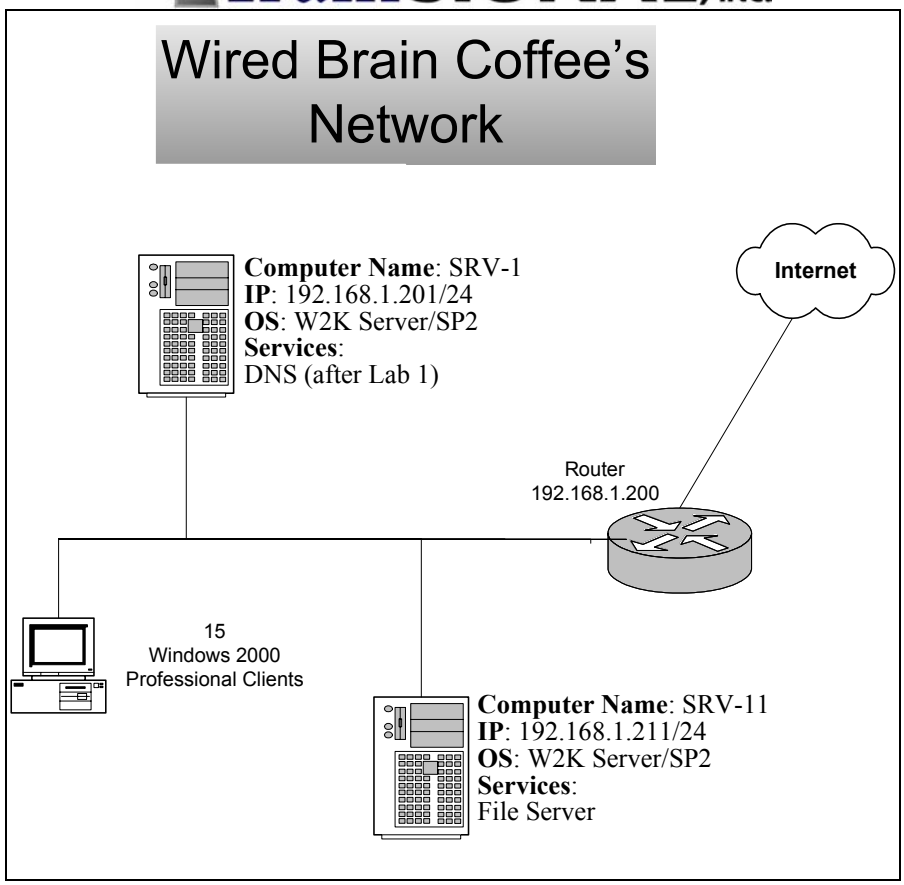
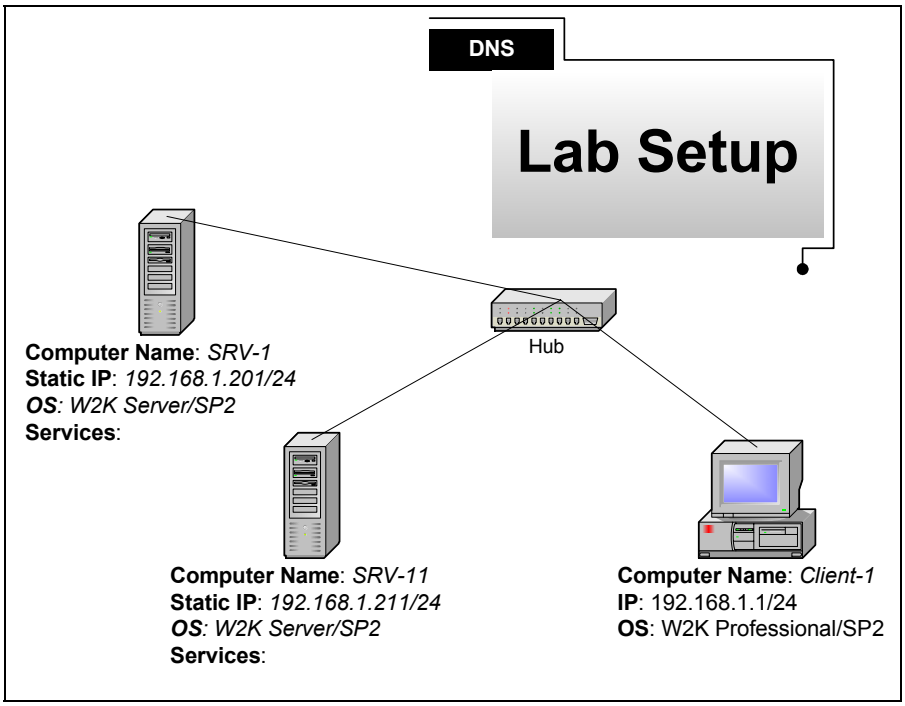
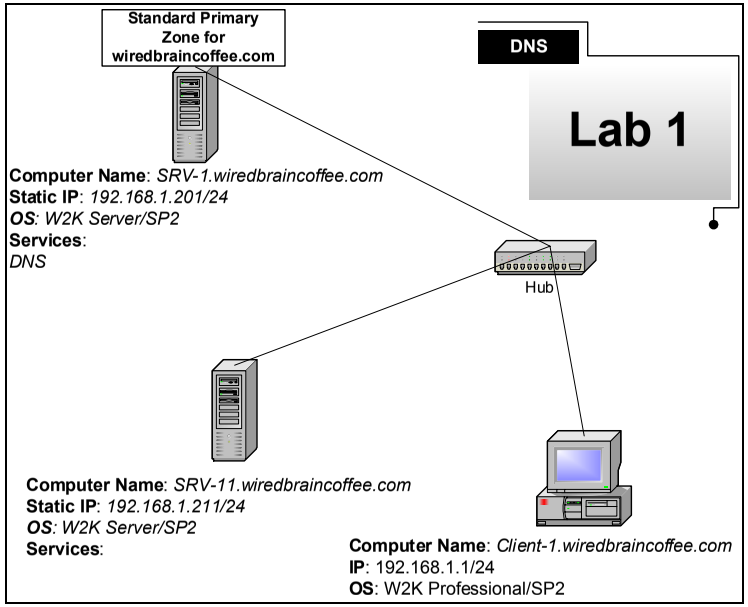
Building a Windows 2000 DNS Infrastructure
for Wired Brain Coffee, Inc.

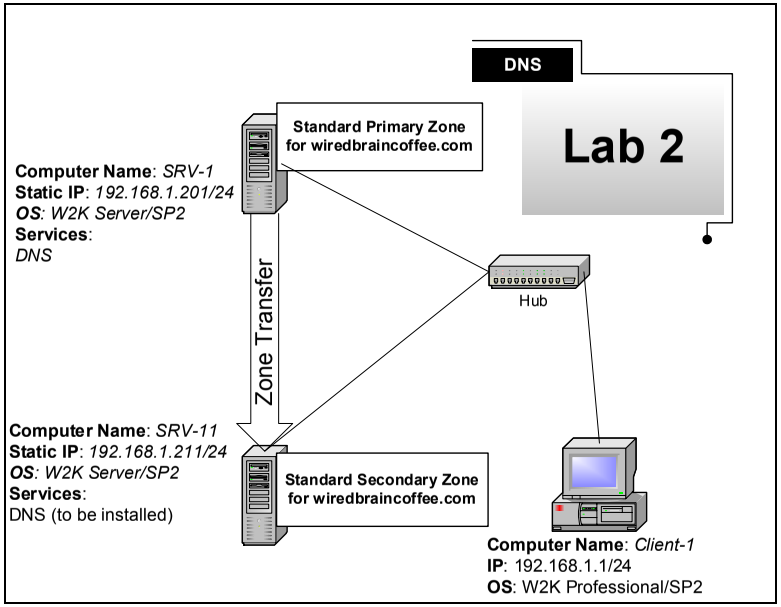
Mega Lab 4

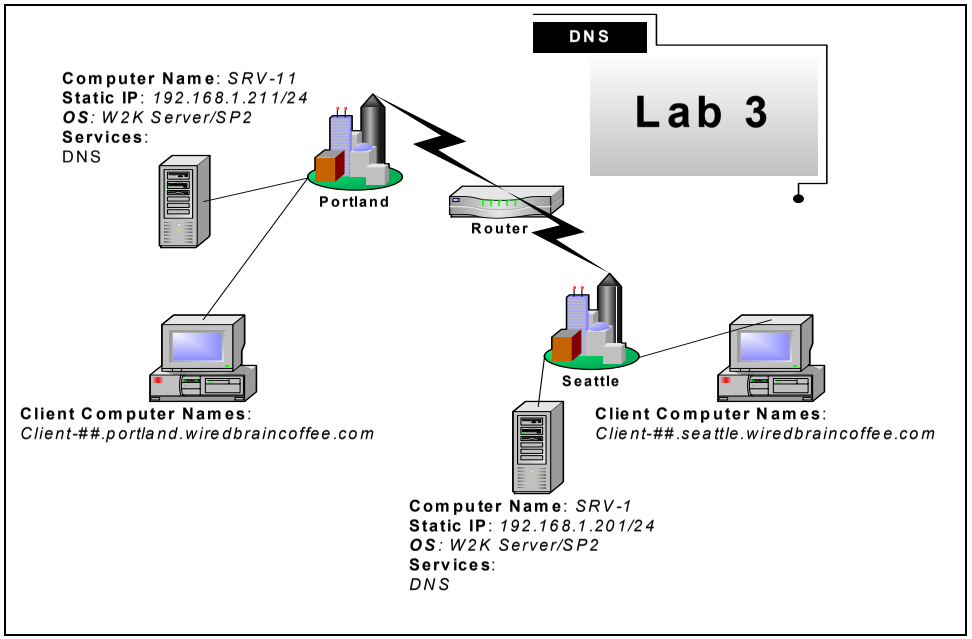
Part 1 of 3 in the Building a Windows 2000/Server 2003
Network Infrastructure Series











Building a DNS Infrastructure for Wired Brain Coffee, Inc.

Mega Lab 4

Part 1 of 3 in the
Building a Windows 2000
Network Infrastructure Series

About the Authors

Scott Skinger (MCSE, CNE, CCNP, A+) is the owner of Train Signal, Inc. and is the course director for the Mega Lab Series. In addition, Scott works as an Instructor and as a Network Integrator with his consulting company, SAS Technology Advisors, Inc.

Jesus Salgado (MCSE, A+) is responsible for content development for the Building a Network Infrastructure Mega Lab Series. He also repairs computer hardware, builds systems and does network consulting for his own company, JSJR3 Consulting.

Train Signal, Inc.
400 West Dundee Road
Suite #106
Buffalo Grove, IL 60089
Phone - (847) 229-8780
Fax – (847) 229-8760
www.trainsignal.com

Disclaimer and Limitation of Liability

Although the publishers and authors of the Information have made every effort to ensure that the information within it was correct at the time of publication, the publishers and the authors do not assume and hereby disclaim any liability to any party for any loss or damage caused by errors, omissions, or misleading information.

TRAIN SIGNAL, INC. PROVIDES THE INFORMATION "AS-IS." NEITHER TRAIN SIGNAL, INC. NOR ANY OF ITS SUPPLIERS MAKES ANY WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. TRAIN SIGNAL, INC. AND ITS SUPPLIERS SPECIFICALLY DISCLAIM THE IMPLIED WARRANTIES OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE. THERE IS NO WARRANTY OR GUARANTEE THAT THE OPERATION OF THE INFORMATION WILL BE UNINTERRUPTED, ERROR-FREE, OR VIRUS-FREE, OR THAT THE INFORMATION WILL MEET ANY PARTICULAR CRITERIA OF PERFORMANCE OR QUALITY. YOU ASSUME THE ENTIRE RISK OF SELECTION, INSTALLATION, AND USE OF THE INFORMATION.
IN NO EVENT AND UNDER NO LEGAL THEORY, INCLUDING WITHOUT LIMITATION, TORT, CONTRACT, OR STRICT PRODUCTS LIABILITY, SHALL TRAIN SIGNAL, INC. OR ANY OF ITS SUPPLIERS BE LIABLE TO YOU OR ANY OTHER PERSON FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY KIND, INCLUDING WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER MALFUNCTION, OR ANY OTHER KIND OF DAMAGE, EVEN IF TRAIN SIGNAL, INC. HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL TRAIN SIGNAL, INC. BE LIABLE FOR DAMAGES IN EXCESS OF TRAIN SIGNAL, INC.'S LIST PRICE FOR THE INFORMATION.

To the extent that this Limitation is inconsistent with the locality where You use the Software, the Limitation shall be deemed to be modified consistent with such local law.

Choice of Law:

You agree that any and all claims, suits or other disputes arising from your use of the Information shall be determined in accordance with the laws of the State of Illinois, in the event Train Signal, Inc. is made a party thereto. You agree to submit to the jurisdiction of the state and federal courts in Cook County, Illinois for all actions, whether in contract or in tort, arising from your use or purchase of the Information.

TABLE of CONTENTS

Introduction

Welcome to Train Signal!

This series of labs on Windows 2000 is designed to give you detailed, hands-on experience working with Windows 2000. Train Signal's Audio-Visual Lab courses are targeted towards the serious learner, those who want to know more than just the answers to the test questions. We have gone to great lengths to make this series appealing to both those who are seeking Microsoft certification and to those who want an excellent overall knowledge of Windows 2000.

Each of our courses put you in the driver's seat, working for different fictitious companies, deploying complex configurations and then modifying them as your company grows. They are not designed to be a "cookbook lab," where you follow along with the steps of the "recipe" until you have completed the lab and have learned nothing. Instead, we recommend that you perform each step and then analyze the results of your actions in detail.

To complete these labs yourself, you will need three computers equipped as described in the Lab Setup section. You also need to have a foundation in Windows 2000 and TCP/IP concepts. You should be comfortable with installing Windows 2000 Professional or Server and getting the basic operating system up and running. Each of the labs in this series will start from a default installation of Windows 2000 and will then run you through the basic configurations and settings that you must use for the labs to be successful. It is very important that you follow these guidelines **exactly**, in order to get the best results from this course.

The course also includes a CD-ROM that features an audio-visual walk-through of all of the labs in the course. In the walk-through, you will be shown all of the details from start to finish on each step, for every lab in the course. During the instruction, you will also benefit from live training that discusses the current topic in great detail, making you aware of many of the fine points associated with the current topic.

Thank you for choosing Train Signal!

Lab Setup

Setting up the Lab

1. Computer Equipment Needed

Item	Minimum	Recommended
Computers	(3) Pentium I 133 MHz	(3) Pentium II 300MHz
Memory	128 MB	256 MB
Hard Drive	2 GB	4 GB
NIC	1/machine	1/machine
Hubs	1	1
Network Cable	(3) 3' cables	(3) 6' cables or greater

I strongly urge you to acquire all of the recommended equipment in the list above. It can all be easily purchased from eBay or another source, for around $500 (less if you already have some of the equipment). This same equipment is used over and over again in all of Train Signal's labs and will also work great in all sorts of other network configurations that you may want to set up in the future. It will be an excellent investment in your education. You may also want to look into a disk-imaging product such as Norton Ghost. Disk imaging software will save you a tremendous amount of time when it comes to reinstalling Windows 2000 for future labs. Many vendors offer trial versions or personal versions of their products that are very inexpensive.

2. Computer Configuration Overview

Computer Number	1	2	3
Computer Name	SRV-1	SRV-11	Client-1
IP Address	192.168.1.201	192.168.1.211	192.168.1.1
OS	W2K Server	W2K Server	W2K Pro
Additional Configurations	Stand-Alone Server SP2	Stand-Alone Server SP2	SP2

3. Detailed Lab Configuration

*****Important Note*****
This lab should NOT be performed on a live production network. You should only use computer equipment that is not part of a business network AND is not connected to a business network. Train Signal Inc., is not responsible for any damages. Refer to the full disclaimer and limitation of liability which appears at the beginning of this document and on our web site, www.trainsignal.com.

Computer 1
Computer 1 will be named SRV-1 and the operating system on this computer will be Windows 2000 Server or Advanced Server. You should also install Service Pack 2 to avoid any unforeseen problems. If you do not have a copy of Windows 2000 Server you can obtain an evaluation copy of Windows 2000 Advanced Server within the Microsoft Press series of books and Service Pack 2 is available for download on Microsoft's web site.

SRV-1 will have a static IP address of 192.168.1.201 with a 255.255.255.0 subnet mask. The default gateway field can be left blank but you should enter the computer's own IP address for the Preferred DNS field (192.168.1.201). The alternate DNS Server field can be left blank.

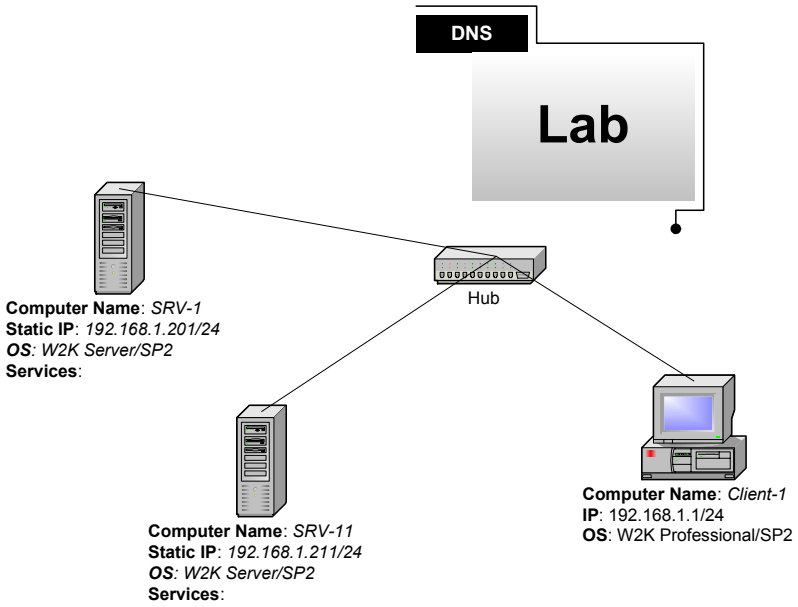
Computer 2

Computer 2 will be named SRV-11 and Windows 2000 (either version again) will be installed on this computer with Service Pack 2. SRV-11 will have a static IP address of 192.168.1.211 with a 255.255.255.0 subnet mask. The default gateway can be left alone at this point. Configure the preferred DNS server setting to point to SRV-1, 192.168.1.201 and leave the alternate DNS setting blank.

Computer 3

Computer 3 will be named Client-1 and have Windows 2000 Professional installed as the operating system. Client-1 will be joined to the wiredbraincoffee.com domain just as SRV-11 was. Client-1 will have a static IP address of 192.168.1.1 with a 255.255.255.0 subnet mask. The default gateway can be left alone at this point. Configure the preferred DNS server setting to point to SRV-1, 192.168.1.201, and leave the alternate DNS setting blank.

Important - You should test the network connections (using the PING command) between each of these machines to ensure that your network is set up properly. Testing before you get started will save you major time and effort later.



(figure 1)

*****Important Note*****

This lab should NOT be performed on a live production network. You should only use computer equipment that is not part of a business network AND is not connected to a business network. Train Signal Inc., is not responsible for any damages. Refer to the full disclaimer and limitation of liability which appears at the beginning of this document and on our web site, www.trainsignal.com.

Lab 1

Building the DNS Infrastructure for Wired Brain Coffee, Inc.

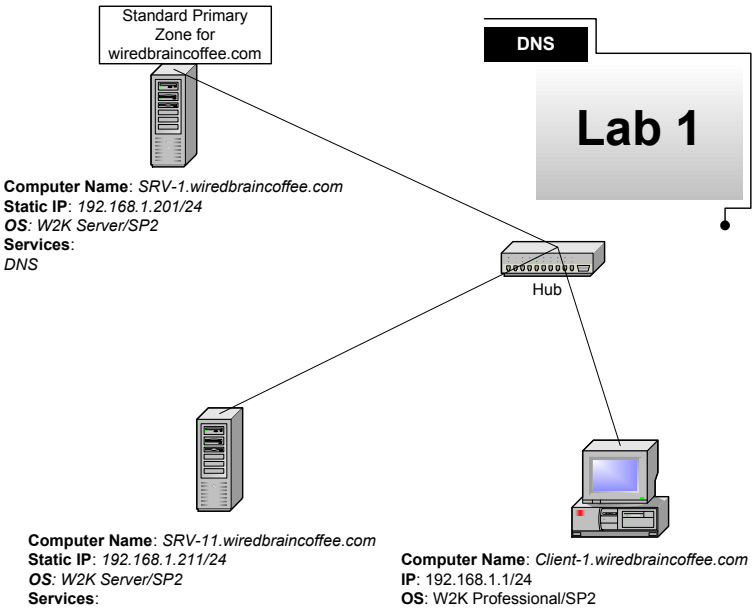
You will learn how to:

- Install and configure a DNS Server
  - Set the Primary DNS suffix
- Create forward & reverse lookup zones
  - Create a Host (A) record
  - Create a Pointer (PTR) record
  - Configure a DNS client
- Troubleshoot DNS using the NSLOOKUP command

Scenario

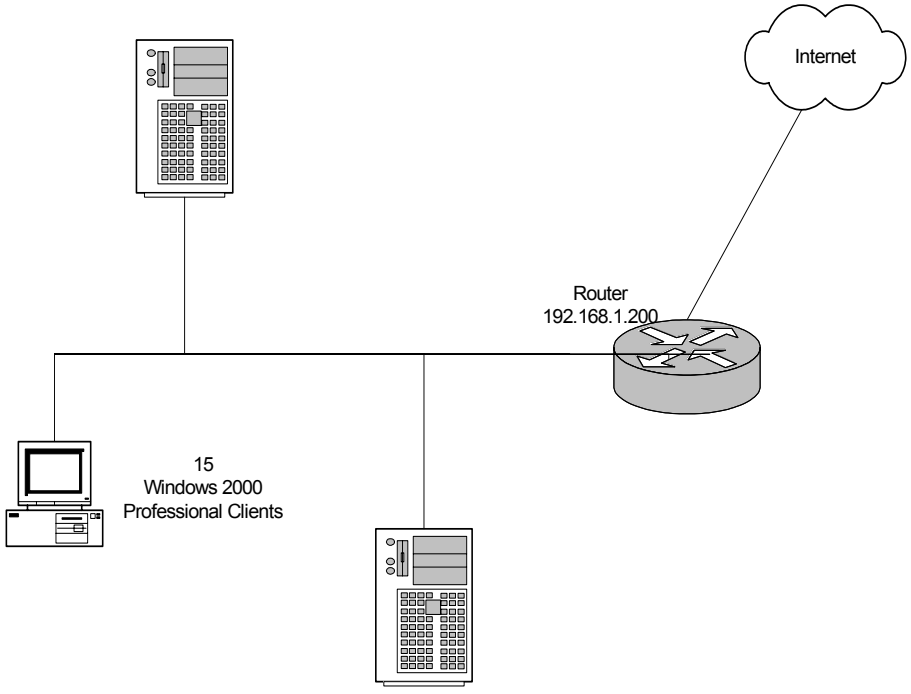
Wired Brain Coffee, Inc., is a small startup company located in Seattle that distributes specialty coffee around the world. They have hired you recently to do some basic networking and get the current employees up and running as soon as possible. Currently, Wired Brain Coffee (WBC) has 15 employees, but within a few months, there will be over 100 full time employees. You were hired as a Jr. Network Administrator to ensure that the first group of employees has no problems with the network. Your instructions are to build a basic network utilizing two servers. One server will act as a file server and the second server will be used as a DNS server. Initially, WBC will be set up as a workgroup with no domain controllers because management has not decided on the exact Active Directory design. You know that workgroups are better suited for very small networks and the WBC will quickly grow out of this type of network, but…this is what the suits want.

In Lab 1 you will install the DNS service on srv-1 and configure both a forward and a reverse lookup zone for WBC. The zone you create will be a Standard primary zone. Keep in mind, that you will not be creating a Windows 2000 domain, so Active Directory Integrated zones will not be available. After creating and configuring the zone, you will test the DNS server from client-1 using the nslookup command.



(figure 2)

Computer Name: SRV-1
IP: 192.168.1.201/24
OS: W2K Server/SP2
Services:
DNS

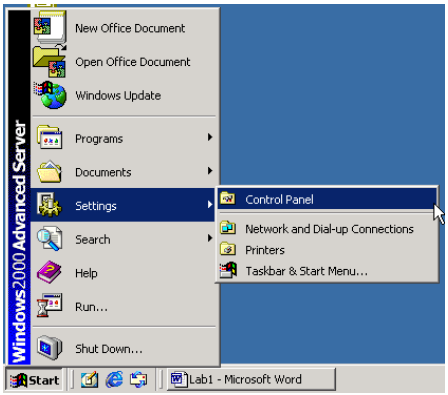


Computer Name: SRV-11
IP: 192.168.1.211/24
OS: W2K Server/SP2
Services:
File Server

(figure 3)

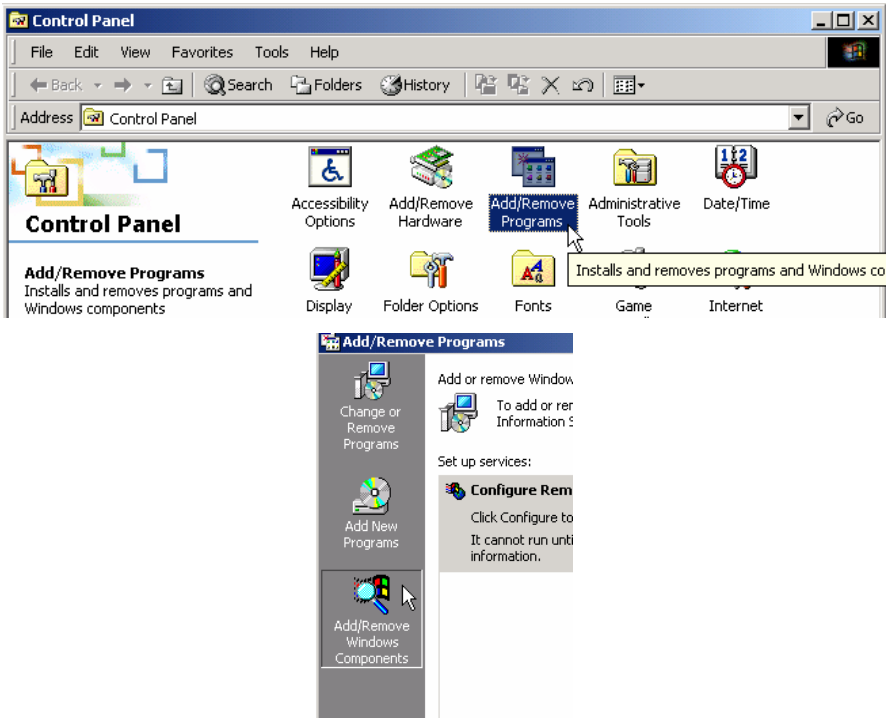
Installing DNS Service

1. On SRV-1 go to **Start→Settings→Control Panel.**



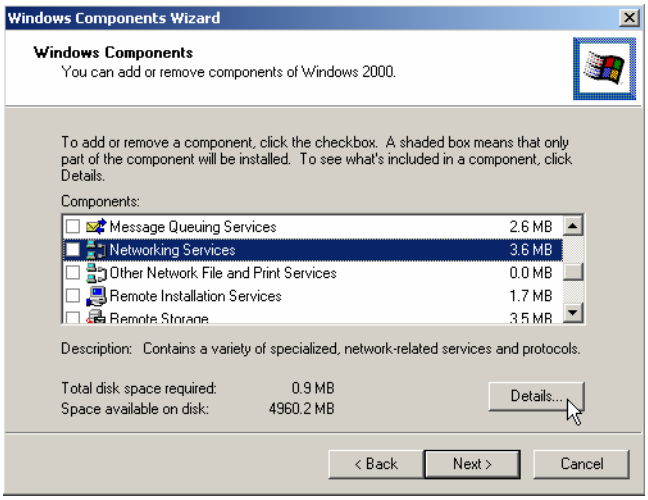
(figure 4)

2. Double click **Add/Remove Programs**, and then click on **Add/Remove Windows Components**.



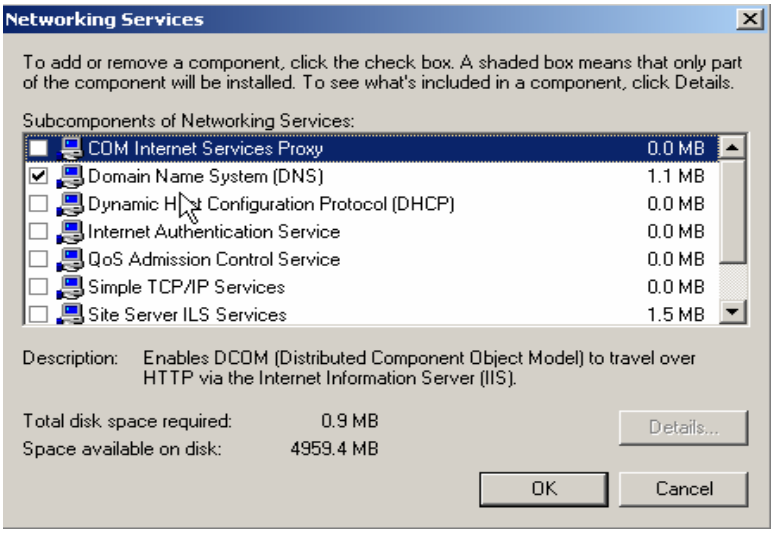
(figure 5)

3. On the next window scroll down and click on **Networking Services**. Then click **Details**.



(figure 6)

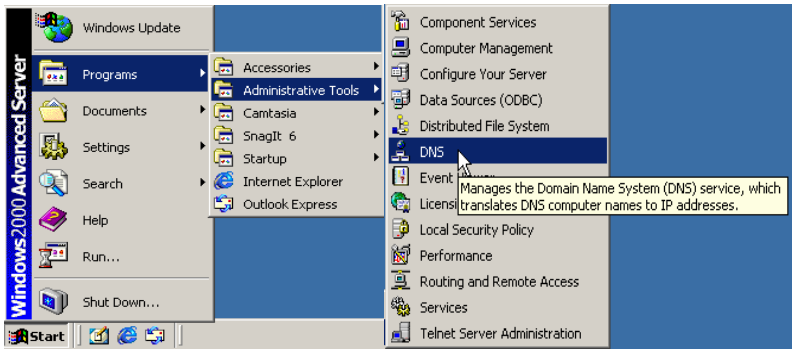
4. Under the Networking Services window find and select **Domain Name System (DNS)**. Click **OK**.



(figure 7)

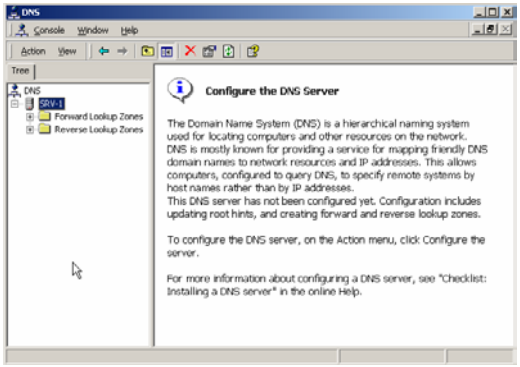
5. Click **Next** and make sure you have your Windows 2000 server CD in the CD-ROM Drive, or browse for the I386 source files if prompted. Click **Next** for the installation to begin. When the installation is done click **Finish**.

6. From your desktop go to **Start→Programs→Administrative Tools→DNS.**



(figure 8)

7. The DNS console will show SRV-1 indicating DNS has been installed on it. Below the server, notice the two folders named ***Forward Lookup Zones*** **and** ***Reverse Lookup Zones***.



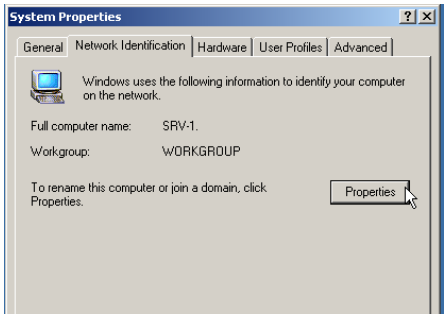
(figure 9)

Setting the Primary DNS Suffix

Before you go on you will need to add the primary DNS suffix to the computer name because the computer is not a part of a Windows 2000 domain. This setting controls where in the DNS namespace you would like this computer to exist. If you do not specify the primary DNS suffix, the computer will not be in the DNS domain wiredbraincoffee.com, and this lab will not work! By adding this suffix, you are effectively making wiredbraincoffee.com part of this computer's name. For example, the computer name for srv-1 would become srv-1.wiredbraincoffee.com.

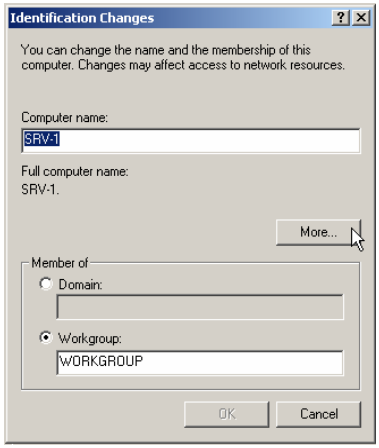
1. To change the computers name on SRV-1 right click on **My Computer** from the desktop and select **Properties**.

2. From properties, go to the **Network Identification** tab. From the Network Identification tab, click on **Properties**.



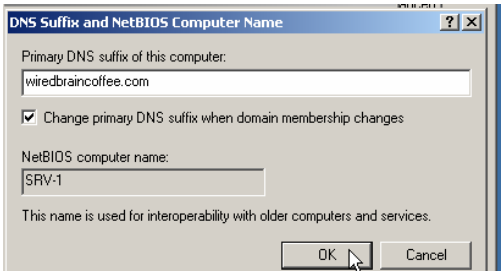
(figure 10)

3. On the Network Identification properties page click on the **More**…Button.



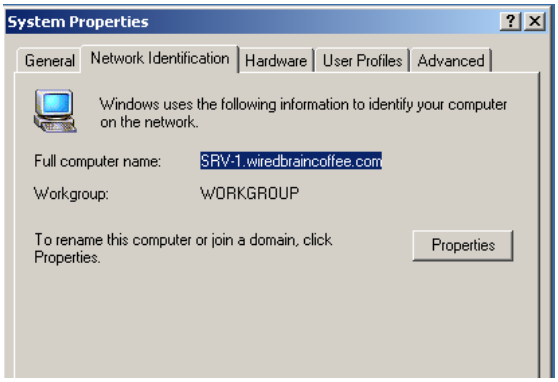
(figure 11)

4. That will bring up a dialog box where you can add the Primary DNS suffix of the computer. Type in ***wiredbraincoffee.com*** as the Primary DNS suffix and make sure the "**Change primary DNS suffix when domain membership changes"** option is selected. That way if the computer becomes a part of new domain other than wiredbraincoffee.com, the DNS suffix will change automatically. Click **OK**.



(figure 12)

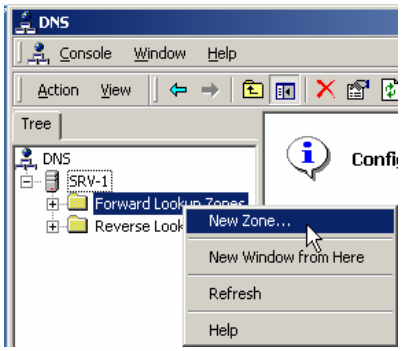
5. Click **OK** until you get back to the Network Identification tab on the **My Computer** properties. Before rebooting, look at the Full computer name and make sure it is correct. Click **OK**. There will be a pop up screen asking if you would like to reboot now for changes to take effect. Click **Yes** for the computer to reboot.



(figure 13)

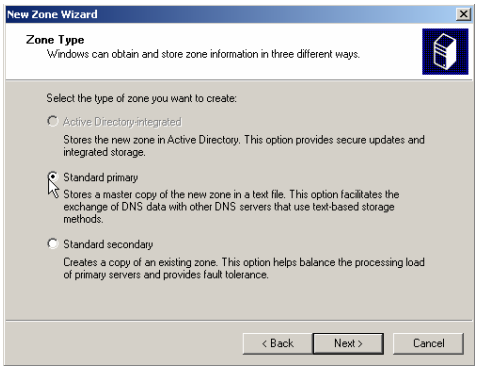
Creating a Forward Lookup Zone

1. Open the DNS console by clicking **Start→Programs→Administrative Tools→DNS.** The next step in setting up DNS is to create a Forward Lookup Zone. A forward lookup zone needs to be created to support Wired Brain Coffee's local network. The forward lookup zone will create a new DNS database that will contain the resource records of computers in the DNS domain. Right click on the **Forward Lookup Zones** folder and select **New Zone**.



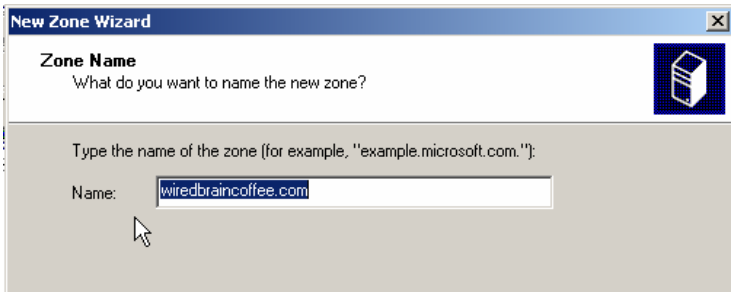
(figure 14)

2. This will start the new zone wizard that will walk you through the basic installation of a new Forward Lookup Zone. The first screen will be a welcome screen, click **Next.** The next screen will show the types of zones that you can create and a brief explanation of each. A Standard Primary zone will store the master copy of the DNS database; this is the selection you would make if this is the first zone you will be creating. A Standard Secondary is only created when you already have a Standard Primary DNS zone on another system. A Standard Secondary zone stores a read-only copy of the primary DNS zone's database by accepting zone transfers (copies) from the primary. Active directory is not installed on this server, so the Active Directory integrated option is grayed out. Choose **Standard Primary** and click **Next**.



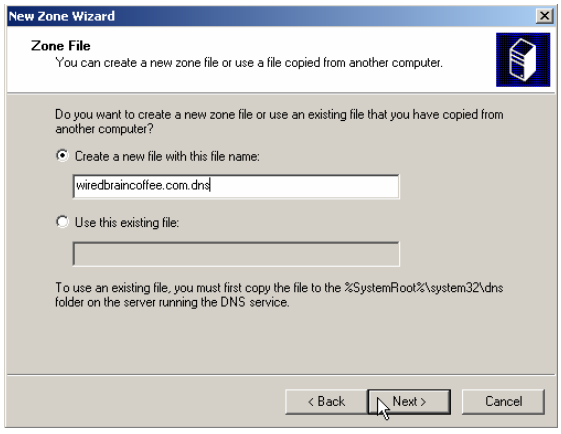
(figure 15)

3. The next screen asks for the name of the zone. Normally this would match the windows 2000 domain. In our example, Wired Brain Coffee does not have a domain setup (you are running stand-alone servers), so you could set up your DNS zone anyway you want. We are going to use **wiredbraincoffee.com** as the DNS zone, regardless. **It is very important** that the name of the zone matches the primary DNS suffix that you set on each computer.



(figure 16)

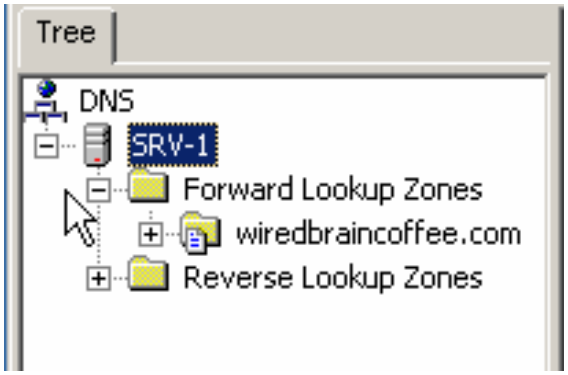
4. The next screen in the wizard will ask if you would like a new zone file created or if you would like to use an existing file. The only time you will likely use an existing file would be in a disaster recovery situation or if you were moving DNS from one server to another. Therefore, for our scenario, you will create a new file with the default name provided. Notice the file name is the name of the zone with the .dns extension. This is the default file name for any new zone. Click **Next**.



(figure 17)

5. The last screen of the wizard is just a summary of the settings that were selected. Look to make sure there are no mistakes and click on **Finish** to create the zone**.**

6. From the DNS console, you should now have ***wiredbraincoffee.com zone*** under the Forward Lookup Zones folder indicating that you successfully created the zone.

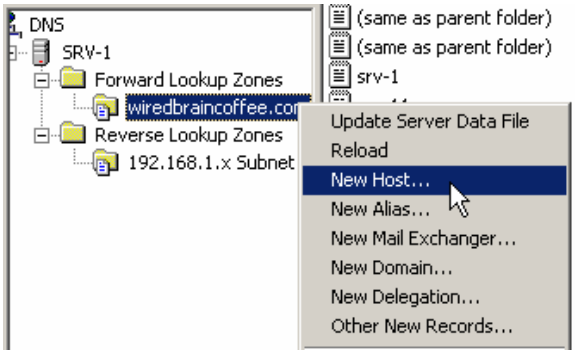


(figure 18)

Creating a Host Record

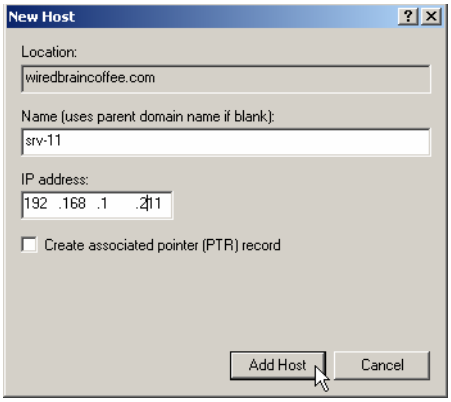
A host record is a simple record that DNS uses to relate names to associated IP addresses. For example if you needed to reach client-1 on your network but you did not know the IP address, you can use the host name, client-1 and DNS would resolve the name to an IP address so that you can reach client-1. In order for DNS to resolve the IP address of a host, a host (A) record must exist for that particular computer. In most cases, all of the computers on your network will have a host record associated with them.

1. To create new host records right click on the **wiredbraincoffee.com zone** and select **New Host**.



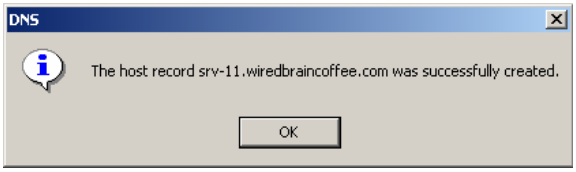
(figure 19)

2. That will bring up a dialog box that will ask for the name of the new record and the IP address for it. Let's create a record for another server on your network. In the name field, type in: *srv-11* and under IP address type in: *192.168.1.211*. For right now, do not check the box that reads **Create associated pointer (PTR) record**; we will come back to this later. Now click **Add host**.



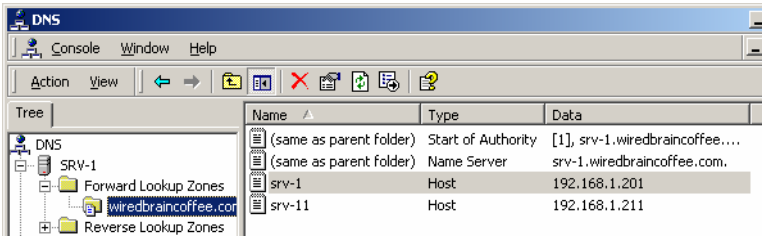
(figure 20)

3. A screen will pop up letting you know that the host record was successfully created. Click OK and that will bring you back to the New Host dialog box so that you can continue to create more host records. Click on **Done**.



(figure 21)

4. Now look at the wiredbraincoffee.com Forward Lookup Zone on the DNS console and notice that there is a host file for srv-11 that you just created and there is another one for srv-1. The host file for srv-1 was automatically created when you installed DNS and created a Forward Lookup Zone on the server.

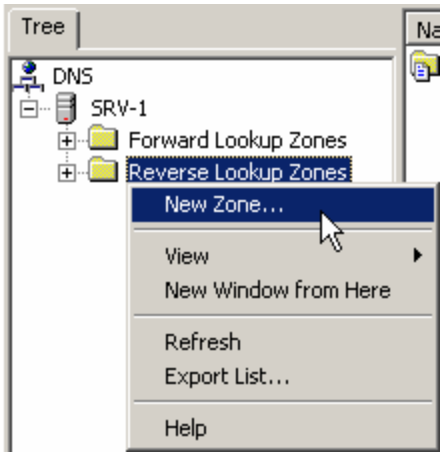


(figure 22)

Creating a Reverse Lookup Zone

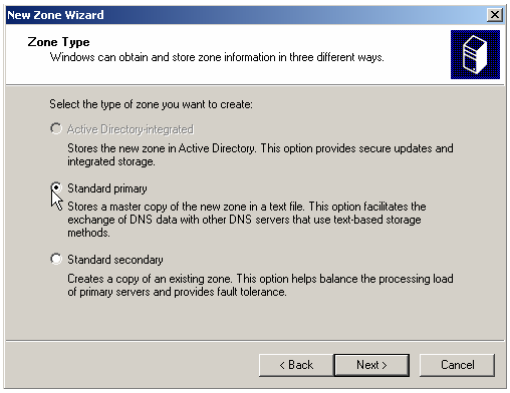
A reverse lookup zone is needed in order to resolve IP addresses to host names, the opposite of a forward lookup zone. Without a reverse lookup zone you will not be able to look up a host name based on its IP address. Reverse Lookup zones are primarily used to troubleshoot your network.

1. To create the reverse lookup zone, open the DNS console, right click on **the Reverse Lookup zone** folder and select **New Zone**.



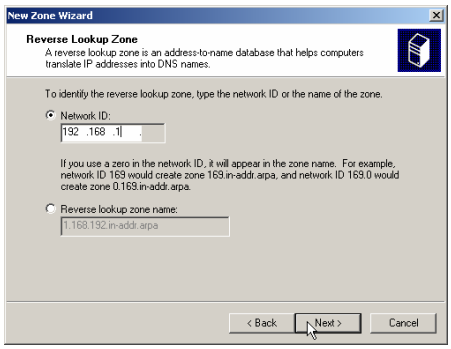
(figure 23)

2. That will start the new zone wizard similar to the one used for creating a Forward Lookup Zone. The first screen will be a welcome screen, click on Next. The next screen will show the types of zones that you can create and a brief explanation of each. Since this is the first Reverse Lookup Zone select **Standard Primary** and click **Next**.



(figure 24)

3. The next screen will ask for the network ID of the zone. Enter the Wired Brain Coffee network ID: ***192.168.1*** and click **Next**. Notice the reverse lookup zone name is automatically generated for you below. Click **Next**.

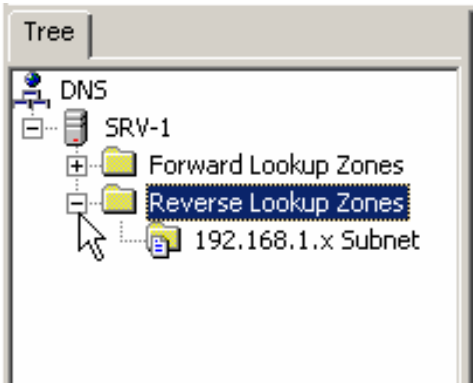


(figure 25)

4. The next screen will ask if you would like to create a new zone file or use an existing file. Again, the only time you will likely use an existing file would be in a disaster recovery situation, so for our scenario we will create a new file with the default name provided. Notice that the default file name was generated from the reverse lookup zone name on the previous screen. Click **Next**.

5. The last screen of the wizard is just a summary of the settings that were selected. Look to make sure there are no mistakes and click on **Finish** to create the zone.

6. From the DNS console, you should now have **192.168.1.x** subnet zone under the Reverse Lookup Zones folder indicating that you successfully created the zone.

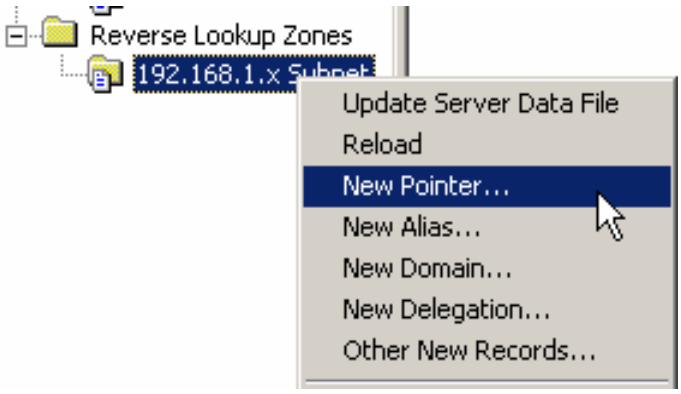


(figure 26)

Creating a PTR Record

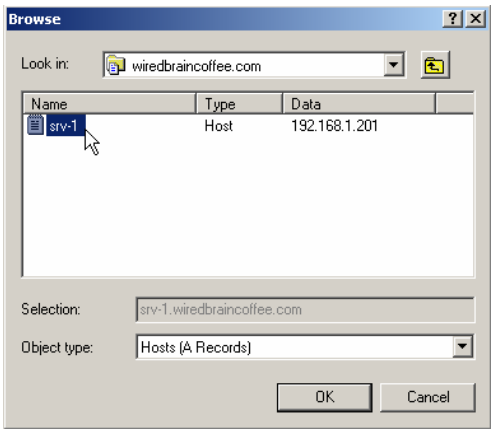
A pointer record is a simple record that does the opposite of a host record. This record uses the IP address to look up the associated host name. Create a PTR record for srv-1**.** Unlike the host record in the Forward Lookup zone, the pointer record is not created automatically in the Reverse Lookup Zone for srv-1.

1. To create a PTR record, right click on the **192.168.1.x subnet zone** and select **New Pointer**.



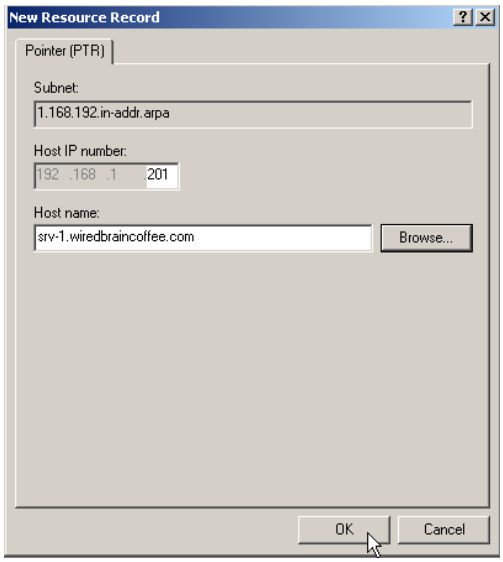
(figure 27)

2. That will bring up a dialog box that will ask for the host IP number and the host name that goes with the IP address. Enter the host IP number of ***201*** and browse for the associated host name srv-1. You will be navigating through the forward lookup zone of wiredbraincoffee.com for this record. Select **srv-1** and click **OK**.



(figure 28)

3. Confirm the information and then click **OK**.

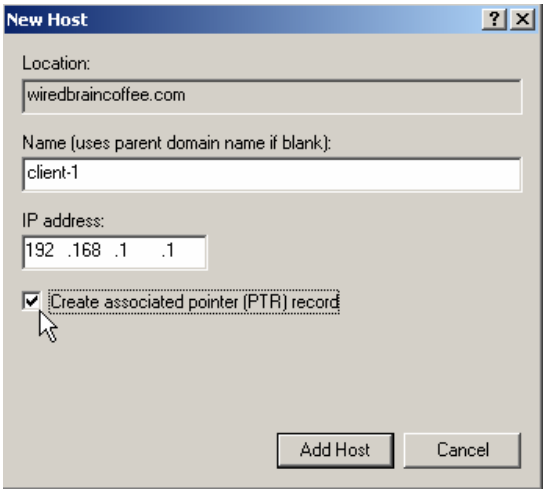


(figure 29)

4. After clicking OK notice there wasn't a pop up screen like there was when you created a host record, but you can check to make sure the entry was created by looking on the DNS console under the **192.168.1.x** subnet zone.

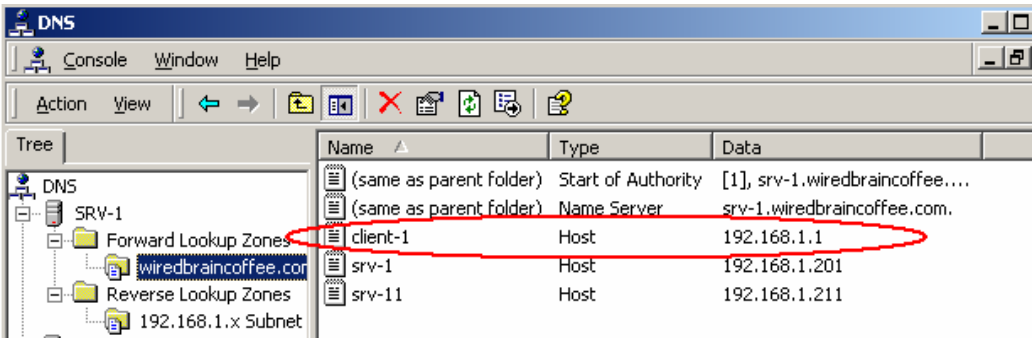
(figure 30)

5. Now that you have created a Forward and a Reverse Lookup Zone you can create a new host (A) record and have it create a PTR record at the same time. On the DNS console, right click on the wiredbraincoffee.com forward lookup zone and select **New Host**. When the dialog box comes up, you will create a host (A) record and a PTR record for client-1**.** For the name, type in ***client-1*** and for the IP address, type in ***192.168.1.1.*** This time, check the box that reads **Create associated pointer (PTR) record**. Click **Add Host,** a screen will pop up letting you know it was created successfully, click **OK** and then click **Done.**



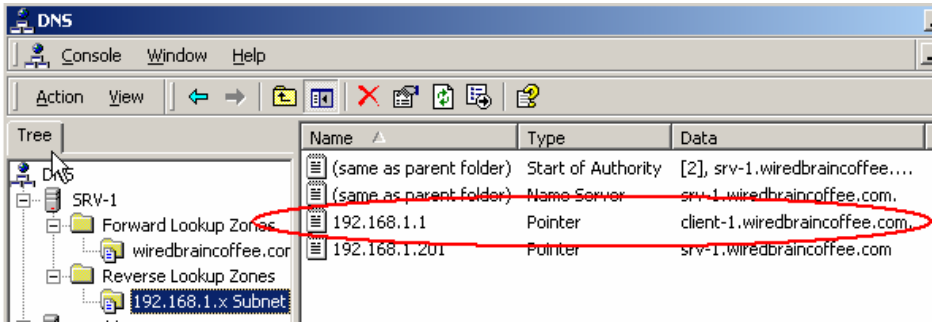
(figure 31)

6. Now look under the wiredbraincoffee.com zone you should see the host (A) record created for client-1.



(figure 32)

7. Also, look under the **192.168.1.x** subnet zone. If you did everything right, you should see the pointer record for client-1.



(figure 33)

8. Now for practice, create new host and pointer records for the following hosts.

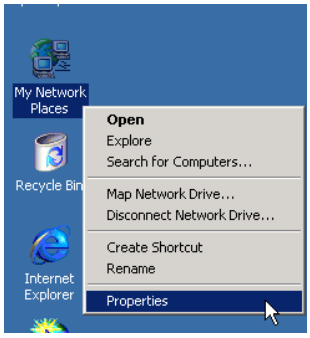
-Computer Name: SRV-11 IP Address: *192.168.1.211* (pointer record only)
-Computer Name: SRV-10 IP Address: *192.168.1.210*
-Computer Name: SRV-2 IP Address: *192.168.1.202*

Configuring a Client for DNS

There are a couple of ways to configure clients to use DNS. DNS clients can be configured with DHCP or they can be configured manually. Since we do not have a DHCP server on the network, we will manually configure client-1 to point to the DNS server for name resolution. Start by logging on to client-1.

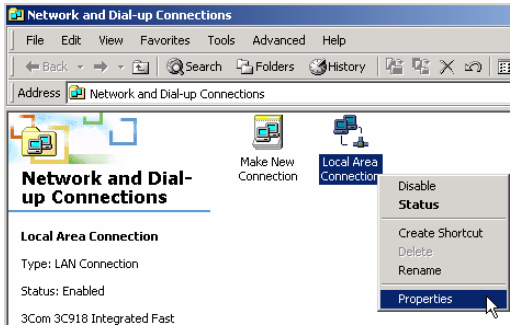
1. Before you continue, **make sure** you entered the Primary DNS suffix for client-1. The primary DNS suffix should be wiredbraincoffee.com (See Setting the Primary DNS suffix, earlier in this lab).

2. From the desktop right click on **My Network Places** and select **Properties**.



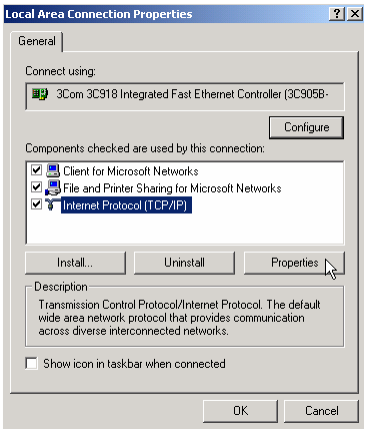
(figure 34)

3. From My Network Places properties page, right click on the **Local Area Connection** icon and select **Properties**.



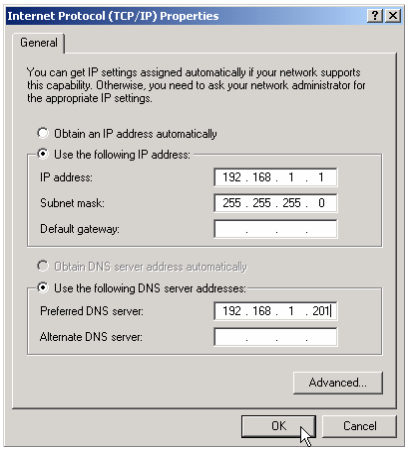
(figure 35)

4. From the Local Area Connection properties click **Internet Protocol (TCP/IP),** then **Properties**.



(figure 36)

5. From the TCP/IP properties page, select Use the following **IP address** and type in ***192.168.1.1*** and a subnet mask of ***255.255.255.0***. Leave the default gateway blank for now. Then, towards the bottom, select Use the following **DNS server addresses.** For the **preferred DNS server,** type in the IP address of the only DNS server presently on your network, ***192.168.1.201***. Leave the alternate DNS server blank right now. Click **OK** on this window and *all* of the open windows.

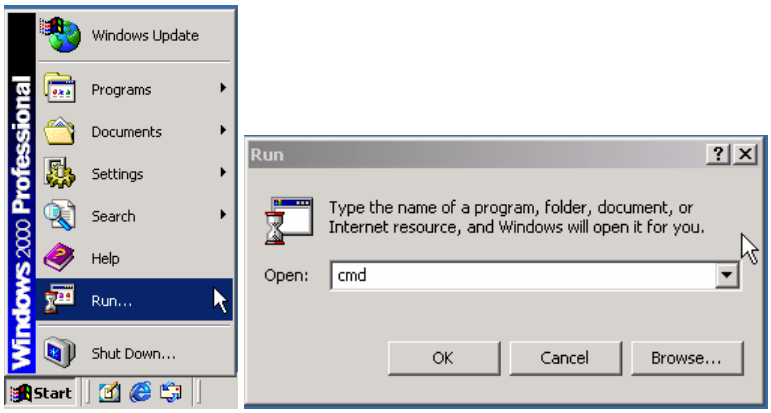


(figure 37)

Troubleshooting DNS with the NSLOOKUP Utility

NSLOOKUP is a diagnostic tool used with DNS. It is a command line utility, so you will need to run it from the command prompt. NSLOOKUP will allow you to talk directly to the DNS server and make simple queries.

1. Open the command prompt. Click on **Start→Run,** and type ***cmd*** in the Run dialog box. Click **OK.**



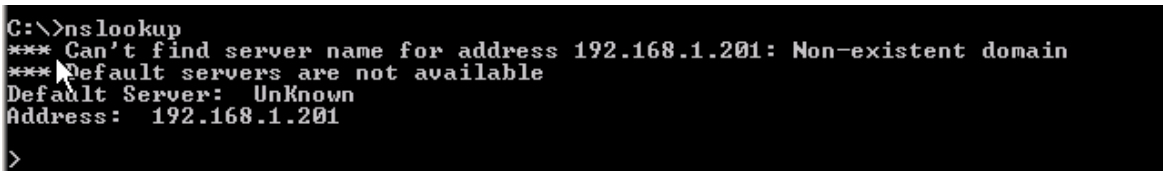
(figure 38)

2. From the command prompt, type in ***NSLOOKUP,*** then press **enter**. You should see the name and the IP address of the DNS server.

(figure 39)

******Important Note******

If you don't see the screen above and instead you see a screen similar to the screen below, you want to go back and check all of your settings to make sure that you configured everything correctly. Most likely, you did not create a Reverse Lookup Zone and a PTR record for the DNS server and you will not be able to use this utility until you correct this problem.



(figure 40)

3. Now try a simple query, type in ***SET TYPE=ANY,*** press **enter** and then type in ***WIREDBRAINCOFFEE.COM*** and press **enter**. This will give you a summary of information about DNS. Notice how the information on the screen matches up with the information within the properties of your DNS server.

(figure 41)

4. Now try to find the IP address of the computer name srv-11 with NSLOOKUP. Type in **srv-11** and press **enter.** That first two lines show the FQDN (Fully Qualified Domain Name) and the IP address of DNS server that did the name resolution. The result of the query will be displayed underneath. Type exit to leave the NSLOOKUP sub-command.

(figure 42)

Lab 2

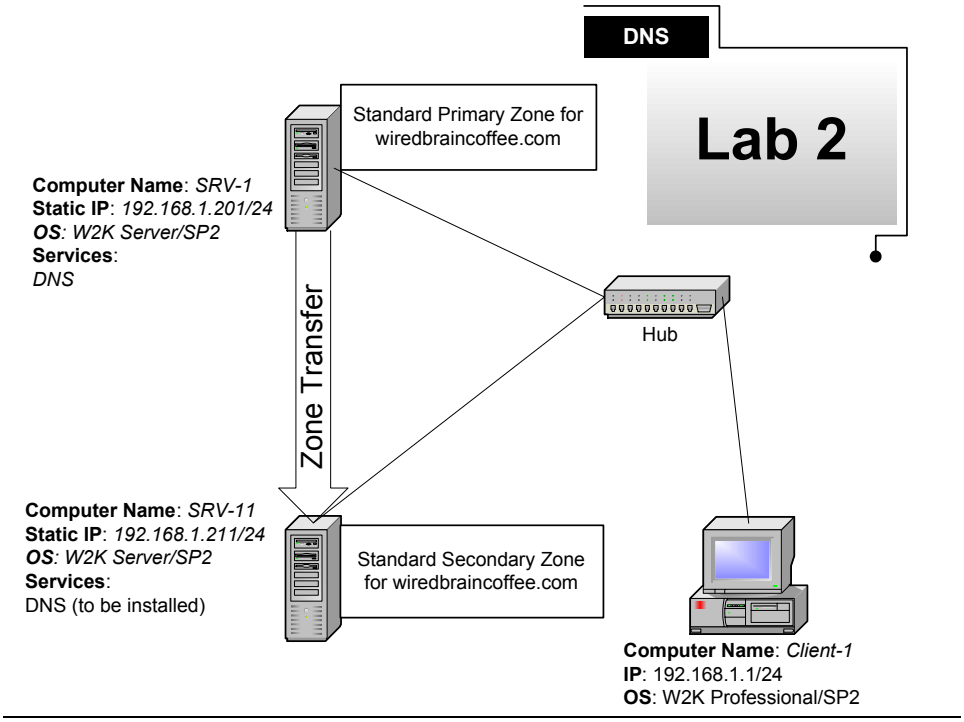
Managing the growth of Wired Brain Coffee's DNS Infrastructure

You will learn how to:

- Configure a Standard Secondary zone on a DNS Server
- Initiate zone transfers between DNS Servers
- Promote the Secondary DNS Server to a Primary DNS Server

Scenario

It has been a couple of weeks since you started working at Wired Brain Coffee and so far things could not be easier. There is no boss around, users do not bother you to much and you have plenty of free time to learn the "finer" points of your favorite game, Age of Empires. Today is shaping up to be different, though. Charlie, the new Network Manager, started today and has already put down the iron fist. "What is this DNS structure you created? Where do you think we will be if this *one* DNS server goes down?" Charlie asks you. "A month from now, we will have 100 more users pounding on this one DNS server," he continues. "Install a Secondary DNS server so our DNS structure has at least a little fault tolerance and make sure you know how to promote it to a Primary in case the current Primary fails." So much for conquering the Greek Civilization in Age of Empires, it is back to work!



(figure 43)

Installing the DNS Service

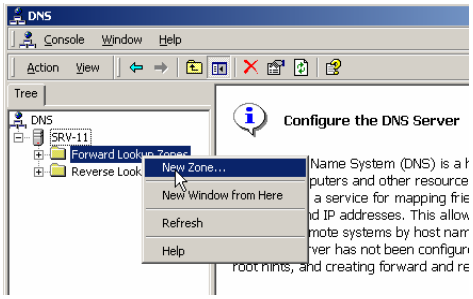
DNS should be installed on srv-11 in the same fashion it was installed on srv-1 in Lab 1. Go to **Start→Settings→Control Panel→Add/Remove Programs→Add/Remove Windows Components** and choose **DNS** from within Network Services.

******Important Note******

Before you continue, make sure you entered the Primary DNS suffix for srv-11, wiredbraincoffee.com (See Setting the Primary DNS suffix, Lab 1).

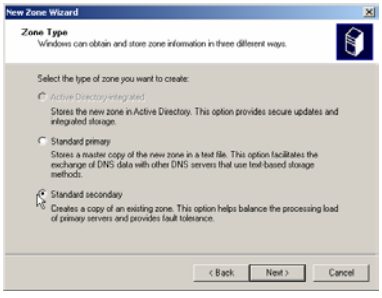
Creating a Forward Lookup Zone for the Secondary Server

1. You will need to create a forward lookup zone on srv-11 so it is able to perform name resolution for DNS clients. Right click on the **Forward Lookup Zones** folder and select **New Zone**.



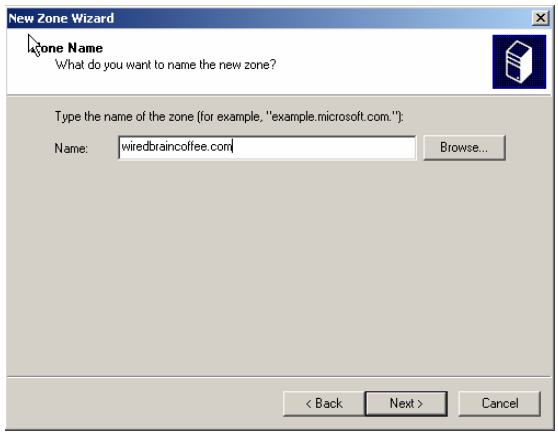
(figure 44)

2. This will start the New Zone Wizard, which will walk you through the basic installation of a new Forward Lookup Zone. The first screen will be a welcome screen, click **Next**. The next screen will show the types of zones that you can create and a brief explanation of each. This time you will select **Standard Secondary,** because you already created the standard primary for wiredbraincoffee.com on srv-1. Select **Standard Secondary**, and then click **Next**.



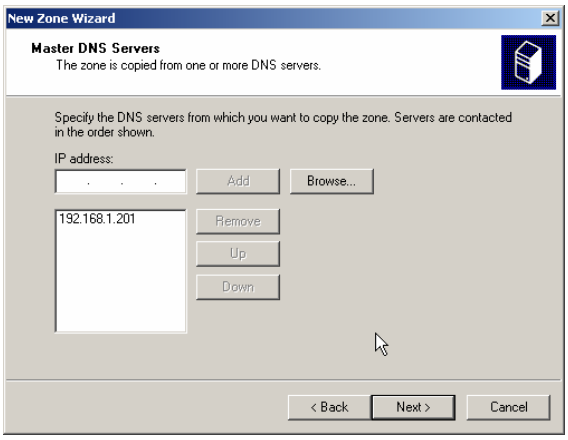
(figure 45)

3. The next screen asks for the name of the zone. This has to be the same name you used when you created the first zone on srv-1. Therefore type in ***wiredbraincoffee.com*** and click **Next**.



(figure 46)

4. The next screen of the wizard will ask for the address of the Master DNS server. Since this is a secondary DNS server, it has to retrieve the DNS database from another DNS server, the Standard Primary server in this case. Type in ***192.168.1.201,*** to tell the secondary how to find the primary **DNS server**. Click on Add, then click **Next**.



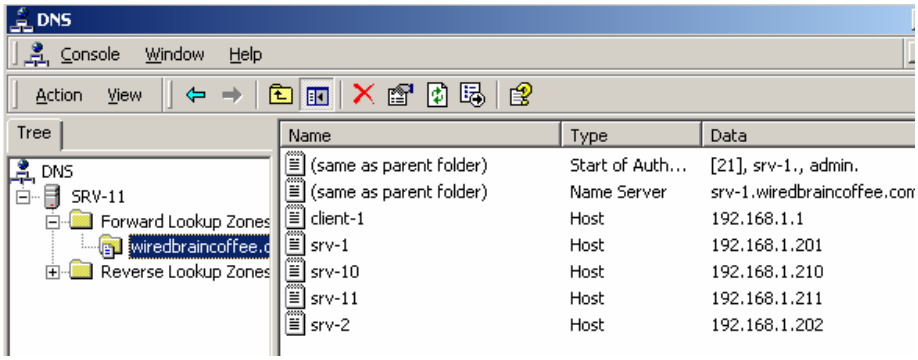
(figure 47)

The next screen will show you a summary of the settings you selected. Confirm that everything is correct and then click **Finish**.

From the DNS console on SRV-11, look under the **Forward Lookup Zones** folder and you should see the **wiredbraincoffee.com zone.** Under the zone should be all the entries that you created in the primary zone. This is because the secondary server copied (known as a zone transfer) the DNS database over from the primary standard server/zone.

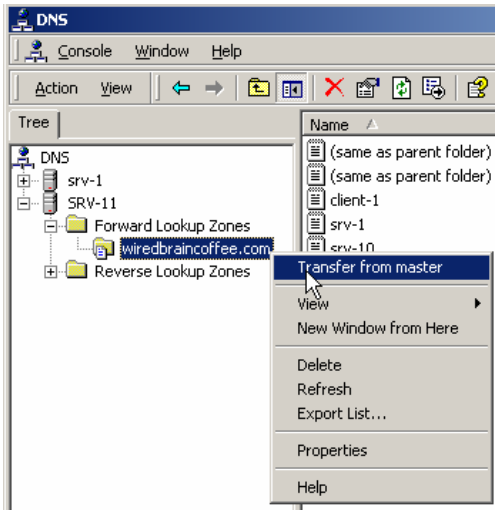
******Note******

The secondary server is a read only database; no changes can be made from here. All changes have to be made in the Primary zone.



(figure 48)

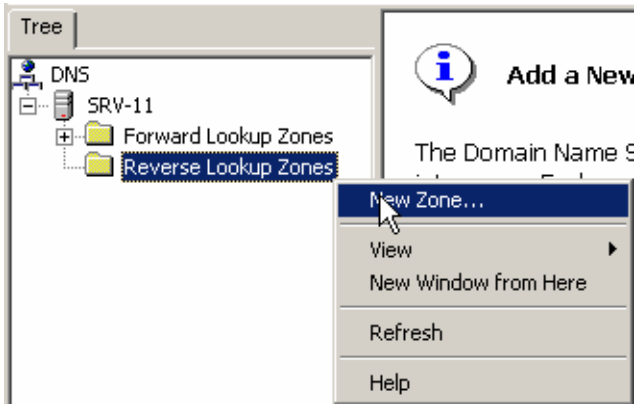
5. If the Primary DNS server does not copy the database over right away, you can force the zone transfer by right clicking on the **wiredbraincoffee.com zone folder** and selecting **Transfer from master.** This can be done at anytime, to force the secondary server to transfer the database and any changes that may have occurred.



(figure 49)

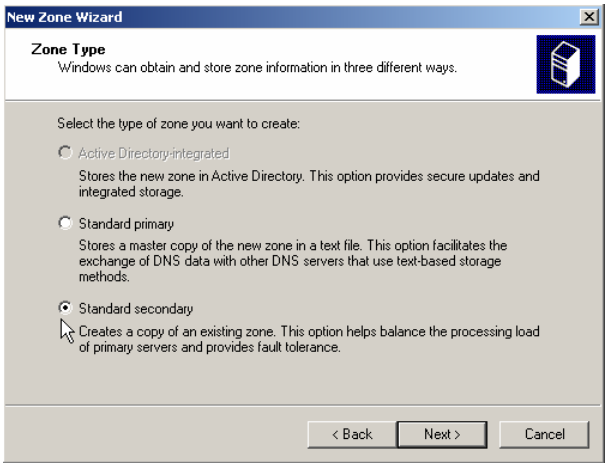
Creating a Reverse Lookup Zone on the Secondary Server

1. The next step is to configure srv-11 with a secondary zone for the primary reverse lookup zone that was created on srv-1. Within the DNS console right click on the **Reverse Lookup Zones** folder and select **New Zone**.



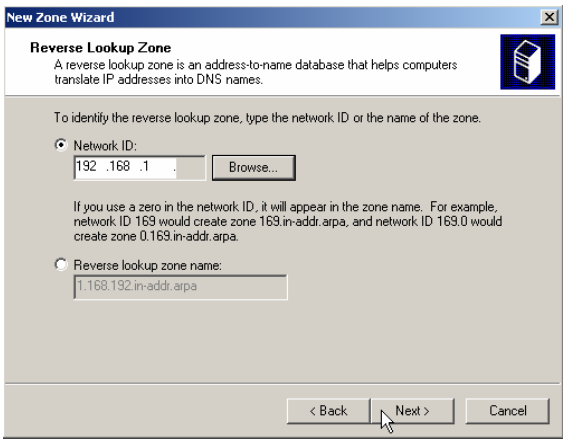
(figure 50)

2. This will start the new zone wizard. The first screen will be a welcome screen, click **Next.** The next screen will show the types of zones that you can create and a brief explanation of each. Since this is the second Reverse Lookup Zone you are going to create for WBC, select **Standard secondary** and click **Next**.



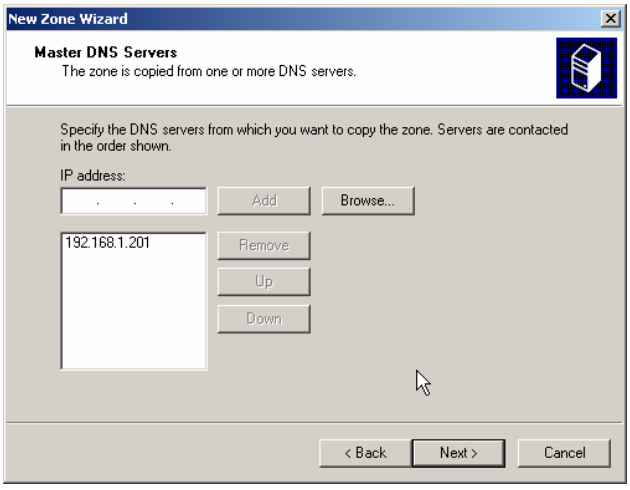
(figure 51)

3. The next screen will ask for the network ID of the zone. Enter the Wired Brain Coffee network ID: ***192.168.1***. Notice the reverse lookup zone name is automatically generated for you. Click **Next**.



(figure 52)

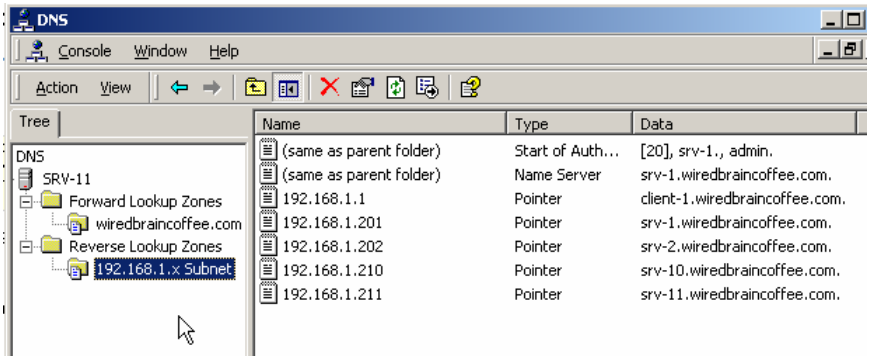
4. The next screen will ask you for the IP address of the master DNS server on your network. Type in the IP address of the Primary DNS server for the **192.168.1** subnet, which is **192.168.1.201**. Click on **Add** and then **Next**.



(figure 53)

5. The next screen will show you a summary of the settings you selected. Confirm that everything is correct and then click on **Finish**.

6. From the DNS console on SRV-11, you should now have the **192.168.1.x** zone under the Reverse Lookup Zone folder. Notice that all of the PTR records from the primary DNS server now appear under the **192.168.1.x** subnet zone.

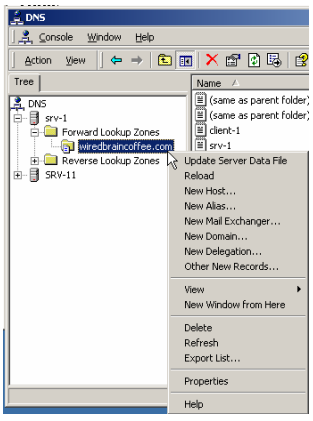


(figure 54)

7. If the Primary DNS server does not copy the database over right away you can force it to the same way as the forward lookup zone (Step 14), only, instead of right clicking on the wiredbraincoffee.com zone folder you would right click on the **192.168.1.x subnet folder.**

Configuring Zone Transfers

1. Open the DNS console on srv-1. Right click on the **wiredbraincoffee.com zone** and select **Properties**.



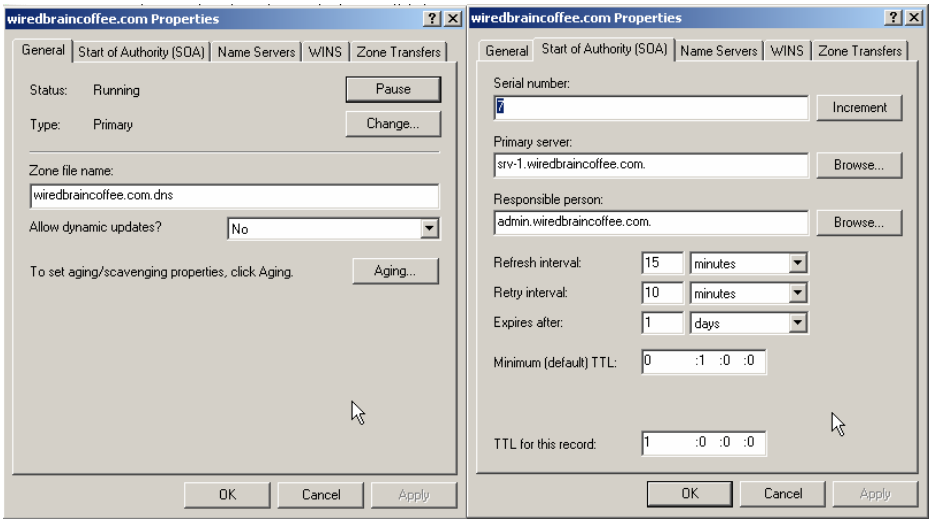
(figure 55)

*** Any setting configured here will be in effect for only the wiredbraincoffee.com zone and not the entire DNS server.

General Tab

On the general tab, you have the ability to pause the DNS service, change the zone types and control what type of updates will be allowed for this zone. Look at your choices for the type of zone and dynamic updates. The type of zone allows you to change the zone to a different type than you originally specified.

The dynamic updates drop down menu allows you to control whether dynamic updates are allowed for this zone. This is set to No by default. If you leave this setting at no, you will have to manually add and update all of the host records in the zone. It is a good idea to change this to **Yes,** in order to allow the client computers to automatically update themselves with the DNS server.



(figure 56)

2. Change the **Allow dynamic updates** setting to **Yes** then click on the **Start of Authority (SOA)** tab.

Start of Authority (SOA) Tab

The SOA tab displays information about the Start of Authority record in graphical form. The SOA record defines general information about the zone. The **serial number** field determines the current version of the zone. Every time a change is made to the records in the zone, the serial number is incremented by one. Secondary DNS servers can then tell if they have an updated copy of the zone by comparing the serial number of the data they have with the current serial number of the zone. The **Primary server** field specifies the DNS server that contains the master database for this zone. The **responsible person** field allows you to specify the email address of the person responsible for managing this zone. Notice

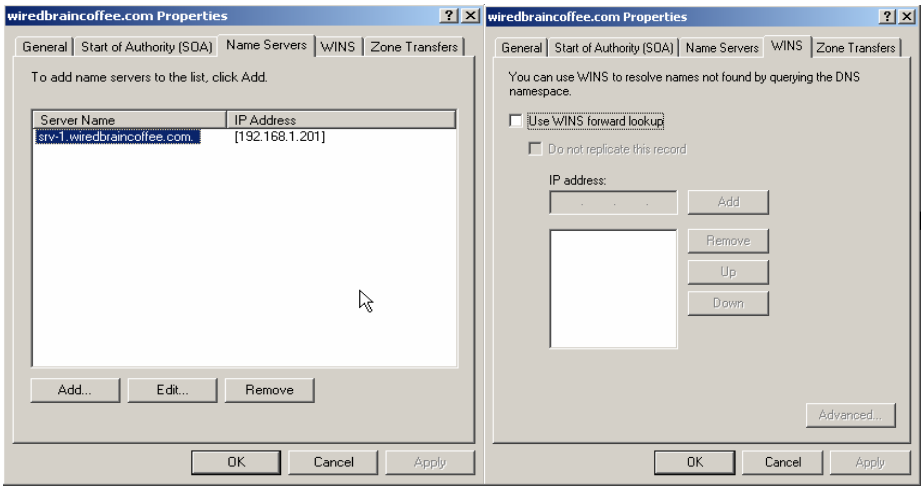
the form that this address takes on, admin.wiredbraincoffee.com is the DNS equivalent of admin@wiredbraincoffee.com. The **Refresh interval** controls how often DNS secondaries check with the primary DNS server for an update. By default, the secondary DNS servers "bother" the primary DNS servers every 15 minutes for their current information. The **Retry interval** field specifies how soon to check back with the primary DNS server if it was not available the first time. **Expires after**, tells the secondaries how long to wait without hearing from the primary, before they should throw out all of the information they learned from the primary. Therefore, by default, after 24 hours, the secondary DNS server would determine that all of its current DNS records for the zone were invalid and quit functioning.

The **minimum (default) TTL** indicates the "Time to Live" or how long a computer will cache the results of a DNS resolution it has received from this DNS server. The default is 1 hour. The **TTL for this record** is exactly that, the time to live for the start of authority record itself.

3. From the SOA tab, change the **Refresh interval to 60 minutes** (this will slow down how often the Secondary DNS servers ask the Primary for a zone transfer). Also, change the Minimum (default) TTL to 1 day, **1:0:0:0** (1 day, 0 hours, 0 minutes, 0 seconds). Click on the **Name Servers** tab.

Name Servers Tab

This tab is used to add name servers that will hold a copy of the zone database. On this screen you can add, edit or remove any servers that are running DNS. By default, only the primary DNS server will be added. Click on the **WINS** tab.



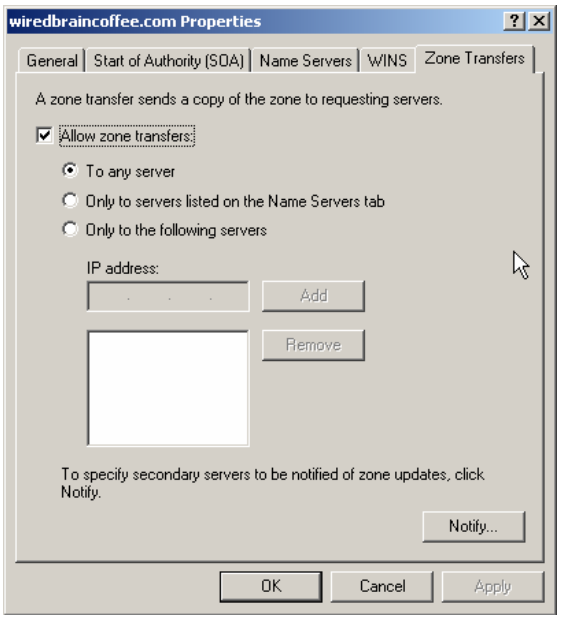
(figure 57)

WINS Tab

If you want a WINS server to help in name resolution, you can select the box in this tab and specify the IP address of the WINS server. This was a good option with NT 4.0 because WINS is very often used and the WINS database is usually more populated than the DNS database. In Windows 2000, DNS handles most of the name resolution duties and WINS is not nearly as important. Click on the **Zone Transfers** tab.

Zone Transfers Tab

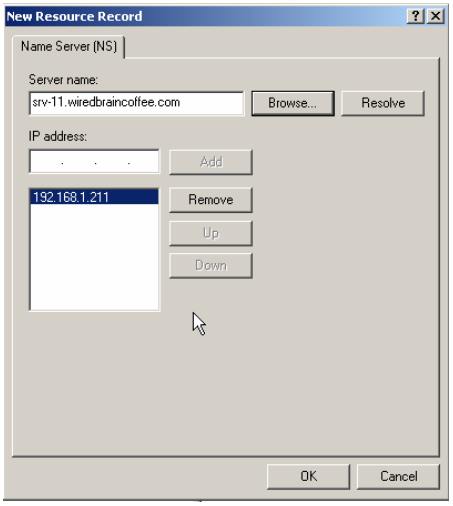
This tab allows you to control how zone transfers are handled. By default, the Allow zone transfers box is selected and the "To any server" option is specified. This default setting allows all of the zone data, computer names and IP addresses, to be transferred to any computer that asks, not the most secure setting in the world. A better choice, is the **Only to servers listed on the Name Servers tab** selection. As you might guess, this utilizes the Name Servers tab that we spoke of previously, to only allow zone transfers to computers that are listed on this tab. You can also specify individual servers by entering their IP addresses.



(figure 58)

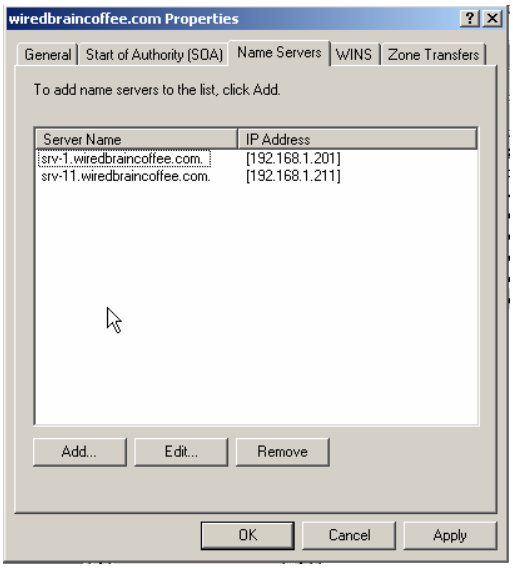
4. For the wiredbraincoffee.com zone, select the **Only to servers on the Name Servers tab** option. Click **Apply**

5. Next, you will add srv-11 to the Name Servers list, so that zone transfers will take place from srv-1 to srv-11. Click on the **Name Servers** Tab. You can type in the FQDN for **srv-11.wiredbraincoffee.com** or you can **browse** to the host file. Click **Add** to enter the IP address below. When finished click **OK**.



(figure 59)

6. You should now see both srv-1 and srv-11 listed on the Name Servers tab. These will be the only servers that are allowed to transfer the wiredbraincoffee.com zone database. Click **OK**.



(figure 60)

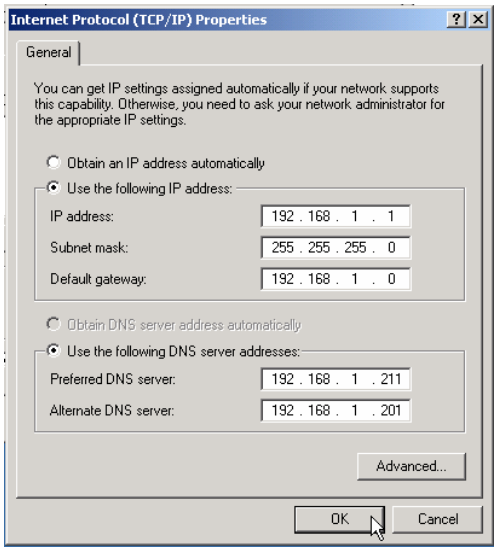
Configuring DNS Clients with a Preferred and Alternate DNS Server

1. Log on to client-1. From the desktop right click on **My Network Places** and select **Properties.**

2. From My Network Places properties page, right click on the **Local Area Connection** icon and select **Properties**.

3. From the Local Area Connection properties click **Internet Protocol (TCP/IP)** then click **Properties.**

4. On the properties screen, type in the IP address of srv-11 (**192.168.1.211**) as the **Preferred DNS server**. Now type in the IP address of srv-1 (**192.168.1.201**) as the **Alternate DNS server**. Click **OK**. Click **OK** again. **Close** the **My Network Places** window.



(figure 61)

5. Open the command prompt. Type in **NSLOOKUP.** The first line will now show the default server and its IP address. **Srv-11** should be listed.

```
C:\>nslookup
Default Server:  srv-11.wiredbraincoffee.com
Address:  192.168.1.211
```

(figure 62)

6. Now try a simple query. Type in ***SET TYPE=ANY,*** press **enter** and then type in ***WIREDBRAINCOFFEE.COM*** and press **enter**. Notice how the first two lines show information for srv-11. That is because it queried that server to gather the information given.

```
C:\>nslookup
Default Server:  srv-11.wiredbraincoffee.com
Address:  192.168.1.211

> set type=any
> wiredbraincoffee.com
Server:  srv-11.wiredbraincoffee.com
Address:  192.168.1.211

wiredbraincoffee.com    nameserver = srv-1.wiredbraincoffee.com
wiredbraincoffee.com    nameserver = srv-11.wiredbraincoffee.com
wiredbraincoffee.com
        primary name server = srv-1.wiredbraincoffee.com
        responsible mail addr = admin.wiredbraincoffee.com
        serial  = 13
        refresh = 900 (15 mins)
        retry   = 600 (10 mins)
        expire  = 86400 (1 day)
        default TTL = 3600 (1 hour)
srv-1.wiredbraincoffee.com      internet address = 192.168.1.201
srv-11.wiredbraincoffee.com     internet address = 192.168.1.211
>
```

(figure 63)

7. The secondary DNS server, srv-11, is now being used, because it was set as the Preferred DNS server for client-1. This is the server that client-1 will send any DNS queries to. If this server were to go offline for any reason, the client would then try to send the DNS query to the alternate server, which in this case would be srv-1.

8. In order to simulate this, you will need to type **EXIT** and **close** the command prompt. Next, find the cable that goes from the hub to srv-11 and **unplug** it.

9. From client-1, **open** the command prompt and run the **NSLOOKUP** command. It will tell you that the DNS request timed out and it was unable to find the server name for the address 192.168.1.211. Under that, it will say that the default server is srv-1, which is the server that was set as the alternate server in case the preferred server was not available.

```
C:\>nslookup
DNS request timed out.
    timeout was 2 seconds.
*** Can't find server name for address 192.168.1.211: Timed out
Default Server:  srv-1.wiredbraincoffee.com
Address:  192.168.1.201
```

(figure 64)

10. Now try a simple query. Type in ***SET TYPE=ANY*** press **enter** then type in ***WIREDBRAINCOFFEE.COM*** and press **enter**. Notice how all of the information is the same as before, when you ran the query from srv-11. Even though the information is obtained from a different DNS server, the zone information is the same.

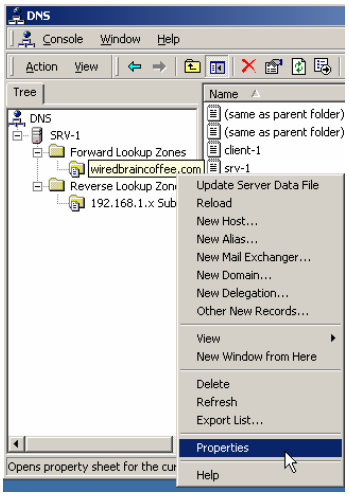
```
C:\>nslookup
DNS request timed out.
    timeout was 2 seconds.
*** Can't find server name for address 192.168.1.211: Timed out
Default Server:  srv-1.wiredbraincoffee.com
Address:  192.168.1.201

> set type=any
> wiredbraincoffee.com
Server:  srv-1.wiredbraincoffee.com
Address:  192.168.1.201

wiredbraincoffee.com    nameserver = srv-1.wiredbraincoffee.com
wiredbraincoffee.com    nameserver = srv-11.wiredbraincoffee.com
wiredbraincoffee.com
        primary name server = srv-1.wiredbraincoffee.com
        responsible mail addr = admin.wiredbraincoffee.com
        serial  = 13
        refresh = 900 (15 mins)
        retry   = 600 (10 mins)
        expire  = 86400 (1 day)
        default TTL = 3600 (1 hour)
srv-1.wiredbraincoffee.com      internet address = 192.168.1.201
srv-11.wiredbraincoffee.com     internet address = 192.168.1.211
>
```

(figure 65)

Promoting the Secondary DNS Server to a Primary DNS Server

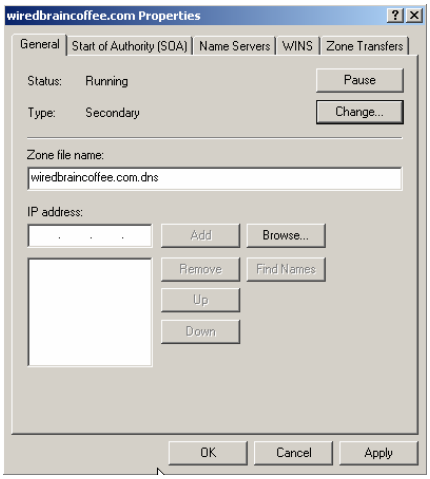
What would happen if srv-1 crashed? Would you hold off on additions or changes until srv-1 was back online? If the Standard Primary DNS server ever crashes or needs to be brought down, a Standard Secondary can be promoted to take its place.

1. Log on to srv-11 and open the DNS console. Right click on the **wiredbraincoffee.com** zone and select **Properties**.



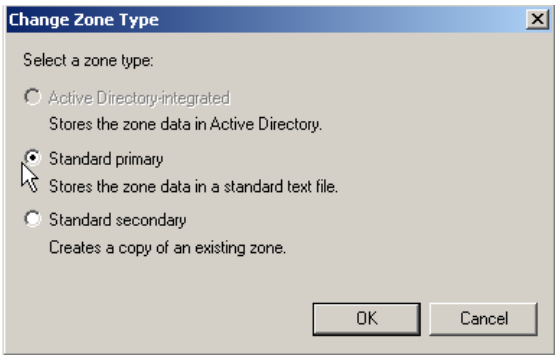
(figure 66)

2. On the General tab, notice that this is a Secondary DNS server. Click on the button that says **Change**…



(figure 67)

3. On the pop-up screen, select **Standard Primary** and click **OK**.



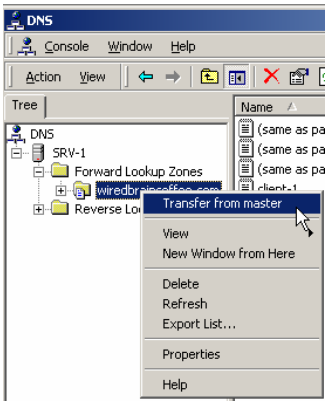
(figure 68)

4. On the General Tab make sure that it now says **Type: Primary** and click **OK**.

5. Follow the same steps for the **192.168.1.x** reverse lookup zone. You have now made srv-11 the primary DNS server for the wiredbraincoffe.com zone. After srv-1 is back in working order, you need to make sure that only one server is configured to host the primary zone for wiredbraincoffee.com or you will have two separate zone databases for wiredbraincoffee.com.

6. Plug the **srv-1 cable** back into the hub. Open the **DNS console** and change the **forward lookup zone** and the **reverse lookup zone** to **Standard secondary zones**, pointing to **srv-11** as the master server.

7. From the DNS console right click on **wiredbraincoffee.com** and select **Transfer from master**. This will transfer any zone updates from srv-11 that srv-1 doesn't already have.



(figure 69)

8. Repeat these steps for the **192.168.1.x** reverse lookup zone.

Lab 3

Modifying the DNS Infrastructure to handle growth at Wired Brain Coffee, Inc.

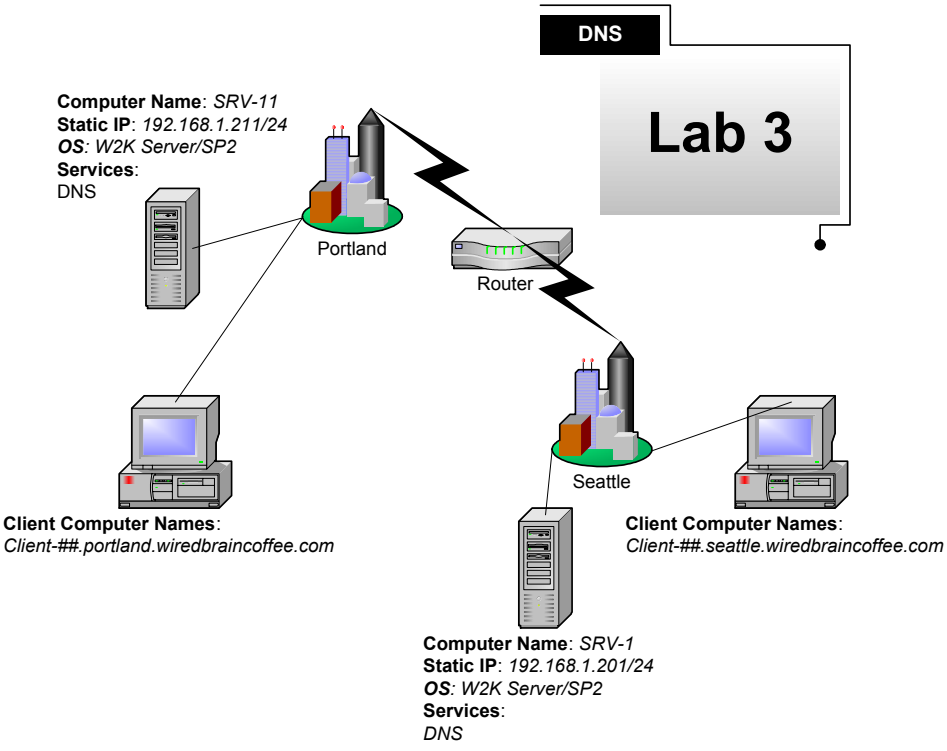
You will learn how to:

- Create additional DNS domains
- Differentiate between a zone and a domain
- Delegate authority to a DNS zone
- Configure a DNS Forwarder
- Install & Configure a Caching-only DNS Server

Scenario

Wired Brain Coffee, Inc. has grown substantially since it first opened doors two months ago. It is unbelievable how much you have learned in such a short time. Your network manager, Charlie, now wants you to organize the DNS structure for even more growth. WBC will be expanding soon to Portland, Oregon, and Charlie wants you to organize DNS so that resources in Portland will have "Portland" as part of their host name. Charlie would also like you to research options to speed up DNS resolution time. Performance is adequate now, but who knows, with the network expanding so rapidly, maybe there is a better way of setting up DNS.

In Lab 3 you will work with several tricky concepts. First, you will create DNS domains within wiredbraincoffee.com and then you will delegate authority to one of them, turning it into a zone. The difference between zones, DNS domains & Windows 2000 domains is sometimes a difficult concept to grasp, so take a close look at the details within this lab and try to get a better understanding of their differences. You will also be exposed to the configuration and theory behind both DNS forwarders and DNS caching-only servers.



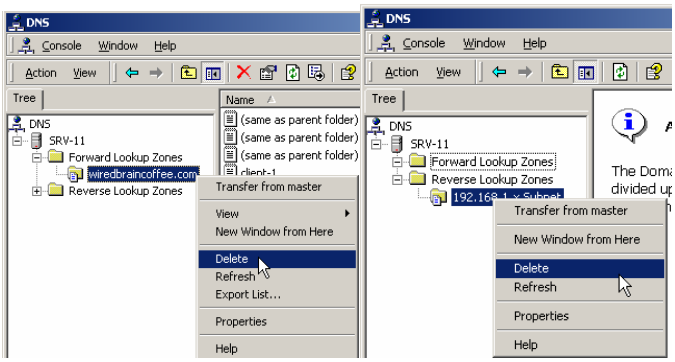
(figure 70)

******Important Note******

Before you get started with Lab 3, you need to delete the secondary zone from srv-11. Under normal circumstances, this would not be done, but for the purpose of this lab you will do this to ensure that we are at a common starting point.

1. Log on to **srv-11** and open the **DNS console**. Right click on wiredbraincoffee.com and select **Delete**. A screen will pop up asking if you are sure you want to delete the zone. Click **Yes**.

2. Next, you will delete the reverse lookup zone for the **192.168.1.x** subnet.



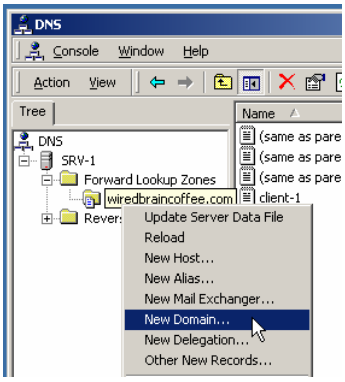
(figure 71)

DNS Domains

The concept of a DNS domain, often, is enough to completely throw students and IT professionals for a loop. It is easy to understand the concept of an Internet or public domain name such as trainsignal.com or Microsoft.com. These are both DNS domains. The concept starts to become a bit fuzzier when you explore a private DNS structure within a company. What is a DNS domain for? How is it different than an Active Directory domain? Or a zone for that matter? A lot of times, there is no difference. If you set up a Windows 2000 domain named wiredbraincoffee.com, by default, you will also have a DNS domain and zone named wiredbraincoffee.com. In the next section, you will be creating DNS domains **not** Windows 2000 Active Directory domains. Creating DNS domains outside of your Windows 2000 domain structure is not that common, but it can be done. In our example, Wired Brain Coffee is expanding to Portland and they would like to be able to use host names to differentiate between machines in Seattle and machines in Portland. Creating DNS domains allows you to split up the DNS namespace. For example, a srv-20 in Portland would take on the name srv-20.portland.wiredbraincoffee.com and a client-50 in Seattle would take on the name client-50.seattle.wiredbraincoffee.com. The thing to remember here is that there is still only **one** Active Directory domain and only **one** DNS zone. What then, is the purpose of DNS domains? Creating DNS domains simply gives you the ability to better organize your resources.

Creating Additional DNS Domains

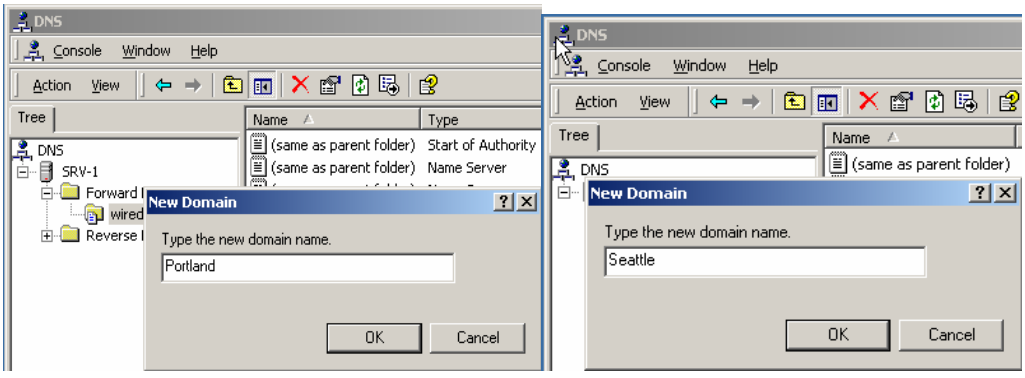
1. Log on to srv-1 and open the DNS console. Right click on **wiredbraincoffee.com** and select **New Domain**.



(figure 72)

2. A screen will pop up asking for the new DNS domain name. Type in **Portland** and Click **OK**.

3. Right click on **wiredbraincoffee.com** again and select **New Domain**. Type in **Seattle** and Click **OK**



(figure 73)

******Important Note******

Keep in mind that the Primary DNS Suffix for the client computers would have to be changed on each computer to reflect which domain you want their host records created in. You would then just create host records for computers in the appropriate domain. Automatic updates will also work, provided you changed the Primary DNS suffix as described above.

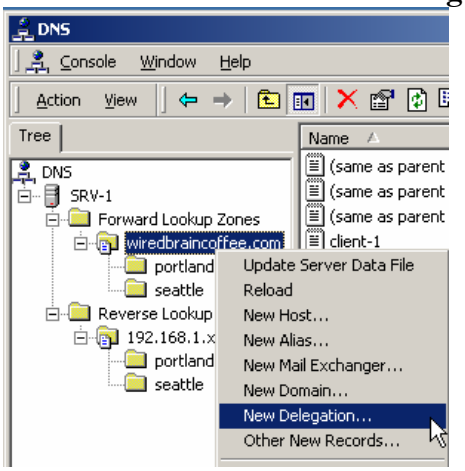
DNS Zones

In the section above, you learned what a DNS domain is and how to set them up. Now we will shift our focus to DNS zones. A DNS zone is formed when go through the New Zone wizard within the DNS console. When you create a new zone, recall that the wizard actually prompts you for the name of the file that will represent the zone's database. So, if you create a zone named wiredbraincoffee.com, a database file (named wiredbraincoffee.com.dns by default) will be generated for this particular zone. Now, when you create a DNS domain, you are adding a name to the DNS namespace (i.e. Portland and Seattle), but you are not creating a new database of resource records. All of the resource records, in both of these domains, are still kept in the wiredbraincoffee.com zone database.

In the following section, you will delegate authority of a new DNS zone to a different DNS server. In other words, not only will you add names to the namespace (like you did with DNS domains), but you will also divide your DNS database up and give a different DNS server responsibility over part of the DNS namespace. For example, using DNS domains, srv-1 held the primary database, which included domains for wiredbraincoffee.com, Seattle and Portland. In the following section, you will delegate authority for the Portland domain to srv-11. This means that srv-11 will now hold the primary copy of the DNS database, but only for the Portland portion. Also, srv-1 will no longer resolve names for computers in portland.wiredbraincoffee.com, these requests would be passed down to the server that is authoritative for Portland, srv-11. So, why would you want to use a zone? Zones are important because they allow you to divide the DNS database into smaller parts, making it more efficient. They also allow you to delegate different parts of the DNS structure to different administrators in different geographical regions.

Delegating Authority of a DNS Zone

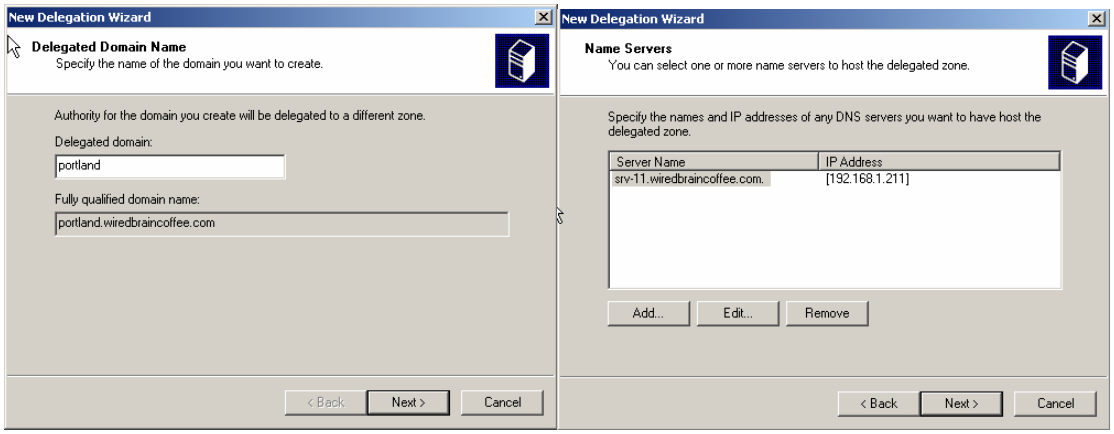
1. Right click on **wiredbraincoffee.com** and select **New Delegation**.



(figure 74)

2. That will open the delegation wizard. Click **Next** on the welcome screen. The next screen will ask for the domain name that will be delegated. You are delegating the Portland domain, so you will type in **Portland** and click **Next**.

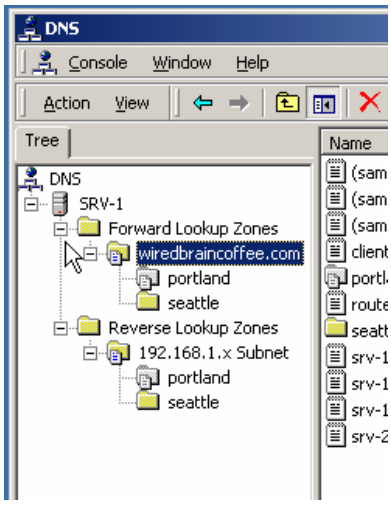
3. This screen will ask you for the Name Servers that the zone will be delegated to. This server will hold the zone database and is considered authoritative over the specified domain. Click **Add**. Enter the IP address and name of **SRV-11** or browse to the host file for **SRV-11**. Click **Next.**



(figure 75)

4. The final screen will be a summary of the information you entered. Make sure there are no mistakes and click **Finish**.

5. On the DNS console, the Portland DNS domain, which was represented by a yellow folder previously, should now be gray (you may have to hit refresh). This indicates that Portland is still a part of the DNS infrastructure, but authority for it has been delegated out to another server.



(figure 76)

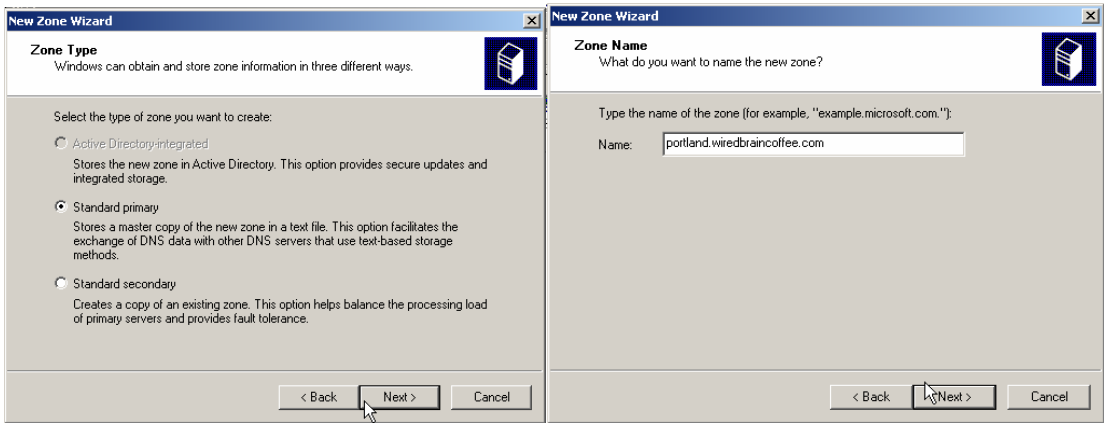
Creating a Standard Primary Zone for the Delegated Zone

Before srv-11 can start resolving host names to IP addresses, a **forward lookup zone** has to be created for **portland.wiredbraincoffee.com**.

1. Log on to srv-11 and open the DNS console. Right click on the **Forward Lookup Zones** Folder and select **New Zone**. This will start the new zone wizard. The first screen will be the welcome screen. Click **Next**.

2. On the next screen select **Standard primary** for the zone type. Click **Next**.

3. On the next screen type in **portland.wiredbraincoffee.com** as the zone name. Click **Next.**



(figure 77)

4. Leave the default name for the file as **portland.wiredbraincoffee.com.dns**. Click **Next**.

5. The next screen is a summary of all the information you entered. Make sure there are no mistakes and click **Finish**.

6. On the DNS console right click on the **Reverse Lookup Zones** folder and select **New Zone**. That will start the new zone wizard. The first screen will be the welcome screen. Click **Next**.

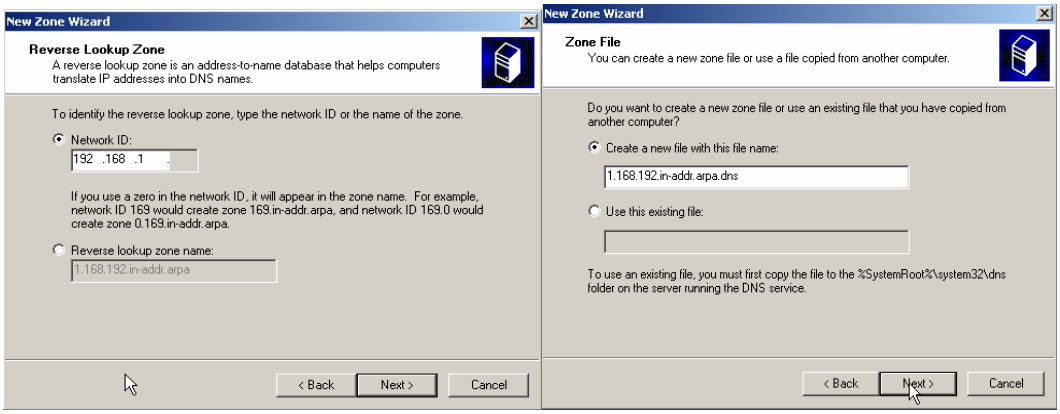
7. On the next screen select **Standard primary** for the zone type. Click **Next**.

8. On the next screen, enter the network ID for Portland **192.168.1**. Click Next.

******Note******

Notice that we are using 192.168.1 again. On a normal routed network, this Network ID would be different because the IP addresses of the hosts would be different.

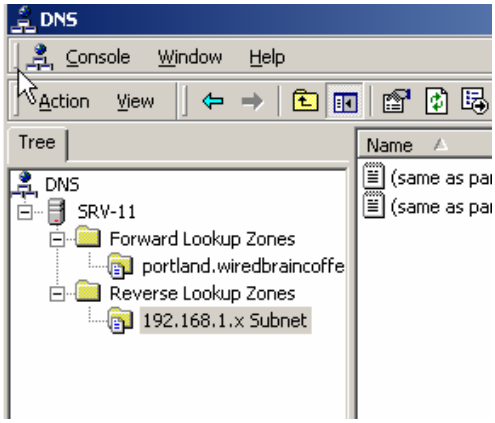
9. On the next screen leave the default name for the filename as **1.168.192.in-addr.arpa.dns**. Click **Next.**



(figure 78)

10. The next screen is a summary of all the information you entered. Make sure there are no mistakes and click **Finish**.

11. On the DNS console, you should now have a standard primary zone for **portland.wiredbraincoffee.com** under the forward lookup zones folder and a standard primary zone for **192.168.1.x** subnet under the reverse lookup zones folder.

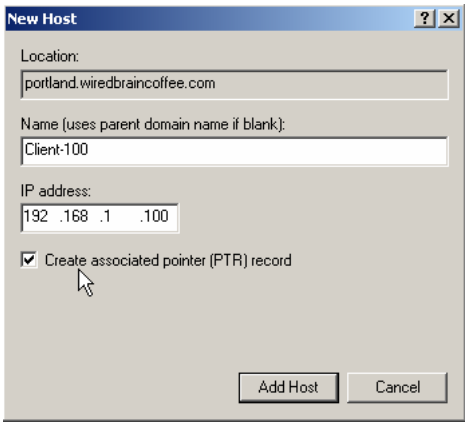


(figure 79)

Creating Hosts on the Delegated Zone

1. Right click on the **Portland.wiredbraincoffee.com zone** and select **New Host**.

2. Create a host file and pointer for **Client-100** with the IP address of **192.168.1.100**.



(figure 80)

Also, create the host and PTR records for the following:

1. Host name: Client-101 IP address: 192.168.1.101
2. Host name: Client-102 IP address: 192.168.1.102
3. Host name: Client-103 IP address: 192.168.1.103

Click **Done**.

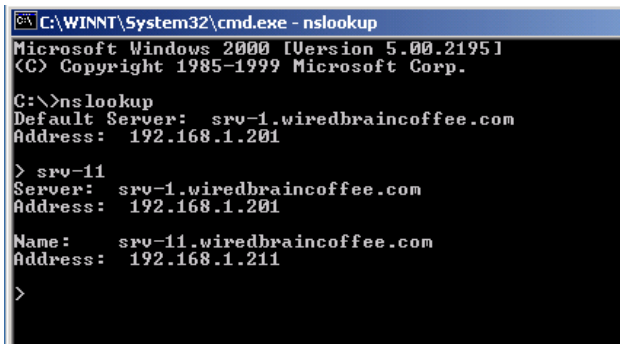
Testing DNS from a Client

******Note******

Make sure that srv-1 is set as your default (preferred) DNS server through the TCP/IP properties on client-1.

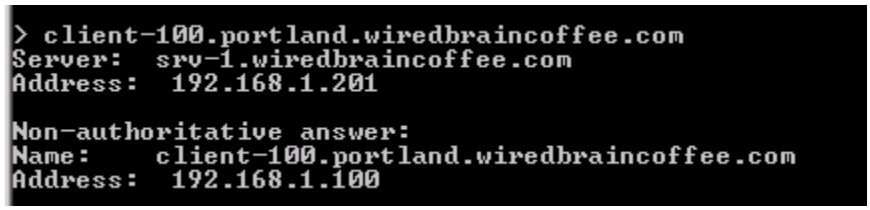
1. Log on to client-1 and open the command prompt. Type in **NSLOOKUP** and press **Enter**. Srv-1 should respond as your default server.

2. Type in **srv-11** to resolve the host name to an IP address. Press **Enter**. The top two lines will tell you the server that resolved the query and the next two lines will be the result of the query.



(figure 81)

3. Now type in **client-100.portland.wiredbraincoffee.com** and press **Enter**. The first two lines will tell you that srv-1 was the server that resolved the query but below this, you will see that it says "Non-authoritative answer", which means that srv-1 did not resolve the query from its own zone, the information was obtained from a different DNS server, srv-11 in this case. You see this result because srv-1 is client-1's preferred DNS server *but* srv-1 is not authoritative over portland.wiredbraincoffee.com, srv-11 is. Therefore, the request was passed on to srv-11 to resolve.

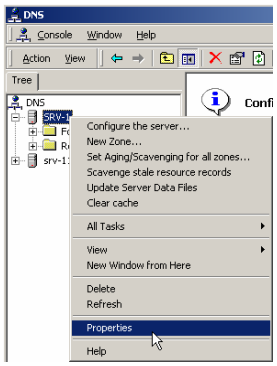


(figure 82)

Configuring a DNS Forwarder

Enabling forwarding on a DNS server allows you to specify an IP address to forward all non-local DNS queries to. If the local DNS server cannot resolve a query from a DNS client, it will forward the request to the IP address of the computer configured as a forwarder. Forwarders are commonly used on a local DNS server to give them the ability to securely resolve Internet names for their local DNS clients. Forwarding is often done to public DNS servers, like ISPs.

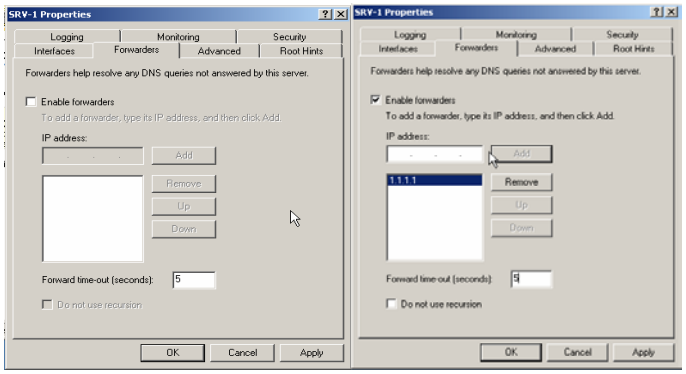
1. Log on to srv-11 and open the DNS console. Right click on srv-11 and select Properties.



(figure 83)

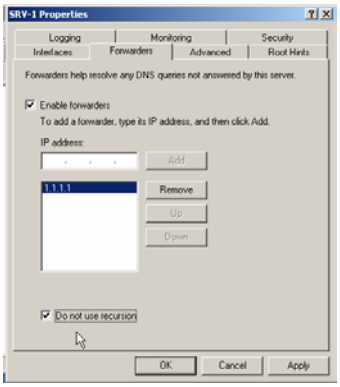
2. On the properties screen select the **Forwarders** tab. Notice that Forwarders are not enabled by default and you are not able to add any IP addresses.

3. Check the box that says **Enable forwarders**. This will allow you to now enter an IP address or IP addresses. For example, type in the IP address **1.1.1.1** (This is a valid IP address and should **not** be used on a network that is live on the Internet). Click **Add.** This is where you would enter the IP address of your ISP's DNS server or possibly your company's public DNS server.



(figure 84)

4. On the bottom of the screen is the **Do not use recursion** box and the **Forward time-out (seconds)** box. If this box is left unchecked (the default), the DNS server will try to resolve the host name itself, after giving the forwarder 5 seconds, or whatever time you configure for the Forward time-out. This is a security no-no, and in most cases, you should check the Do not use recursion box which causes the Forward time-out box to disappear and keeps the local DNS server from ever going out onto the Internet and attempting to resolve host names on its own.



(figure 85)

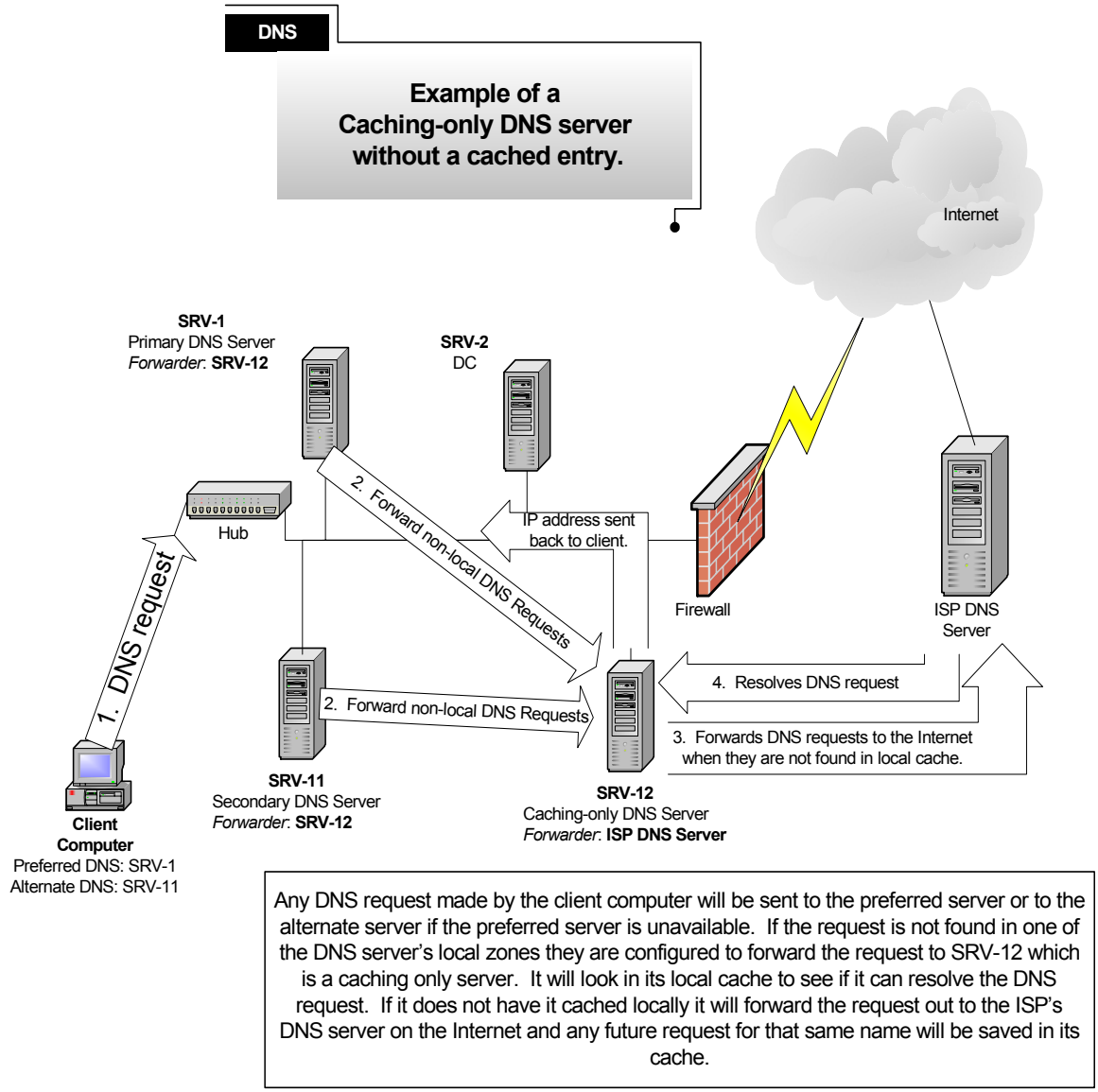
Installing and Configuring a Caching Only DNS Server

A caching only DNS server can be setup by installing DNS on a server, without configuring any DNS zones. Any DNS server is capable of caching, but by not installing zones, you are making this DNS server *only* capable of resolving name resolution queries from its cache. Caching only DNS servers are best used in conjunction with local DNS servers that contain zones. Lets take a step back, before we introduce the caching only DNS server into the mix, and describe how caching works on individual DNS servers.

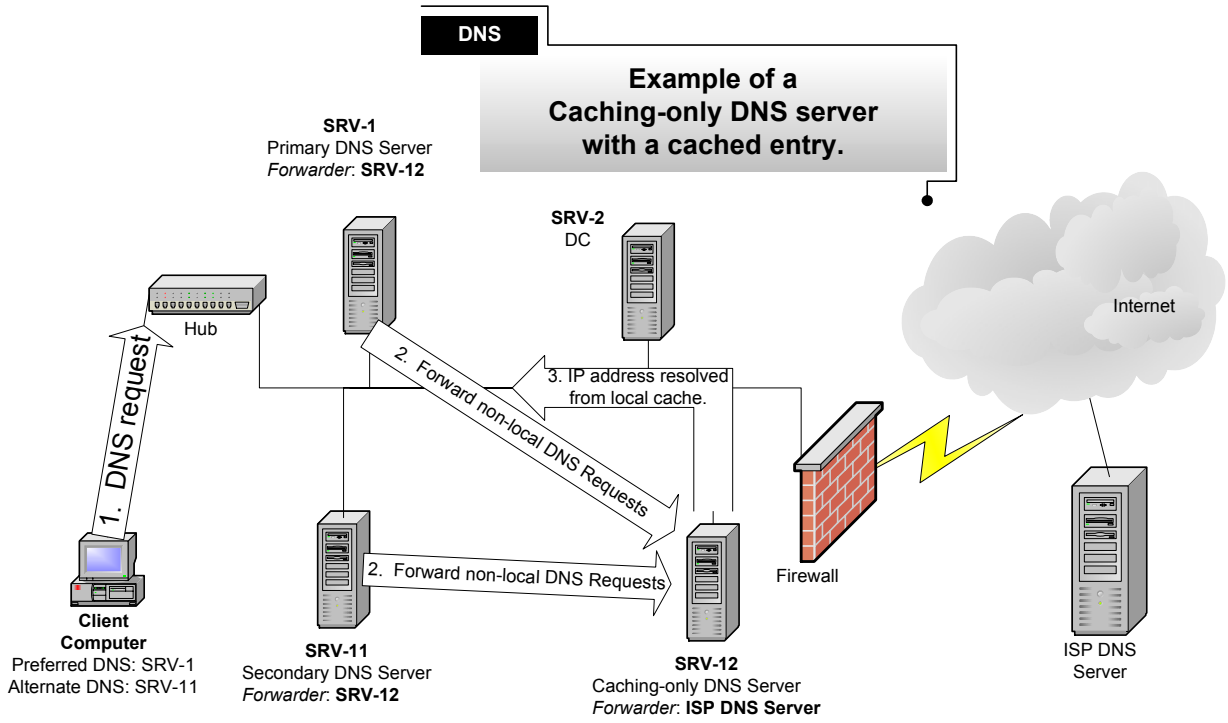
If you have five DNS servers on your network that forward any non-local DNS requests (i.e. web site requests) off to an Internet DNS server, each of these servers will maintain a separate cache. Therefore, although one DNS server might hold a cached entry for www.espn.com, the other four DNS servers do not hold this cached entry. DNS servers do not share their caches with each other. Therefore, if one of the four *other* DNS servers gets a request for www.espn.com, they will have to go back out to the Internet to resolve the host name to an IP address. The result is slower DNS resolutions and consumption of more precious WAN bandwidth. This is where the caching only DNS server comes in.

If you configure each of the five DNS servers to forward non-local requests to the caching only DNS server first and then have the caching only DNS server forward to an Internet DNS server (ISP or Root server), the caching only DNS server will hold a common cache for the five local DNS servers. Do not get me wrong, each DNS server will still maintain a local cache, but the caching only DNS server will maintain a common cache, because all of the DNS resolution requests to the Internet, from each of the five local DNS servers, will have passed through it.

Now, when the first DNS server requests www.espn.com, things will be no different than before, except that the request passed through the caching only DNS server and the caching only DNS server entered the information into its cache. When the second DNS server requests www.espn.com, the resolution will not be its local cache. However, when it forwards the request on to the caching only DNS server, the caching only DNS server will be able to resolve the host name to an IP address from its local cache, without going out to the Internet. In a large company, this can significantly reduce DNS resolution time and conserve WAN bandwidth. Look at the diagrams on the following pages to get a better understanding of this concept.



(figure 86)



(figure 87)

Lab 4

Configuring a public DNS Server

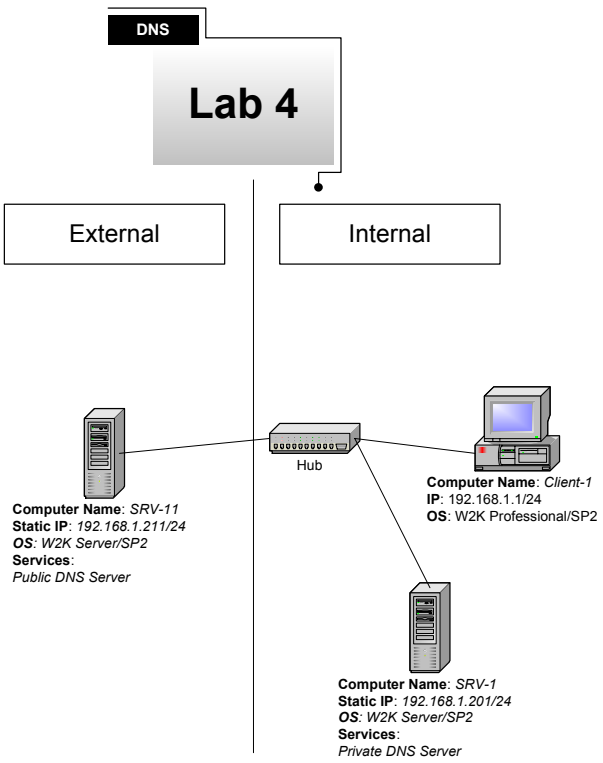
You will learn how to:

- Install and configure a DNS server for use on a public network
- Create host records for a Web, FTP & Mail Server
- Set up Round Robin DNS
- Differentiate between Public & Private DNS zones

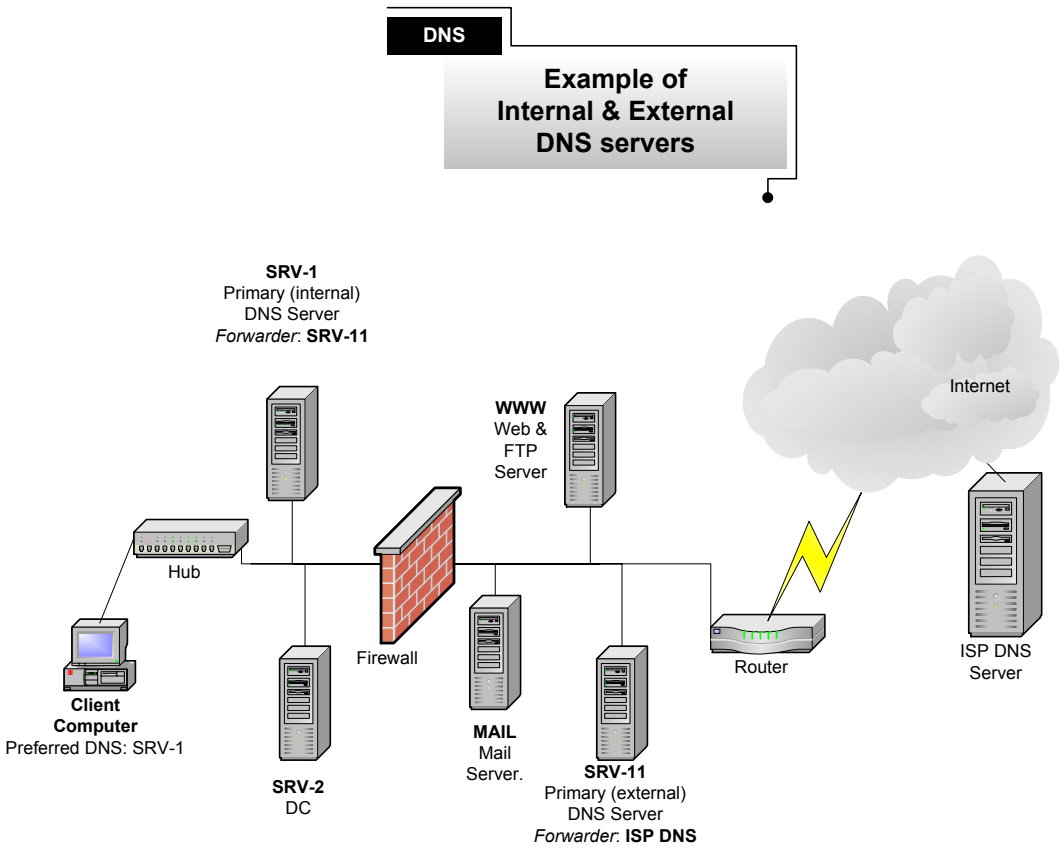
Scenario

Wired Brain Coffee's network has taught you a lot about DNS, but one piece you have not been exposed to yet, is how to configure DNS for a public network, such as where your web or email server might sit. Charlie has warned you that you have to look at DNS from a completely different perspective when you configure it for a public network. "The fundamentals are the same but because of security concerns, the DNS settings are substantially different," Charlie said. What exactly did he mean, I wondered? What settings and why is it different?

Remember, that a public DNS server is a DNS server that is exposed openly on the Internet. It has to be able to be reached from the Internet or your web site and mail server will not be able to be accessed. In this lab, you will learn how to set up, configure and secure a public DNS server. You will also set up "split" or "split-brain" DNS, where the same domain name is utilized on the internal and the external DNS structures but the DNS zone databases are different. Normally, the public DNS servers would be outside of the firewall, but we are not using a firewall on our test network, so our internal and external DNS servers will be plugged into the same hub/switch (See figure 88 below). You will also be using a private class network ID for the public network (192.168.1.0). In a production environment, you would need to obtain public IP addresses from your ISP.



(figure 88)



(figure 89)

Prerequisites

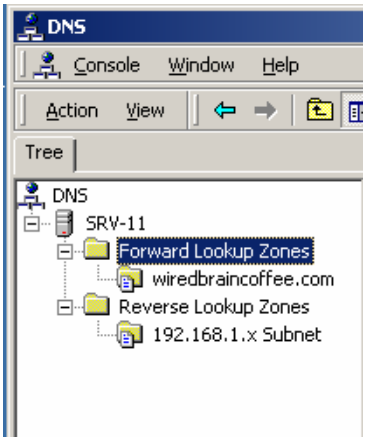
Before starting this lab, you need to go back and delete the DNS zones created on both srv-1 and srv-11. You will be creating a Split or Split-Brain DNS, which means that you will have two separate zones for wiredbraincoffee.com. One will be created for the internal network and the other will be created for the public network (Internet). This way, your internal network will not be exposed to the Internet while users on the Internet will still be able to access your web, ftp and mail servers, using the wiredbraincoffee.com domain name.

Creating and Configuring an External (Public) DNS Server

The public DNS servers on your network are directly exposed to the Internet, therefore, extra caution has to be used in order to prevent these servers from being compromised. The public DNS servers will not make any zone transfers with the internal DNS servers and should not accept any registrations or zone transfers from other public DNS servers.

******Important Note******
Normally the public DNS server and any of the machines on your public network will have public IP addresses that you would obtain from an ISP. Throughout this lab, the private class network ID ***192.168.1.0*** *has been used. This configuration would NOT work on a public network.*

1. Log on to srv-11 and open the DNS console. You should have **no** zones currently, because these should have been deleted in the prerequisite steps to this lab. Now, Create a **Standard primary** forward lookup zone for **wiredbraincoffee.com** and a **Standard primary** reverse lookup for **192.168.1.x.** Srv-11 will be the DNS server for the external network.



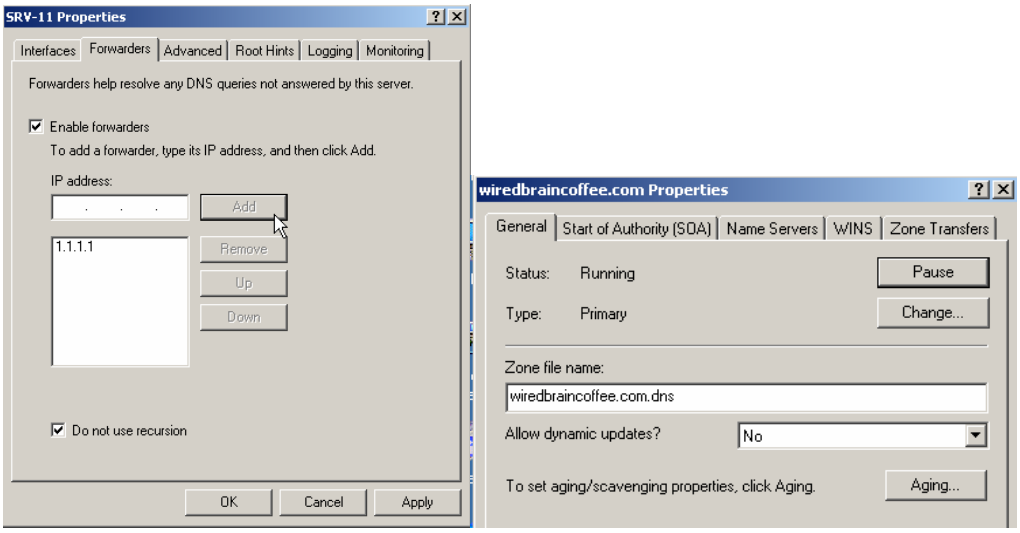
(figure 90)

2. Create **Host (A)** & **Pointer** (**PTR) records** on Srv-11 for:

Computer Name	IP Address	Record Type
srv-11	192.168.1.211	*Host & PTR*
www	192.168.1.250	*Host & PTR*
mail	192.168.1.251	*Host & PTR*

3. From the DNS console right click on **srv-11** and select **Properties**. On the properties screen select the **Forwarders** tab. Enable forwarding by selecting the box next to **Enable forwarders,** then disable recursion by selecting the box next to **Do not use recursion**. Finally, add the IP address of your ISP's DNS server. We will use 1.1.1.1, but you would enter the IP address of your ISP's DNS server if you were on a live network.

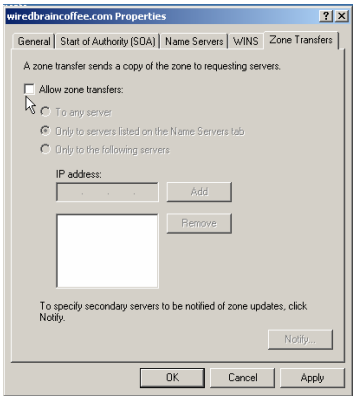
   Forwarding is not required for DNS to work on the public network. The public would still be able to reach your web and ftp servers without forwarding enabled. You would enable forwarding if your *internal* DNS servers were forwarding to your *public* DNS servers. This would allow internal DNS requests to pass from the client to the internal DNS server to the public DNS server and then on to the ISP's DNS server, if necessary.



(figure 91)

4. Right click on the **wiredbraincoffee.com** zone and select **Properties**. On the **General** tab make sure that the setting **Allow dynamic updates** is set to **No**. This will prevent computers on the Internet from dynamically registering with this DNS server and will force you to enter the host records for the public zone manually.

5. Click on the **Zone Transfers** tab and remove the checkmark next to **Allow zone transfers**. Everything will become grayed out meaning that there will be no zone transfers to or from this zone. Click **OK**. If you had additional DNS servers on your public network, you would want to allow zone transfers *only* to these other DNS servers on your public network.

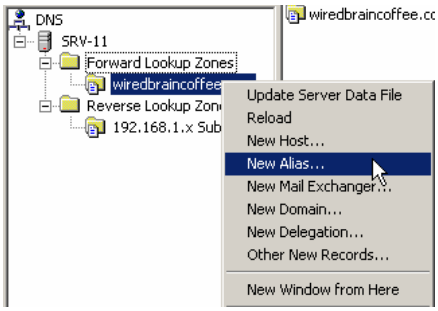


(figure 92)

Creating an Alias Record

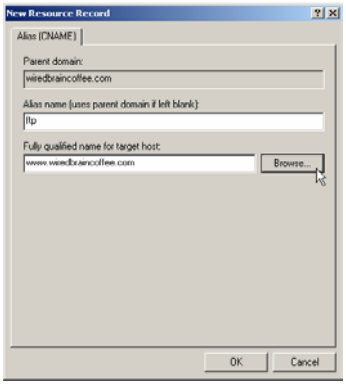
If you are hosting the web server and the ftp server on the same computer you want to set up your naming, so requests to www.wiredbraincoffee.com or ftp.wiredbraincoffee.com will find their way to the same server. One way of accomplishing this is to create an alias record with the name **ftp**, which points to the already created **www** host record. Alias records are also known as **CNAME** (Canonical Name) records.

1. Right click on **wiredbraincoffee.com** zone and select **New Alias**.



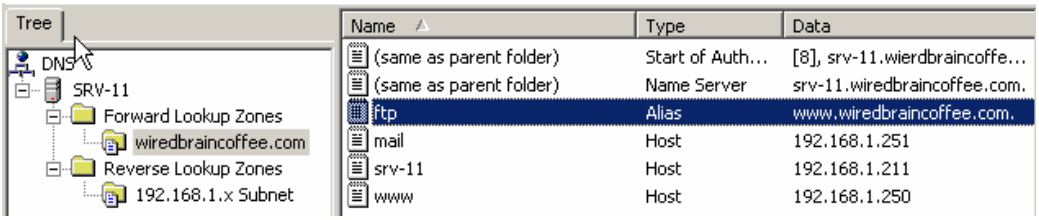
(figure 93)

2. In the dialog box, type in **ftp** as the **Alias name** and then browse to the host file for **www.wiredbraincoffee.com**. This is found by clicking on browse and then looking in SRV-11→forward lookup zones→wiredbraincoffee.com and here you will find the host record for www. Select **www** and click **OK**.



(figure 94)

3. Now look in the **wiredbraincoffee.com zone folder** and you should see an alias record for ftp that points to the host record www.wiredbraincoffee.com. Any requests that come in for ftp will be directed to the host record www. The IP address associated with the www record will be supplied to the DNS client.

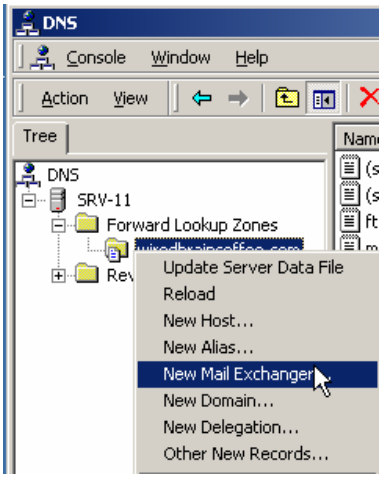


(figure 95)

Creating a MX Record

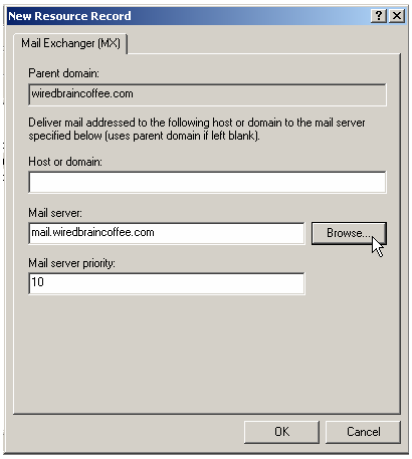
The MX record is created on a DNS server to identify the location of the mail server. Any request that has an email suffix attached to it, such as sales@trainsignal.com, will be redirected to the host record specified in the MX record.

1. Right click on **wiredbraincoffee.com** zone and select **New Mail Exchanger**.



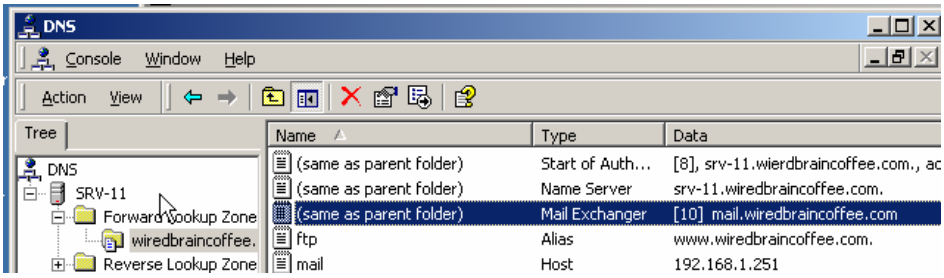
(figure 96)

2. Leave the **Host or Domain** area blank so that it will use the parent domain wiredbraincoffee.com. For the **Mail server** entry, browse for the host record that you created for the mail server named **mail.wiredbraincoffee.com.** The mail server priority is used if you have multiple mail servers and you want to give one a higher priority than the others. Leave the default setting of 10 and click **OK**.



(figure 97)

3. When you look in the **wiredbraincoffee.com zone,** you should see an MX record for wiredbraincoffee.com that points to the host record mail.wiredbraincoffee.com.

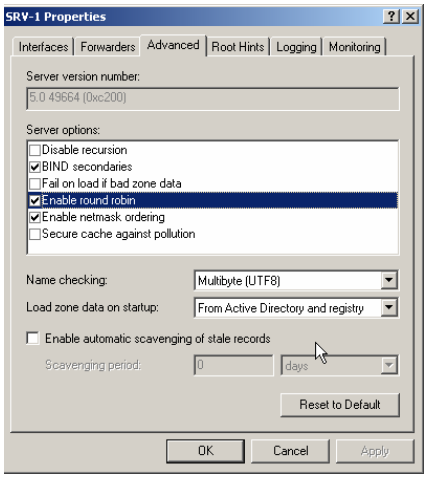


(figure 98)

Round Robin DNS for Load Balancing

Round Robin DNS allows a DNS server to alternate referrals to different computers for load balancing purposes. It is not meant to be an enterprise level solution, but rather a cheap alternative for balancing the load across multiple servers. For example, if your web site is very busy and one server is not able to handle the load you can put your web site on several different computers, each with a different IP address. Within DNS, you will need to create several "www" host records, each pointing to one of the computer's IP addresses. When round robin is enabled, the DNS server will refer requests out evenly, to each of the "www" host records. Round robin DNS is not fault tolerant. If one of the web servers goes down, the DNS server will still give out that computer's IP address whenever it is that web server's turn.

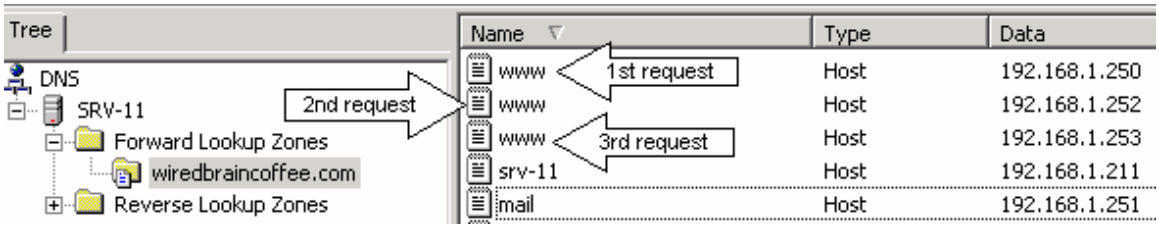
1. Right click on **srv-11** and select **Properties**. Go to the **Advanced** tab. Make sure that round robin is enabled by checking the box next to it if it is not already enabled. Click **OK.**



(figure 99)

2. Go to the **wiredbraincoffee.com** zone and create two additional entries for the **www** host record. You have already created an entry for www → **192.168.1.250**. Use the IP addresses **192.168.1.252** and **192.168.1.253**. In a production environment, you would have a server hosting your web site at each of these IP addresses.

3. When you look at the **wiredbraincoffee.com** zone, you should see three entries for www. Requests for www.wiredbraincoffee.com will now be alternated between the three different IP addresses. Be aware, that Round Robin DNS does not provide fault tolerance. Even if one of these web servers goes down, the DNS server will continue to forward web requests to it every third time, returning "page not found" errors to the web browser trying to visit your site.

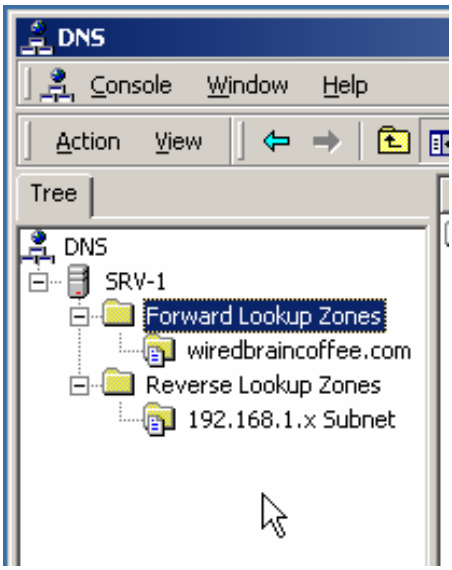


(figure 100)

Configuring DNS for the internal network

Now that you have created and configured the external DNS server, you will need to create and configure the internal DNS server for your network. The internal DNS servers will only resolve DNS queries within the network, for any zone created internally, which is just wiredbraincoffee.com in our case. Any queries that can not be resolved by the internal DNS server will be forwarded to WBC's external (public) DNS server. If the external server can not resolve the query, either from its zone or its cache, it will forward the query on to the ISP's DNS servers (configured previously).

1. Log on to srv-1 and open the DNS console. Create a **Standard primary** forward lookup zone for **wiredbraincoffee.com** and a **Standard primary** reverse lookup zone for **192.168.1.x.** This will be the DNS server for your internal network.



(figure 101)

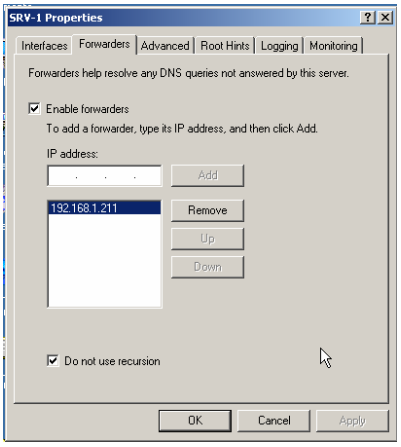
2. Create **Host (A)** & **Pointer (PTR) records** on Srv-1 for:

Computer Name	IP Address	Record Type
srv-1	192.168.1.201	*Host & PTR*
srv-2	192.168.1.202	*Host & PTR*
srv-12	192.168.1.212	*Host & PTR*

Configuring a forwarder to the external DNS server

1. From the DNS console, right click on **srv-1** and select **Properties**. On the properties screen select the **Forwarders** tab. Enable it by selecting the box next to **Enable forwarders** then disable recursion by selecting the box next to **Do not use recursion**. Finally add the IP address of your external DNS server: **192.168.1.211**. Click **OK**.

   Disabling recursion prevents the DNS server from taking matters into its own hands and attempting to resolve the DNS query itself, which is not secure. Normally, the DNS server will give the forwarder 5 seconds before it will go off on its own. By disabling recursion, this DNS sever will depend upon the forwarder and will not attempt to resolve any DNS name that is outside of the local DNS structure.



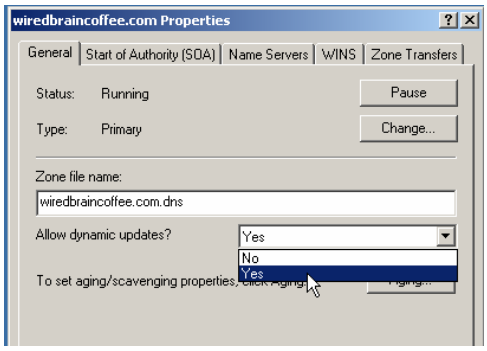
(figure 102)

Configuring the Internal DNS Zone to Allow Dynamic Updates

Dynamic updates can be enabled on the internal zone (they were not allowed on the external zone) to allow internal clients to automatically register with the DNS server, saving you the time of manual entry. They need to be enabled separately on both the forward and the reverse lookup zones.

1. Right click on the **wiredbraincoffee.com zone** and select **Properties**.

2. On the General tab, change the **Allow dynamic updates** setting to **Yes**. Click **OK**.

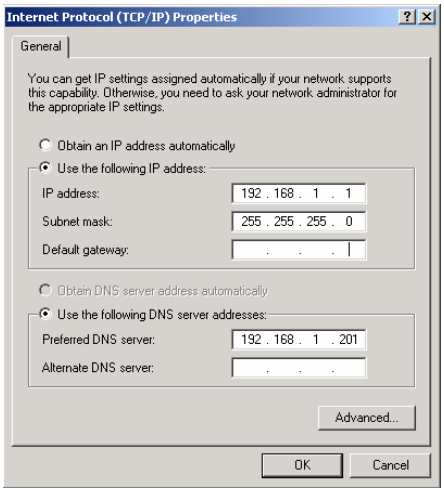


(figure 103)

3. Repeat this process for the reverse lookup zone, enabling dynamic updates.

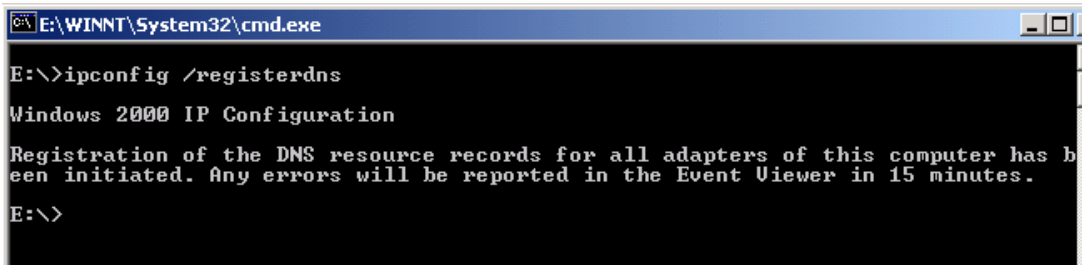
Testing Dynamic Updates from the Client

1. Log on to **client-1** and check that the Internet Protocol (TCP/IP) settings are correct. The IP address should be **192.168.1.1**, the subnet mask should be **255.255.255.0**, the default gateway should be blank and the Preferred DNS server should be set at **192.168.1.201**.



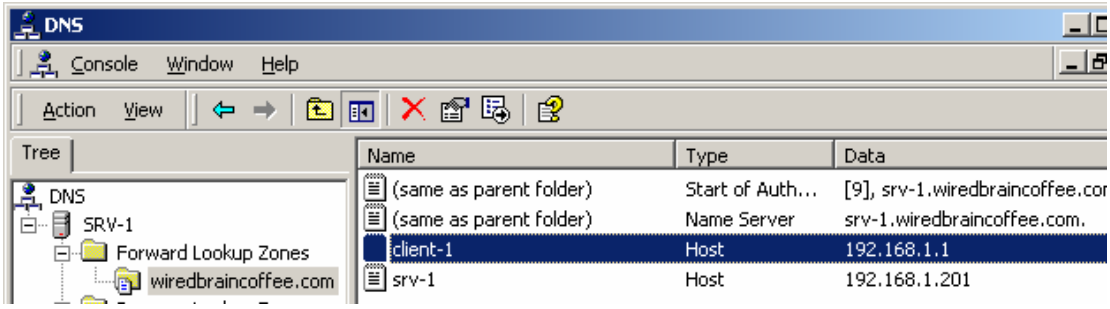
(figure 104)

2. From client-1, enter the command **ipconfig /registerdns.** This will force client-1 to reregister with its preferred DNS server. Try deleting the **client-1 host record** and rerunning this command several times, to verify that it works. The zone **must** be configured to accept dynamic updates or this command will not work.



(figure 105)

3. Log on to **srv-1** and open the DNS console. Look under the **wiredbraincoffee.com zone** and you will see that there is an entry for **client-1**.



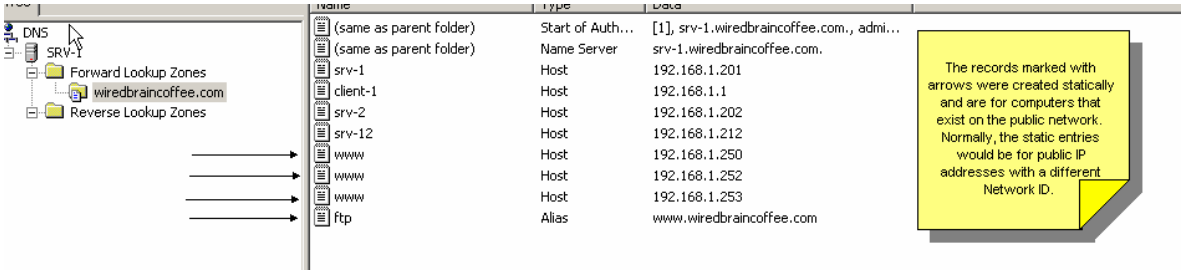
(figure 106)

4. Check the reverse lookup zone as well. Remember that dynamic updates must be enabled the same way on the reverse lookup zone for the client to update its PTR record automatically.

Creating Static Host Records on the Internal Zone

Wired Brain Coffee now has two separate zones, both named **wiredbraincoffee.com**. If an internal client wants to access a website like www.microsoft.com, the internal DNS server will realize that it is not authoritative for microsoft.com and will send the request to the forwarder. What happens though, if an employee wants to view his or her own company web site located at www.wiredbraincoffee.com on the public network? The client sends a DNS request to the internal DNS server, which is authoritative for wiredbraincoffee.com. The internal zone, however, does not contain an entry for the "www" computer. This entry is contained in the external wiredbraincoffee.com zone. Since the internal DNS server *is* authoritative for the zone and it does not contain an entry, it just responds with a host not found error. To correct this problem you need to create static host records for any host names on your public network that internal computers may need to access.

1. On srv-1, create a host record within the internal wiredbraincoffee.com zone for each of the www entries and create an alias record for ftp. When you are finished, your forward lookup zone should look similar to figure below.



(figure 107)

2. From **client-1**, attempt to run nslookup and verify the results for **www & ftp.**

(figure 108)