capture on Hamilton when it pings the IP of Ottawa

Notice the first two frames are an ARP request and an ARP reply.

**2. Explain the purpose to the two ARP frames. In your explanation use the computer names, not the IP addresses.**

Once Hamilton has Ottawa’s MAC address, the first ping is sent to Ottawa.

Ottawa then ARPs for Hamilton’s MAC. When Hamilton sends its MAC address, Ottawa sends the ping replay.

What happens if Hamilton pings Ottawa by name instead of IP address? The name must be translated into an IP address. This is the job of DNS or NetBIOS. Since there is no DNS server, we must rely on NetBIOS.

\_x\_\_ Clear the NetBIOS cache by typing **nbtstat –R**. Check the NetBIOS cache by typing **nbtstat -c** to make sure it is empty.

\_x\_\_ Start a Wireshark capture on Hamilton.

\_\_x\_ Ping Ottawa by name; **ping Ottawa**. (The command is not case sensitive).

\_x\_\_ Stop the Wireshark capture.

**3. Capture the Wireshark Display. It should look the same as**

**figure 2.**

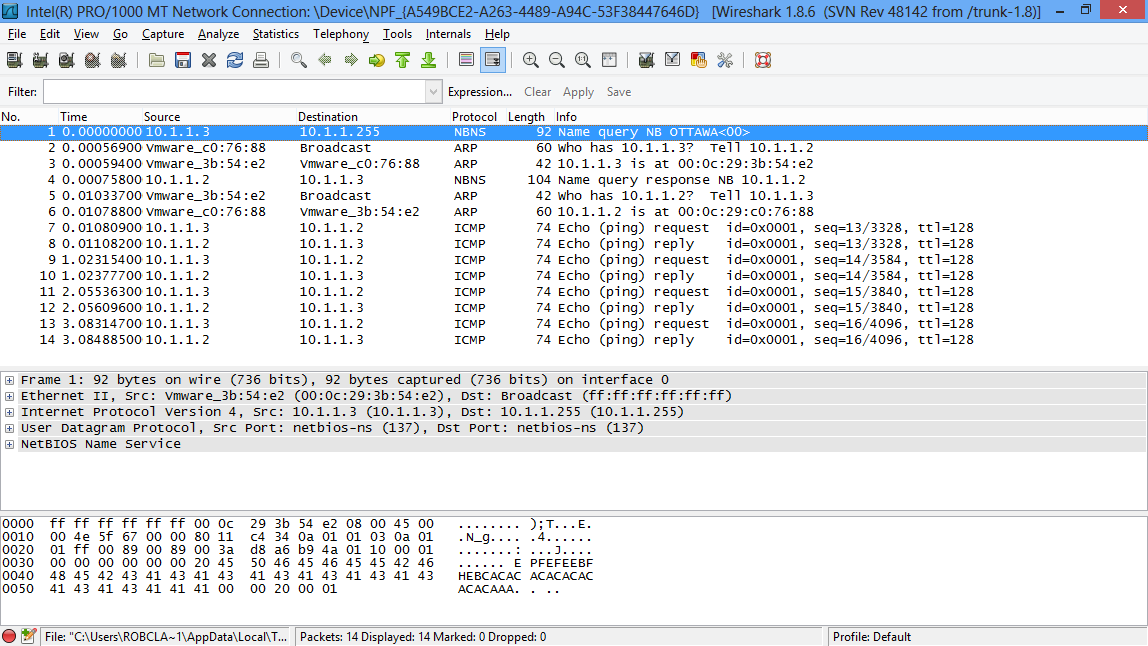


Fig. 2 Wireshark capture when Hamilton pings Ottawa by name.

\_\_x\_ Display the NetBIOS cache on Hamilton; **nbtstat –c**. There should be an entry for Ottawa.

**4. Capture the NetBIOS cache on Hamilton showing that the name Ottawa has been mapped to an IP address.**

This is the explanation of the frames in figure 2.

Frame #1 Hamilton (10.1.1.3) broadcasts (10.1.1.255) to find the IP address

of the computer called Ottawa. This is an **NBNS** (NetBIOS Name

Service) frame.

Frame #2 Ottawa ARPs to find out the MAC address of Hamilton.

Frame #3 Hamilton sends an ARP telling Ottawa what its MAC address is.

Frame #4 Ottawa sends a NetBIOS reply telling Hamilton what its IP address

is.

Frame #5 Hamilton asks for Ottawa’s MAC address.

Frame #6 Ottawa sends Hamilton its MAC address.

Frames #7 through #14 The pings go through successfully.

\_x\_\_ Ping Ottawa by name, again.

This will ensure the mapping for Ottawa to 10.1.1.2 is still found in the NetBIOS cache. It also ensures the MAC to IP mapping is still in the ARP cache.

\_x\_\_ Start a new Wireshark capture on Hamilton.

\_x\_\_ Ping Ottawa from Hamilton, again.

\_x\_\_ Stop the Wireshark capture when the pings have finished.

**5. Capture Wireshark display showing only pings are generated.**

**6. Explain why there is no ARP frames or NetBIOS frames generated this time.**

NetBIOS uses the following methods to map a name into an IP address.

**NetBIOS WINS broadcast lmhosts**

**cache server file**

Fig. 3 4 steps NetBIOS will try when it attempts to translate a name into an IP

We saw how NetBIOS broadcasted to find out Ottawa’s IP address. When we pinged again, we saw there was no NetBIOS request to find out Ottawa’s IP address because after the first ping, Ottawa’s IP address was added to the NetBIOS cache. The second time we pinged, Hamilton found Ottawa’s IP address in the NetBIOS cache and it’s MAC address in the ARP cache.

We still have to investigate how the WINS server works.

\_x\_\_ On Hamilton, type **ipconfig /all**.

Notice there is no WINS server configured. We currently do not have a WINS server running. Let’s install WINS on Calgary.

**Calgary:**

\_x\_\_ Select **Server Manager** as shown in figure 4.

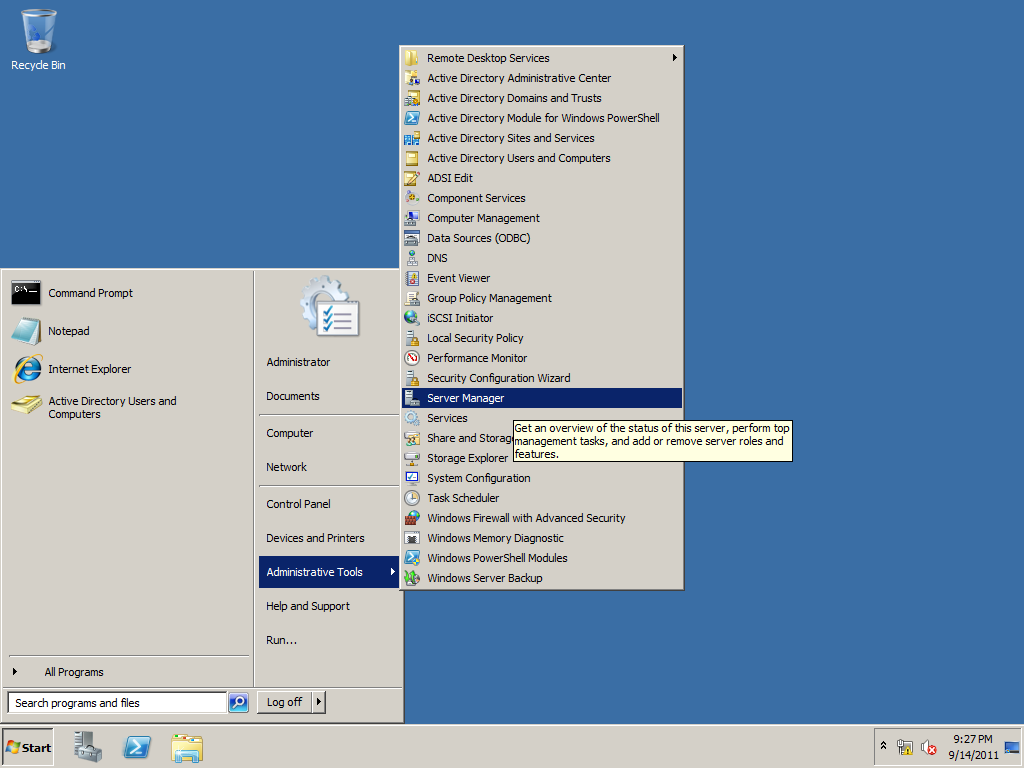


Fig. 4 Starting the Server Manager

\_x\_\_ Click on **Features** in the left pane. Then click on **Add Features** in the right pane.

\_x\_\_ Scroll to the bottom of the list and check the box opposite **WINS server**.

\_\_x\_ Finish installing WINS on Calgary.

**Hamilton:**

\_x\_\_ On Hamilton, configure Calgary (10.1.1.10) as the WINS server. See

figure 5.

\_\_x\_ In figure 5, the gateway shows up as 10.1.1.2. If you have an address for the gateway, remove it. There should be no gateway.

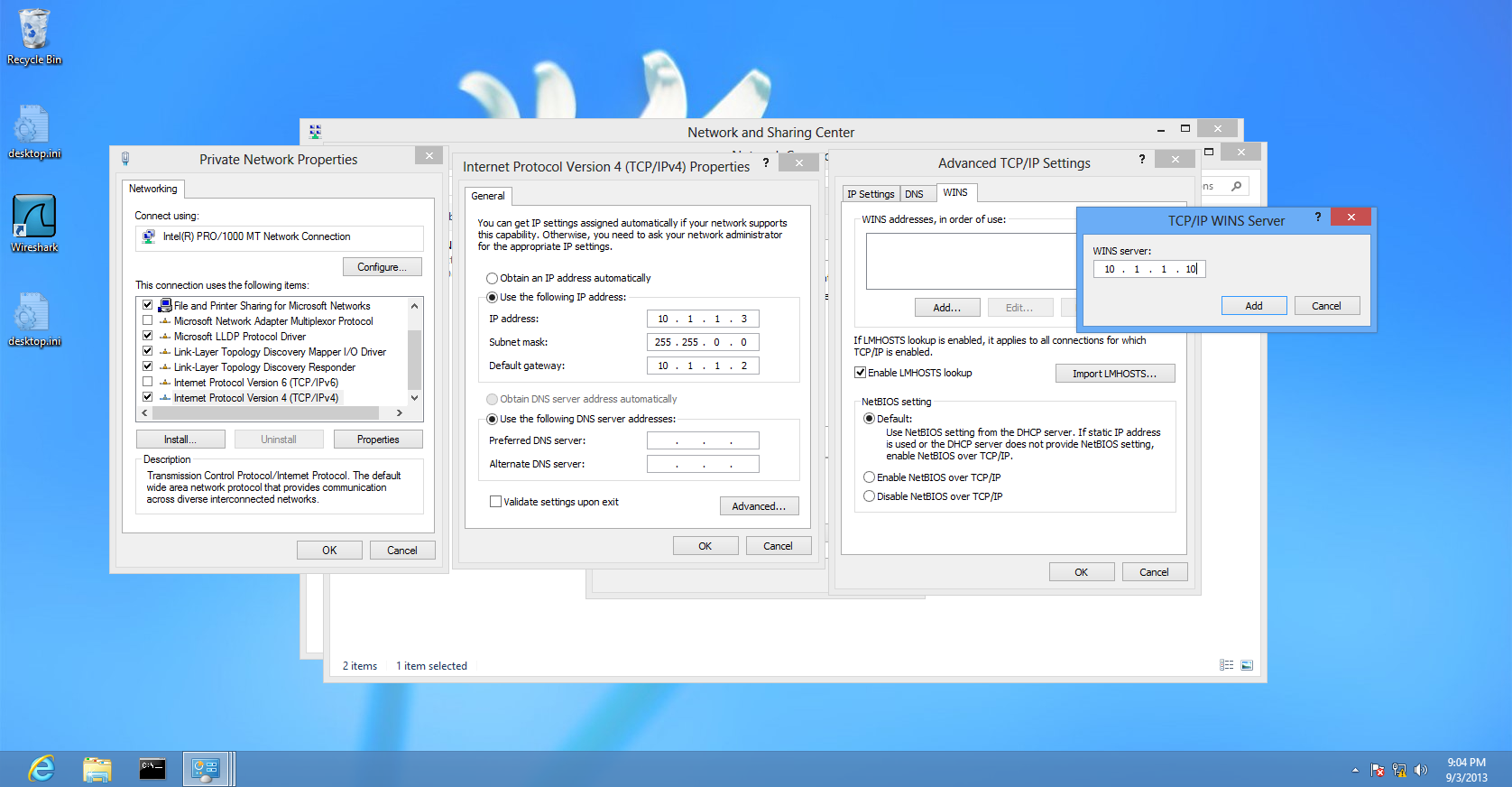


Fig. 5 Configuring Hamilton so it uses Calgary as the WINS server

\_x\_\_ On Hamilton, type **ipconfig /all**.

The primary WINS server should show up as 10.1.1.10 (Calgary’s IP).

\_x\_\_ Clear the NetBIOS cache on Hamilton.

\_x\_\_ Start a capture in Wireshark.

\_x\_\_ Ping Ottawa from Hamilton.

\_\_x\_ Stop the Wireshark capture.

**7. Capture the Wireshark display. It should look like figure 6.**

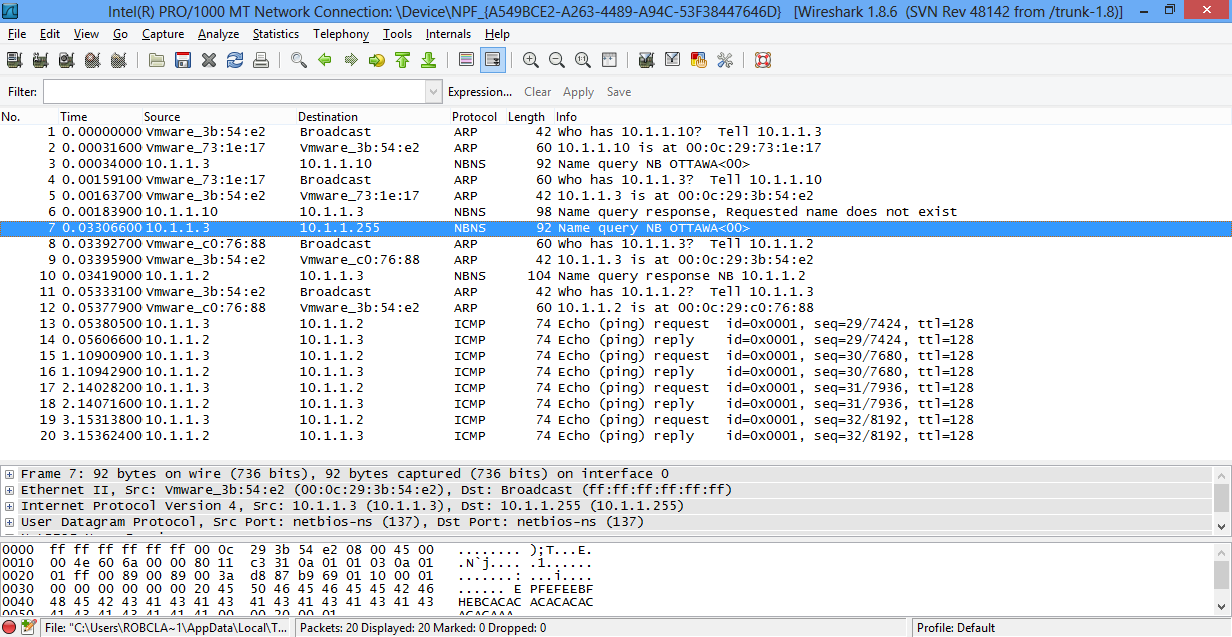


Fig. 6 The result of pinging Ottawa from Hamilton when Hamilton has a WINS

server configured.

According to the flow chart on page 4 of this lab, Hamilton would have checked its NetBIOS cache first. Having found no entry for Ottawa (since we cleared the NetBIOS cache), the flow chart says step 2 is contact the WINS server. Here’s an explanation of the frames in figure 6.

Frame #1 Hamilton wants to contact the WINS server so it ARPs for the MAC address of the WINS server.

Frame #2 Calgary, the WINS server sends an ARP reply. Hamilton now

knows the MAC address of Calgary.

Frame #3 Hamilton (10.1.1.3) sends a name resolution request to the WINS server, Calgary at 10.1.1.10.

Frame #4 Calgary ARPs to get Hamilton’s MAC address

Frame #5 Hamilton sends Calgary an ARP reply so Calgary now knows

Hamilton’s MAC address.

Frame #6 Calgary tells Hamilton it does not know the IP address of Ottawa. We haven’t configured Ottawa to point to a WINS server so it did not register its WINS record with Calgary.

Frame #7 Hamilton broadcasts on 10.1.1.255 to find out if Ottawa exists on the same segment.

Frame #8 Ottawa ARPs to get Hamilton’s MAC address.

Frame #9 Hamilton sends an ARP reply to tell Ottawa what its MAC address

is.

Frame #10 Ottawa sends Hamilton its IP address.

Frame #11 Hamilton ARPs to get Ottawa’s MAC.

Frame#12 Ottawa sends its MAC to Hamilton.

The rest of the frames are Hamilton successfully pinging Ottawa.

Let’s take a look at WINS on Calgary.

**Calgary:**

\_x\_\_ On Calgary, click on Start, Administrative Tools, and WINS at the bottom of the list.

\_\_x\_ Expand **Calgary (10.1.1.10)**. Right-click on **Active Registrations** and select **Display Records**. Click on the **Find now** button. Figure 7 should be visible.

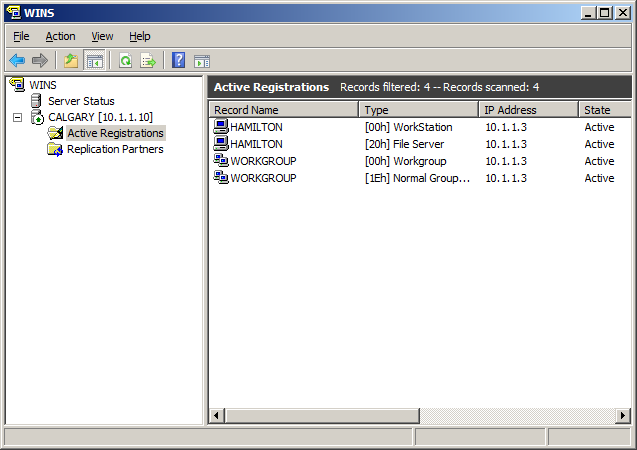


Fig. 7 The NetBIOS records found in the WINS server

Figure 7 shows a list of all the NetBIOS records found on the WINS server.

\_x\_\_ Configure the WINS page of the properties of the NIC on Calgary so it points to itself as the WINS server. If there are any entries in the WINS box, remove them so only the 10.1.1.10 IP address is left.

**Ottawa:**

\_x\_\_ Configure Ottawa’s NIC to point to Calgary as the WINS server. You may find an IP address for 10.10.0.2 already on the WINS page. Delete it.

\_x\_\_ Force Ottawa and Calgary to register their NetBIOS records with the WINS server. To do this type **nbtstat –RR** at a DOS prompt on both machines.

**Calgary:**

\_x\_\_ On Calgary, in the WINS snap-in, right-click on Calgary (10.1.1.10) and select **Refresh**. Then display the records again. The display should look like figure 8.

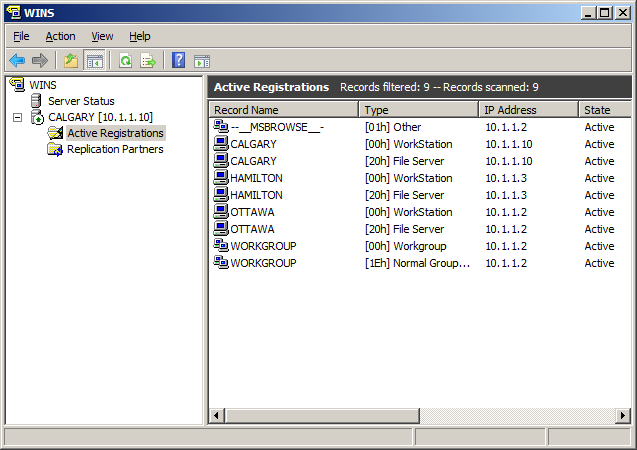


Fig. 8 WINS on Calgary showing the proper records has registered

**8. Capture the WINS display. It should look like figure 8.**

**Hamilton:**

\_x\_\_ Clear the NetBIOS cache on Hamilton. **(nbtstat –R**)

\_x\_\_ Start a Wireshark capture on Hamilton.

\_x\_\_ Ping Ottawa by name.

\_x\_\_ Stop the Wireshark capture. The display should look like figure 9.

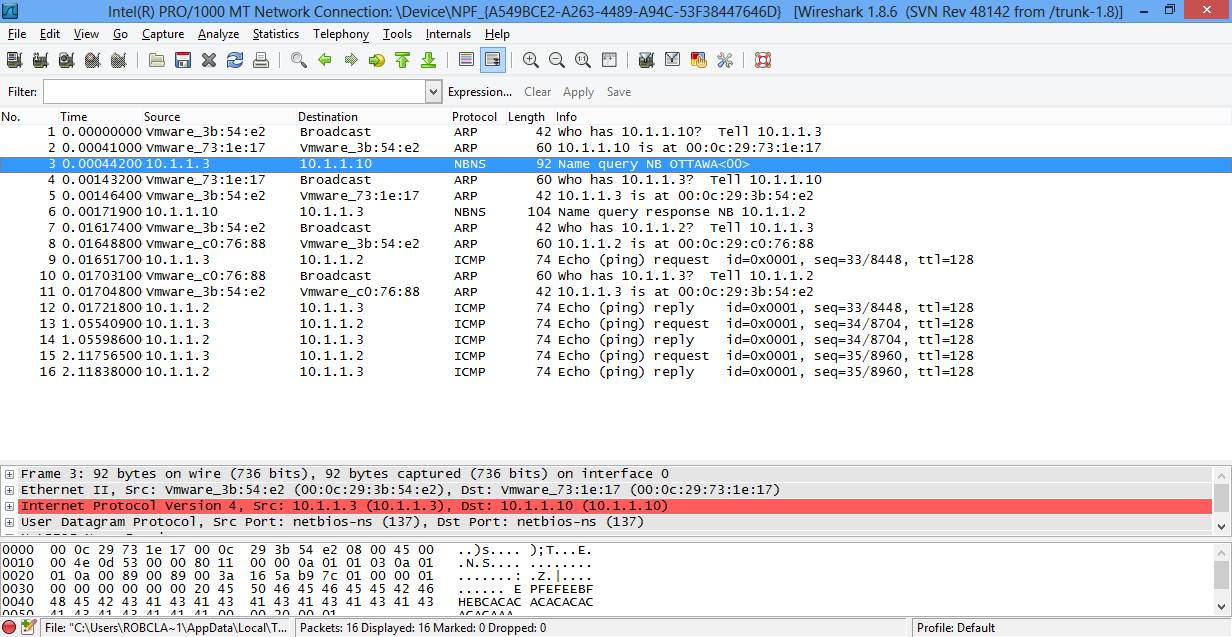


Fig. 9 Hamilton obtains the IP address of Ottawa from the WINS server.

**9. Explain the sequence of events in figure 9. Provide an explanation each of the first 12 frames. Use computer names instead of IP addresses.**

We have seen how the first 3 blocks of the flowchart work. The last remaining

block is the configuring of the lmhosts file. The lmhosts file is used to statically

configure host to IP mappings. This is useful if you do not have a WINS server

available in your network, yet you do have multiple networks that will not allow

hosts to be found with broadcasts.

**Ottawa:**

\_\_x\_ Configure the NIC so the gateway address is 10.1.1.10, Calgary’s address.

Normally, you would point to the router but we don’t have one and we need a

gateway address configured to perform the next steps.

\_\_x\_ Open the Windows Explorer. Navigate to the **c:\windows\system32\drivers\etc** folder.

\_x\_\_ Use **Notepad** to open the **lmhosts.sam** file.

Let’s pretend we have a computer called **Japan** with a network address of

20.20.20.20. Since this is a different network than the one Ottawa is on, we

cannot use a broadcast. Our WINS server does not have a record for it. We’ll

put a record in the lmhosts file to allow Ottawa to find Japan.

\_x\_\_ Add the following entry to the bottom of the lmhosts file:

**20.20.20.20 Japan**

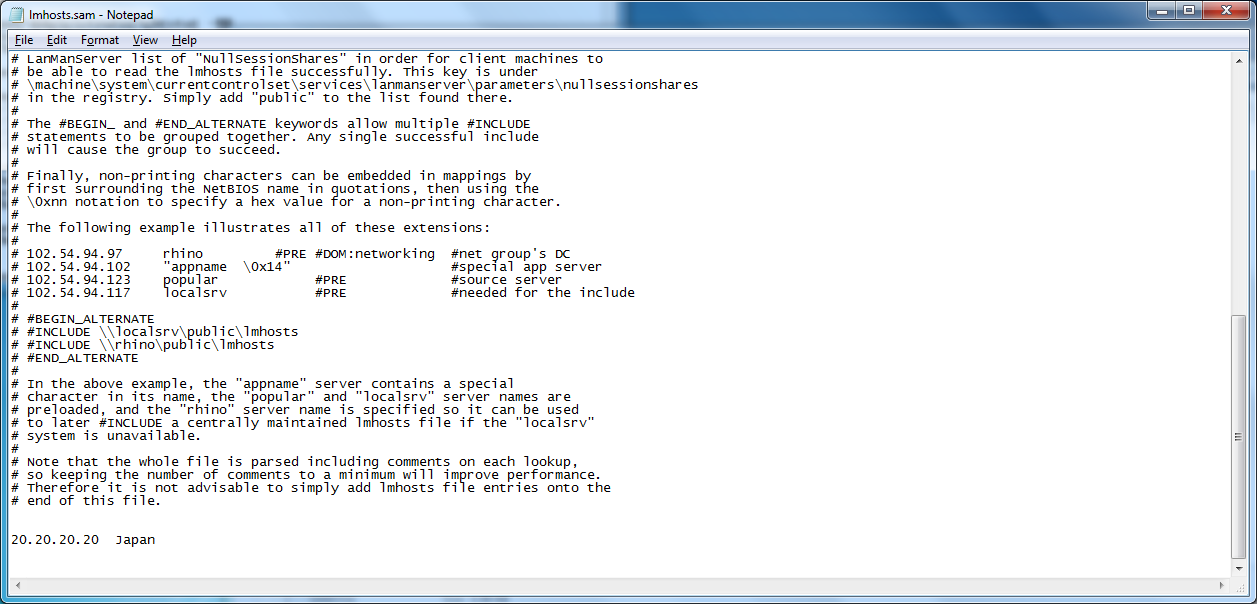
****

Fig. 10 The lmhosts file after the record for Japan has been added

**10. Capture the lmhosts file showing the recorded you added for Japan.**

\_x\_\_ Save the file as lmhosts without an extension. Notepad will try to add an extension but you can prevent this by placing quotes around the name lmhosts. Save the file as “lmhosts” including the quotes.

\_\_x\_ Clear the NetBIOS cache on Ottawa.

**Hamilton:**

\_x\_\_ Start a fresh Wireshark capture on Hamilton.

**Ottawa:**

\_x\_\_ Ping Japan.

**Hamilton:**

\_x\_\_ Stop the Wireshark capture.

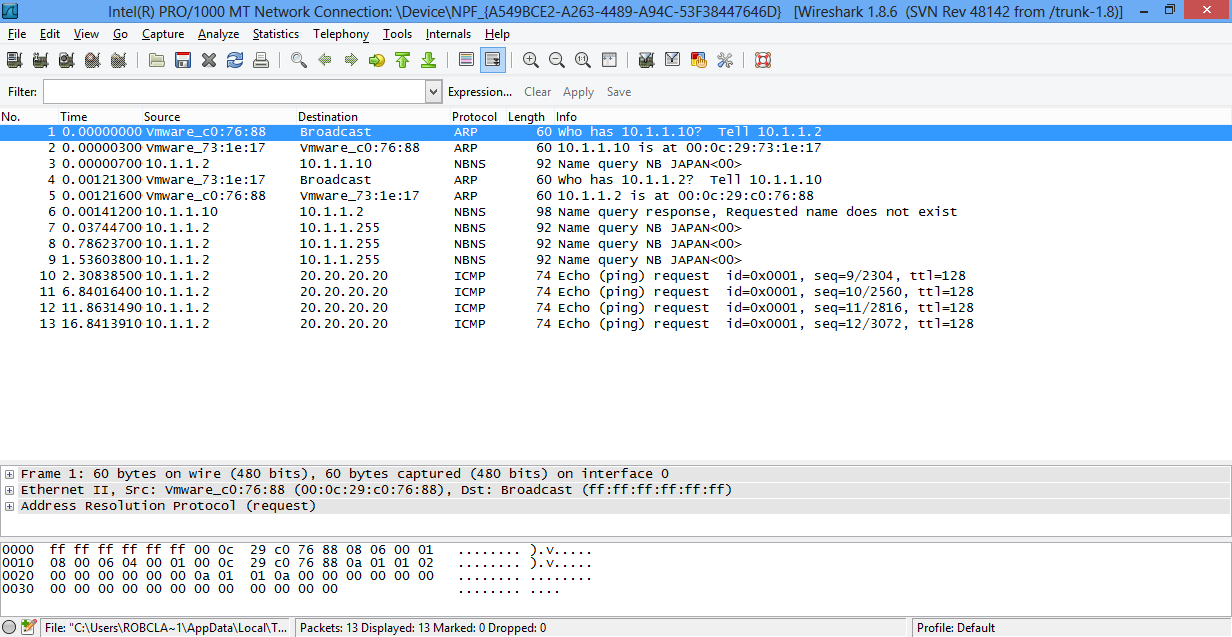


Fig. 11 Pinging Japan from Ottawa. Japan is in the lmhosts file.

**11. Capture the output of the Wireshark display when Ottawa tries to ping Japan.**

Here’s the explanation of what happened this time.

Frame #1 Ottawa wants to contact the WINS server so it ARPs for the MAC address of the WINS server.

Frame #2 Calgary, the WINS server sends an ARP reply. Ottawa now

knows the MAC address of Calgary.

Frame #3 Ottawa (10.1.1.2) sends a name resolution request to the WINS server, Calgary at 10.1.1.10.

Frame #4 Calgary ARPs to get Ottawa’s MAC address

Frame #5 Ottawa sends Calgary an ARP reply so Calgary now knows

Ottawa’s MAC address.

Frame #6 Calgary tells Ottawa it does not know the IP address of Japan.

Frame #7 Ottawa broadcasts on 10.1.1.255 to find out if Japan exists on the same segment.

Frame #8 Ottawa doesn’t get a reply so it broadcasts again just in case the first broadcast got destroyed.

Frame #9 Ottawa doesn’t get a reply so it broadcasts one more time

Frame #10 – 13 Ottawa has found the IP address of Japan in the lmhosts file. It

realizes Japan is on another network so Ottawa now wants to send the packet to its gateway at 10.1.1.10. (We configured Ottawa with a gateway that points to Calgary). Ottawa sends the pings to 20.20.20.20 by passing them to the gateway.

*You’re all done*

[](http://www.google.ca/url?sa=i&rct=j&q=&esrc=s&frm=1&source=images&cd=&cad=rja&docid=1PZRBdD60MKEyM&tbnid=xJEzEag91L6KAM:&ved=0CAUQjRw&url=http://www.pixopop.com/daily-pop/2012/3/22/time-to-go-home.html&ei=8GOIUfP7McmgqwHc6oDoCQ&bvm=bv.45960087,d.aWc&psig=AFQjCNHx4q4tZQCRdxj24OBmaGvYxLmbCw&ust=1367979281630786)