AVAYA

SCS 4.0

Configuring DNS and DHCP for Windows Server 2003

Task Based Guide

Copyright © 2010 Avaya Inc.
All Rights Reserved.

Notices
While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer
Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer
Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation(s) provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty
Avaya provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Web site: http://www.avaya.com/support
Please note that if you acquired the product from an authorized reseller, the warranty is provided to you by said reseller and not by Avaya.

Licenses
THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER.
UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER, AND AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS
AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Copyright
Except where expressly stated otherwise, no use should be made of the Documentation(s) and Product(s) provided by Avaya. All content in this documentation(s) and the product(s) provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third Party Components
Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/Copyright.

Trademarks
The trademarks, logos and service marks ("Marks") displayed in this site, the documentation(s) and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the documentation(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party. Avaya is a registered trademark of Avaya Inc. All non-Avaya trademarks are the property of their respective owners.

Downloading documents
For the most current versions of documentation, see the Avaya Support. Web site: http://www.avaya.com/support

Contact Avaya Support
Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site:http://www.avaya.com/support

Copyright © 2010 ITEL, All Rights Reserved

The copyright in the material belongs to ITEL and no part of the material may be reproduced in any form without the prior written permission of a duly authorised representative of ITEL.

Table of Contents

Introduction 5

DHCP (Dynamic Host Configuration Protocol) 7

DNS (Domain Name Service) 8

Impact on Installation 9

Configuring Windows Server 2003 DHCP 11

Reserving IP Addresses on Windows Server 2003 11
Setting Option 66 on Windows Server 2003 15
Setting Option 6 (When Utilizing SCS Onboard DNS) 19
Other DHCP Options 22

Configuring Windows Server 2003 DNS 23

Single Server System – A Records 23
Testing DNS 26
Single Server System – A Records & SRV Records 27
Creating an A Record 28
Creating SRV Records 31
Testing DNS 34
Dual Server (HA) System – A Records & SRV Records 35
Creating a sub-domain and A Record for each server 36
Creating SRV Records 42
Creating Redirect SRV Records 47
Testing DNS 56
Concluding Setup 57
Updating DNS Data Files 57
Rebooting the SCS Server 58
Data Replication Error 59

Avaya Documentation Links 61

Introduction

DHCP and DNS play an important part in the operation of any SCS installation. There are many configuration variables to consider when installing a new SCS system: what type of DNS is in use on the network? Is Dynamic IP addressing in use? What host name and IP address have been reserved for the SCS? The aims of this document are:

- To highlight network configuration issues you should consider before starting the installation.

- Show you how to configure DNS and DHCP for use with the SCS.

The Pre-Installation checklist can be found in the opening pages of the *SCS Release 4.0 Initial Install* guide and *SCS Release 4.0 Configuring the SCS with High Availability* and is a recurring topic in any discussion concerning the installation of the SCS simply because it aids preparation by both providing the installer with the information they need to successfully perform their task, and informs the site network administrator of the work that will be undertaken on his network – allowing him to take all necessary steps. The questionnaire is reproduced on the next page.

Note: There are a multitude of different DNS systems around the world. This guide uses as its example Windows Server 2003. The instructions and screenshots concerning how to configure DNS and DHCP settings are therefore relevant to this system only. However, the values prescribed for DNS A Records and SRV Records can be applied to any DNS system.

Parameter	Value
Root User Password	
Time Zone	
Host Name (please supply a fully qualified domain name, for example **scshost.domainname.com**)	
IP Address (as set in the DNS)	
Default Gateway	
Subnet Mask	
Does the network have a DNS server?	Yes/No
Is your DNS server capable of generating SRV records? (SRV records are not a necessary requirement when configuring a non-HA SCS system, but if they are present in the DNS they have an impact on how you configure the SIP domain later in the configuration process, i.e., they determine whether you define the SIP domain with a fully qualified domain name or just a domain name)	Yes/No/NA
Primary DNS (the IP address of your host)	
Secondary DNS (the IP address of your host)	
Does the network have a DHCP server?	Yes/No
On the DHCP server, can Option 66 be configured to point at the SCS IP address for TFTP provisioning?	Yes/No/NA
Is network time configured through NTP?	

DHCP (Dynamic Host Configuration Protocol)

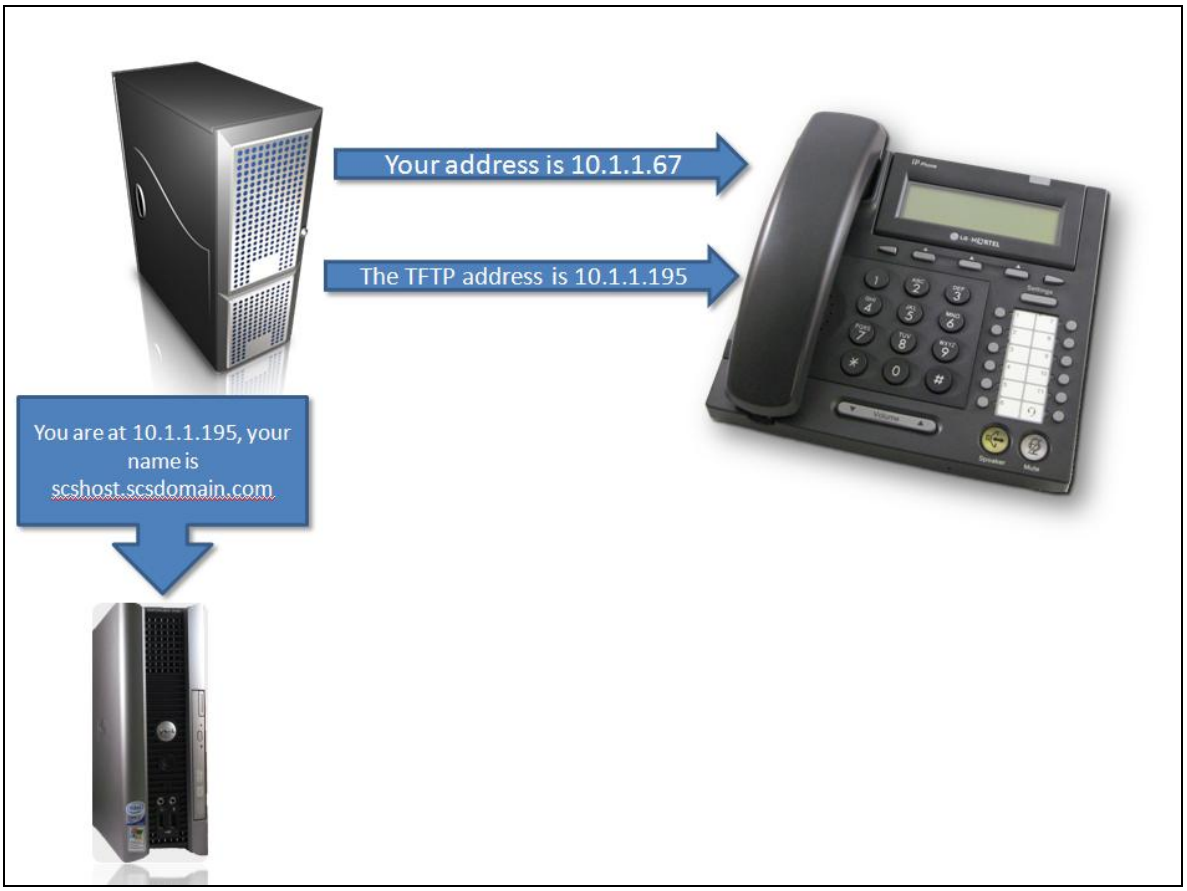
In the context of the SCS, DHCP is used to:

- Allocate IP addresses to IP phones and gateways when they are connected to the LAN.

- Optionally provide newly connected phones with the location of the TFTP or FTP (depending on phone type) service used to issue managed phones with configuration data necessary to operate in the SCS network.

Certain configuration changes will have to be made to a network's DHCP service (if indeed it is in use; not all sites will necessarily utilize DHCP, in which case IP addresses for devices such as phones will be configured statically) before the SCS installation can take place. These changes will be covered in step-by-step detail later in this document, but for now, they are:

- Reserve an IP address for the SCS.
- Define the host name that will reside at that address.
- Configure Option 66 – this is a completely optional setting that simply helps in the phone configuration process; the system will function perfectly well without it.



The relationship between DHCP and the SCS

DNS (Domain Name Service)

DNS is used to help the flow of data to the correct networking equipment by translating domain names to IP addresses. Not all sites utilize DNS, but a large majority do. In this document we will look at how best to configure DNS to suit a range of SCS scenarios.

You will probably be aware that a range of different DNS servers are used across the world, for the purpose of this guide we have focussed on Microsoft Server 2003. Some of the principles discussed over the coming pages will bear some similarity to most systems, but the way in which some information is configured will differ.

On sites that utilize DNS, 'records' that relate to the SCS will have to be configured in order that the DNS can resolve queries relating to the SCS. These records can take the form of:

- **A Records** – used to translate a host name to the IP address of the specific machine.

- **SRV records** – used to identify exactly which machine or machines offer a particular service, e.g. SIP.

Depending on the configuration and make-up of the network, and the type of installation you are going to perform (single server or dual server HA), different types of record will be needed. Put simply: a single server (non-High Availability) system will function perfectly well with DNS A Records on their own **or** A Records and DNS 'SRV Records; whereas a dual server (High Availability) system will **only** function with a combination of A Records and SRV Records. So Question 1 is this: **Are you installing a single or dual server system?**

Of course, there are other factors to consider. For instance, a third party DNS server is not the only possibility. It is entirely possible that you may encounter a site that does not make use of DNS, in which case you will have to enable the SCS's own DNS service. Question 2: **What type of DNS, if any, is in use on the site?**

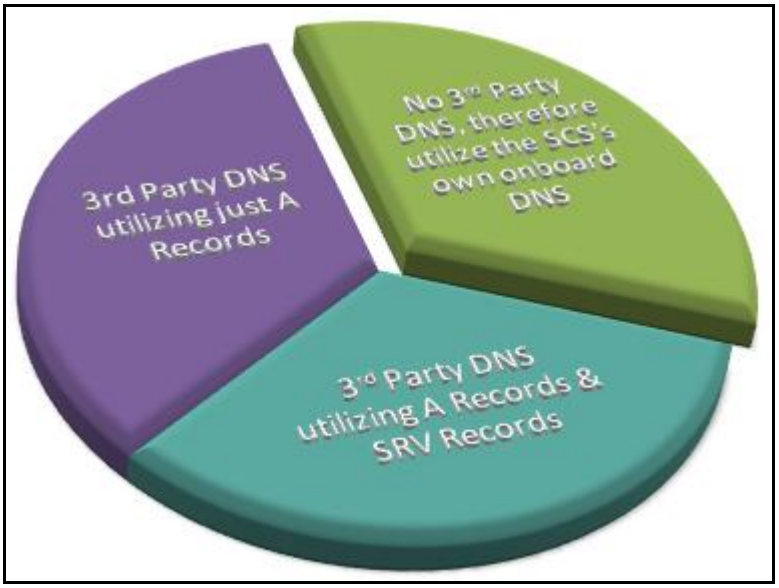
When using the onboard SCS DNS with a third party DHCP server, ensure that you change the DNS address referenced in Option 6 on the DHCP server. This is covered later in this guide.

The SCS's own DNS facility is simple to use: it has two configurable settings: On and Off. You will not need to configure any records since the SCS takes care of that for you by creating its own SRV records.

WARNING: You should not mistake this feature for a quick route to avoiding creating records on a third party DNS. It is recommended that in circumstances where a site operates a third-party DNS, the SCS's own DNS should be disabled since all requests will be handled by the primary DNS (i.e., the Microsoft server,

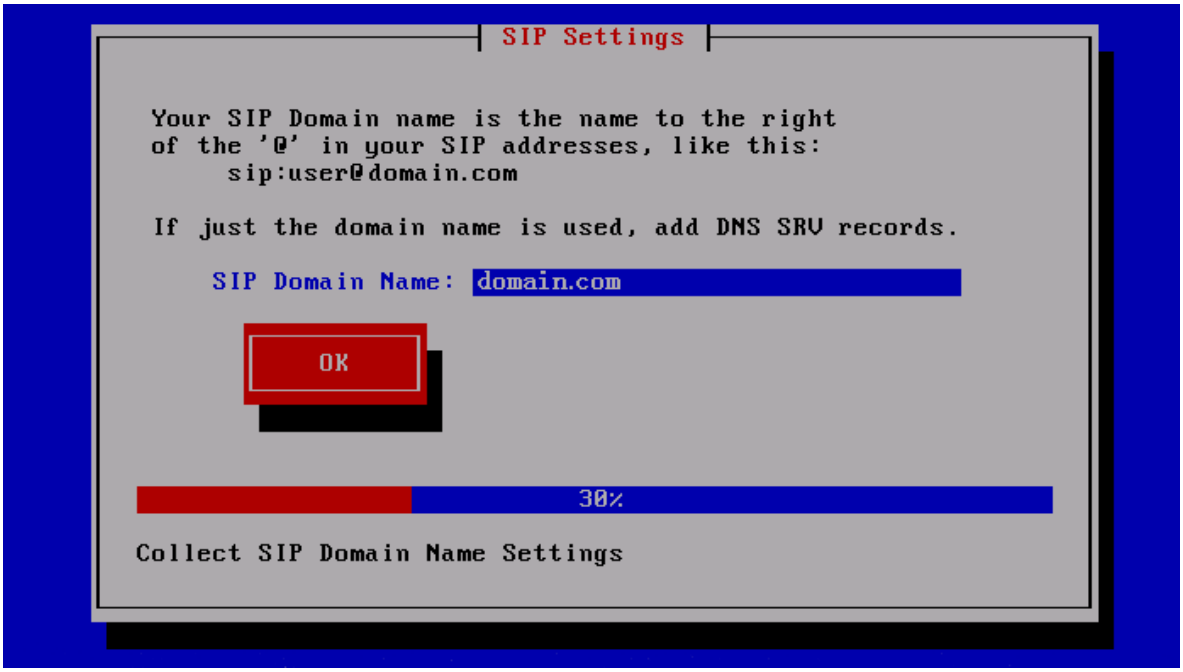
Linux server, etc). In such circumstances, enabling the SCS DNS does not remove the need to create records on the third-party DNS.

You will likely meet one of three DNS scenarios when rolling out the SCS:



Impact on Installation

The DNS configuration in use on the destination network has a direct impact on a key area of the installation process – namely what you enter in the SIP Domain field.



Basically, the rule of thumb is this:

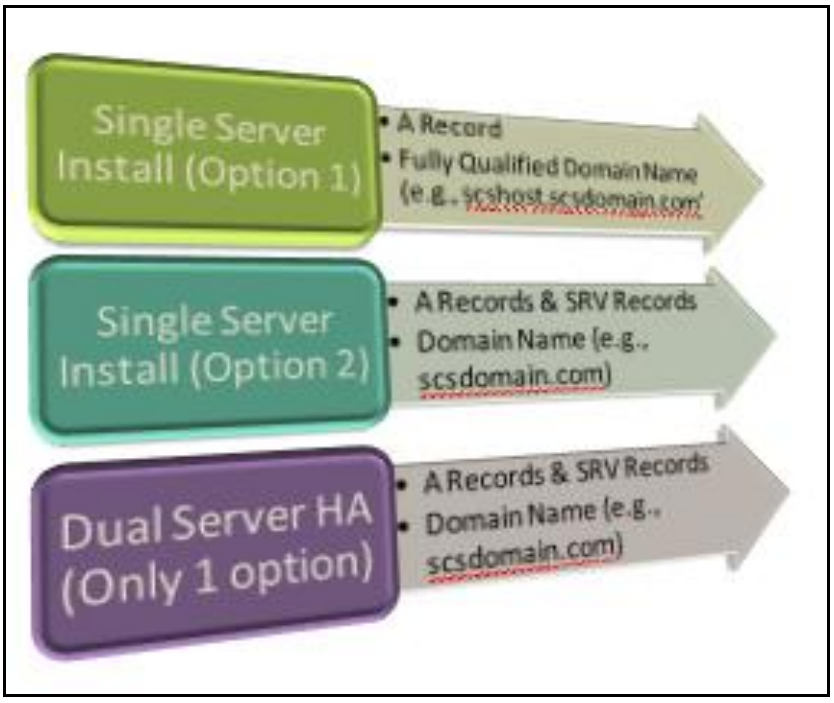
- If SRV records **are not** in use, you must enter the fully qualified domain name (FQDN) of the SCS server – that is, the host name *and* domain name configured on the DNS, e.g., *scsserver.domain.com*.

- If SRV records **are** in use, enter just the domain name – e.g., *domain.com*.

So what does this mean for single server installs and dual server installs? Just this:

- Single server installations function perfectly properly with either A Records or A Records with SRV records, just be aware of what records are in use so that you enter the correct value in the SIP Domain screen.

- Dual server installs **must always** have A Records *and* SRV records configured in the DNS, therefore you will always just enter the domain name in the SIP Domain screen for any server being configured as part of a High Availability system.

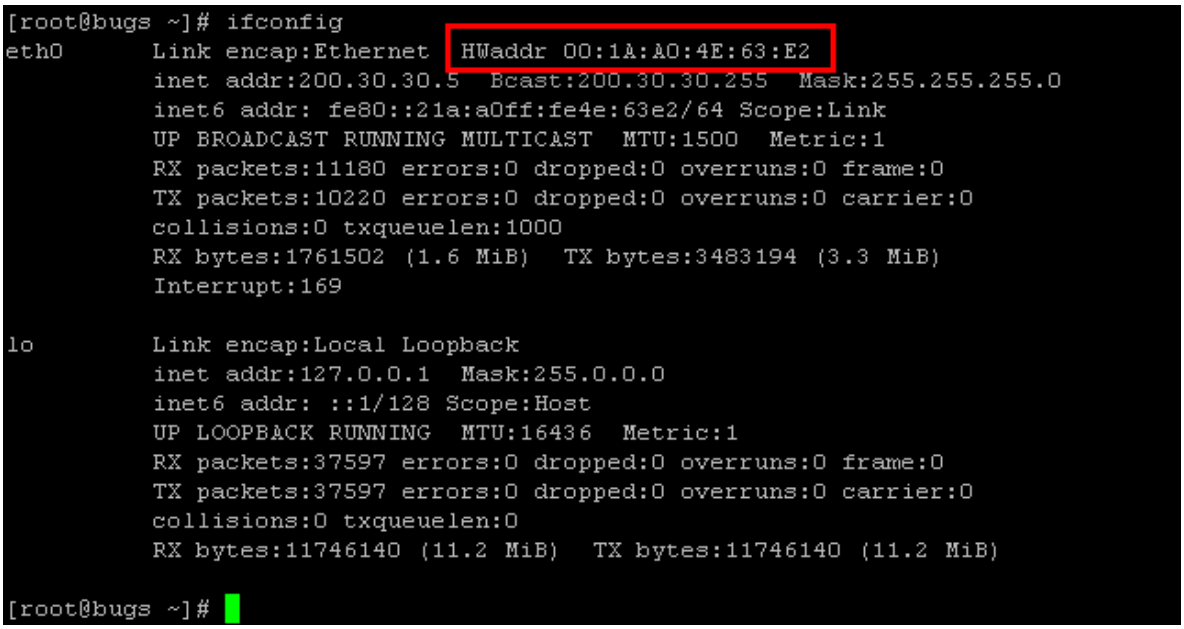


Configuring Windows Server 2003 DHCP

Reserving IP Addresses on Windows Server 2003

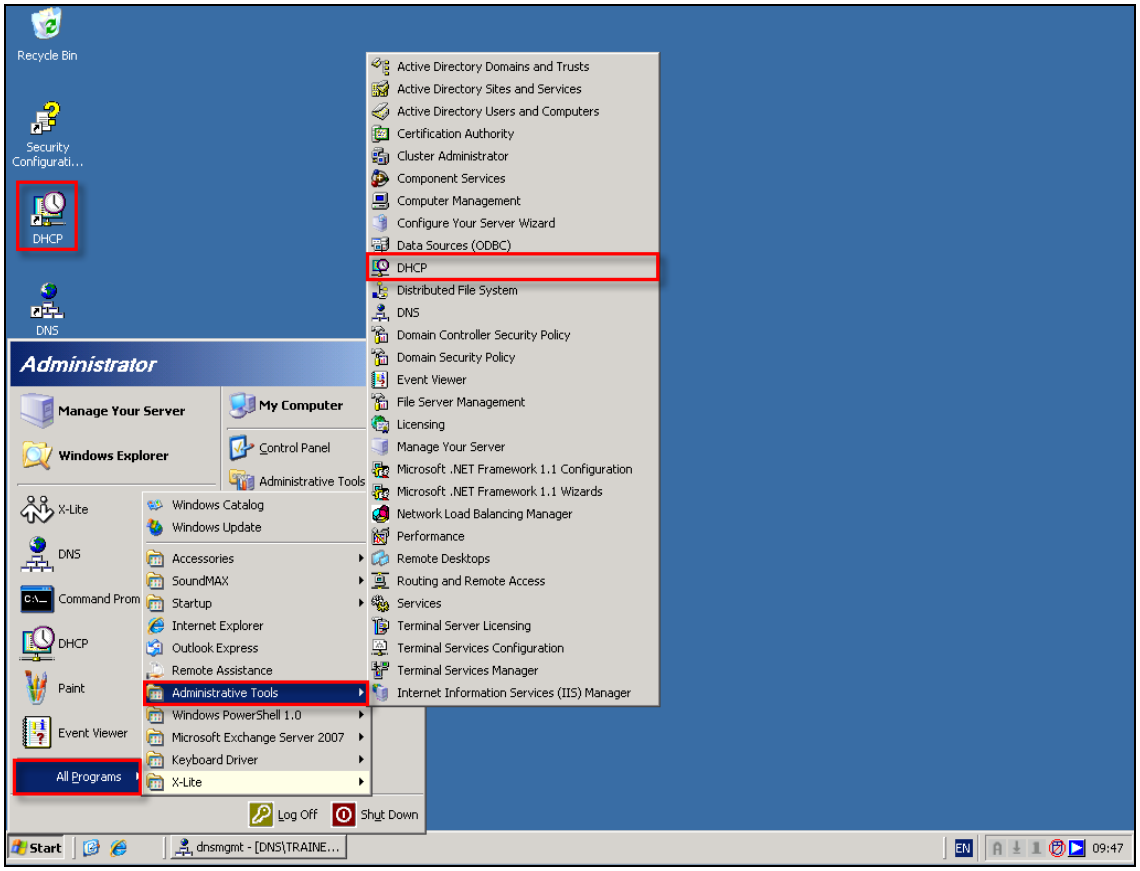
On sites that utilize a DHCP server it may be necessary to reserve the IP address that the SCS will use; this will prevent that address from being used by other devices that join the network. To reserve the address you will need to know 3 things:

- What address the SCS server (or servers in the case of an HA configuration) will use.
- The host name that the server will be assigned – this will also be used to configure DNS records.
- The server's MAC address. A MAC address is a 12 character alpha-numeric code that on some devices can be found on a label at the rear or on the underside. If there is no obvious MAC address label on the server you can run the `ifconfig` command once the setup wizard has been run and you have access to the command prompt.

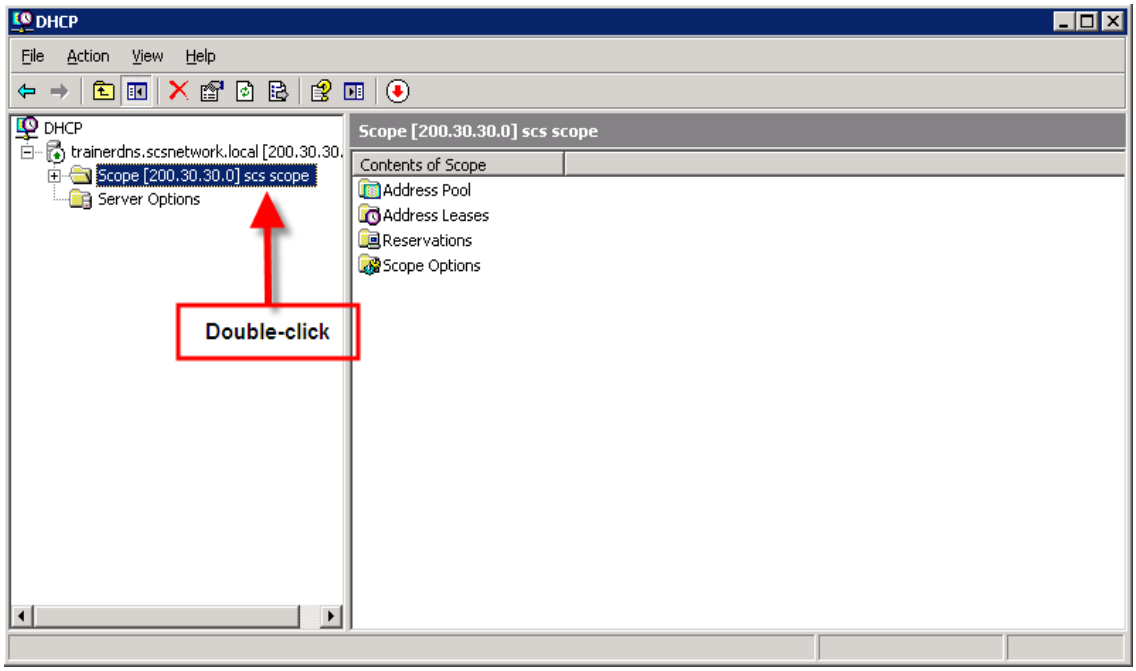


Note: Static LAN settings **can** be configured on the SCS before **DHCP and DNS have been properly configured** so that you can access the command prompt to run `ifconfig` to obtain the MAC address. Once Windows Server configuration is complete you must reboot the SCS servers so that they connect properly.

1. On the Windows Server, open the DHCP server application, either by double-clicking on the desktop icon, or by navigating through the **Start** menu.

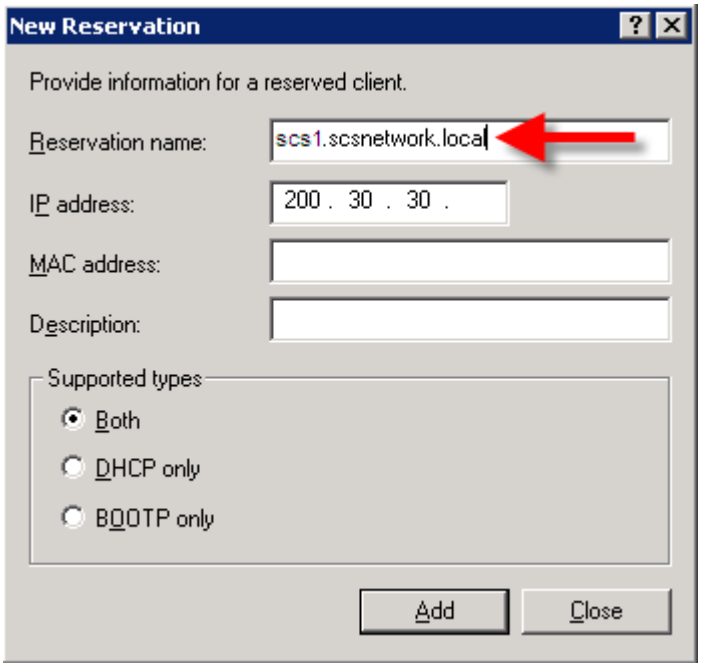


2. In the left-hand pane, double-click on the ‘Scope’ in which the SCS will be situated – a scope is merely a range of IP addresses to which devices can be assigned.

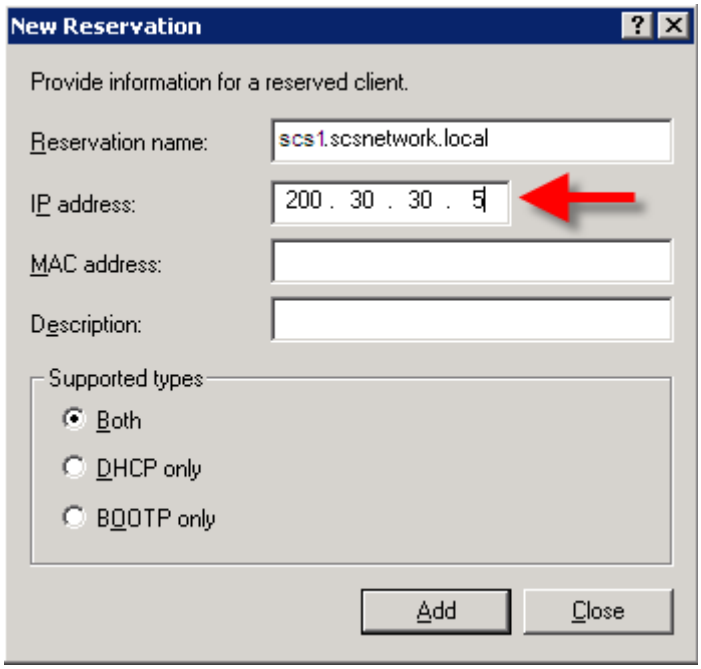


3. Right-click on **Reservations** and select **New Reservation**.

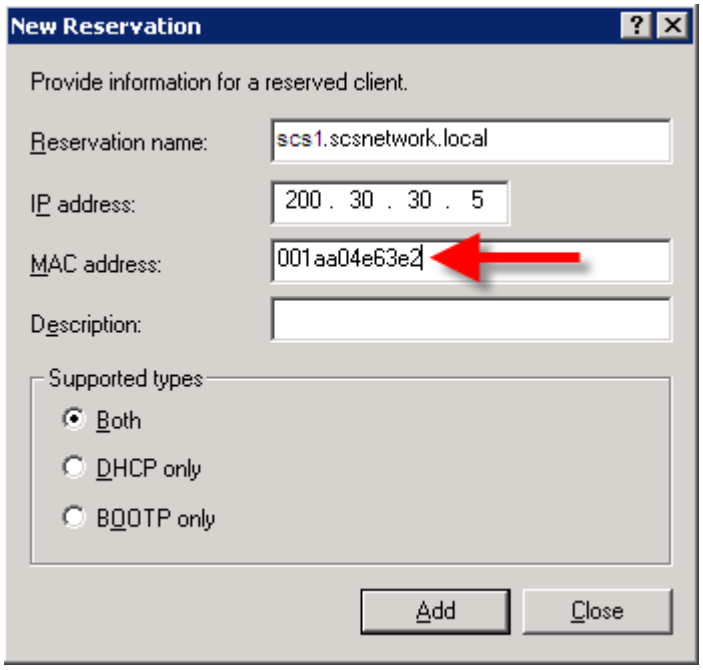
4. In the New Reservation window, enter the server's fully qualified domain name – the host name and domain name, for example, in this illustration the device name is *scs1.scsnetwork.local*.



5. Enter the IP address that you would like reserved for this server.



6. Enter the server's MAC address (without the colon separators).

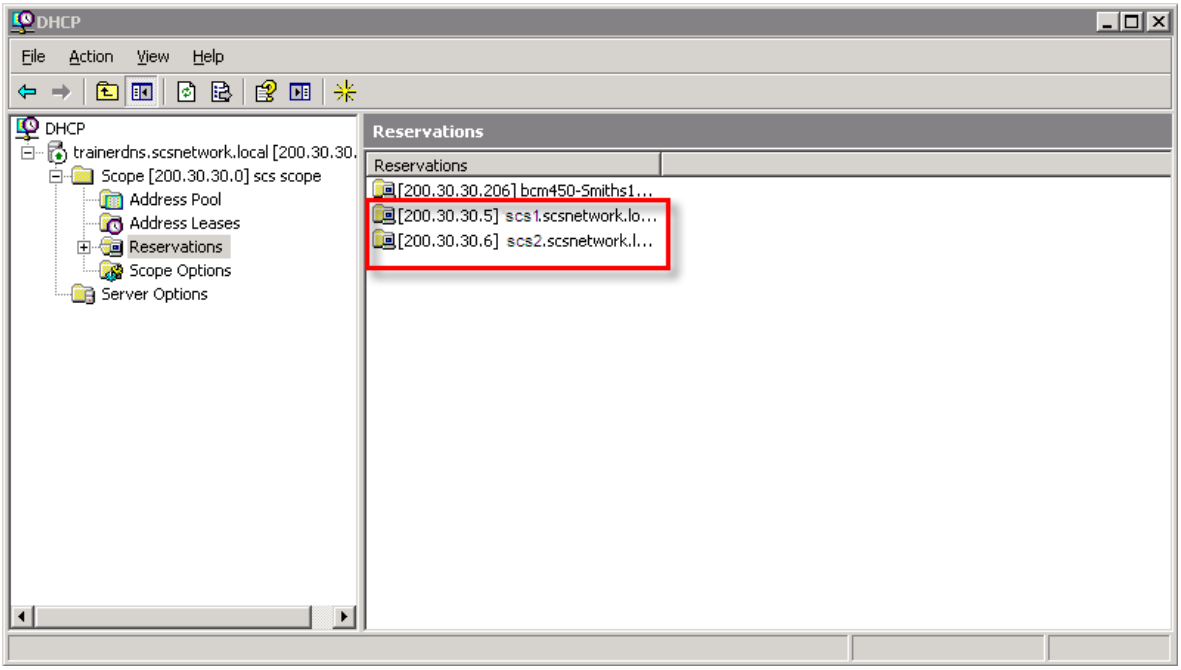


7. Click **Add**.

8. Repeat steps 4-7 to add another reservation if you are installing two servers.

9. Click **Close** when you have finished adding servers.

10. To view your new reservations, single-left-click on **Reservations** in the left-hand pane. All reservations are displayed in the right-hand pane. In this example, two reservations have been configured for *scs1.scsnetwork.local* and *scs2.scsnetwork.local*.



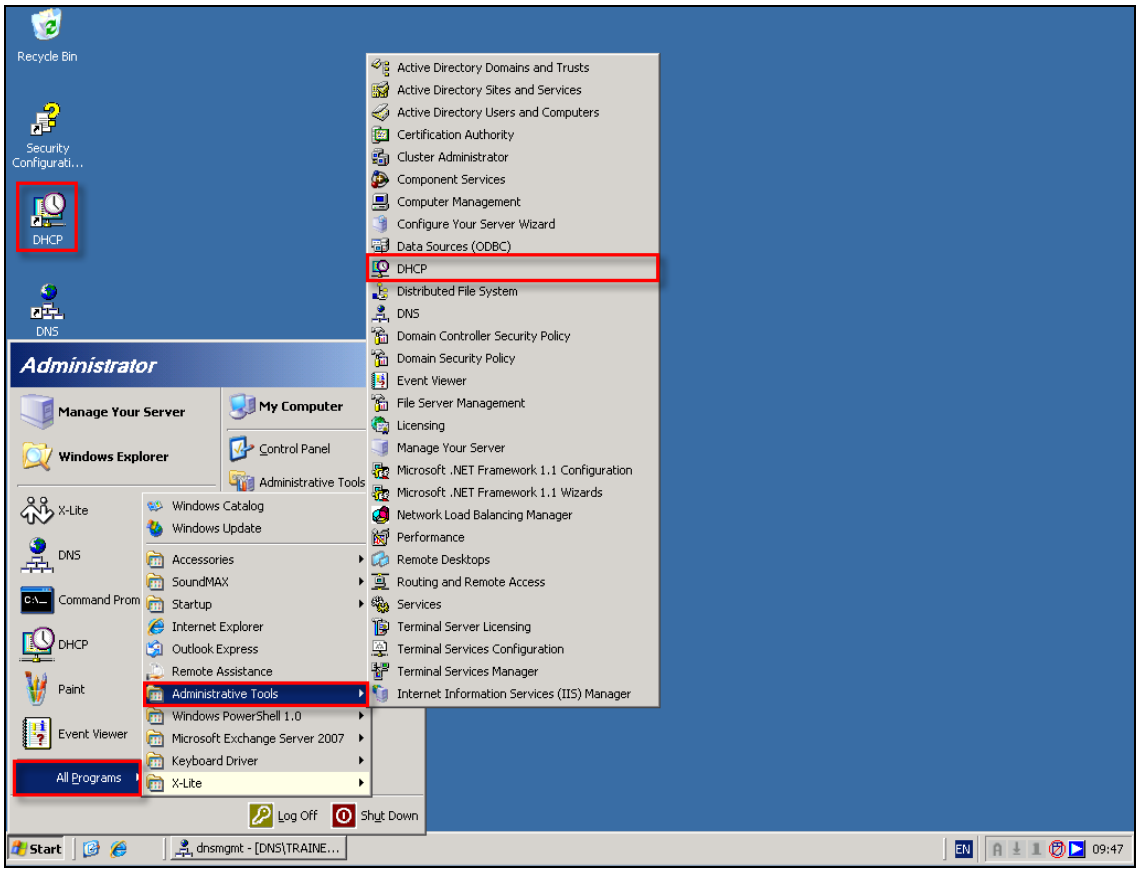
Setting Option 66 on Windows Server 2003

Note: Option 66 is a DHCP option used for provisioning Avaya 1200 series phones and Polycom phones. Other phones may function with other DHCP options.

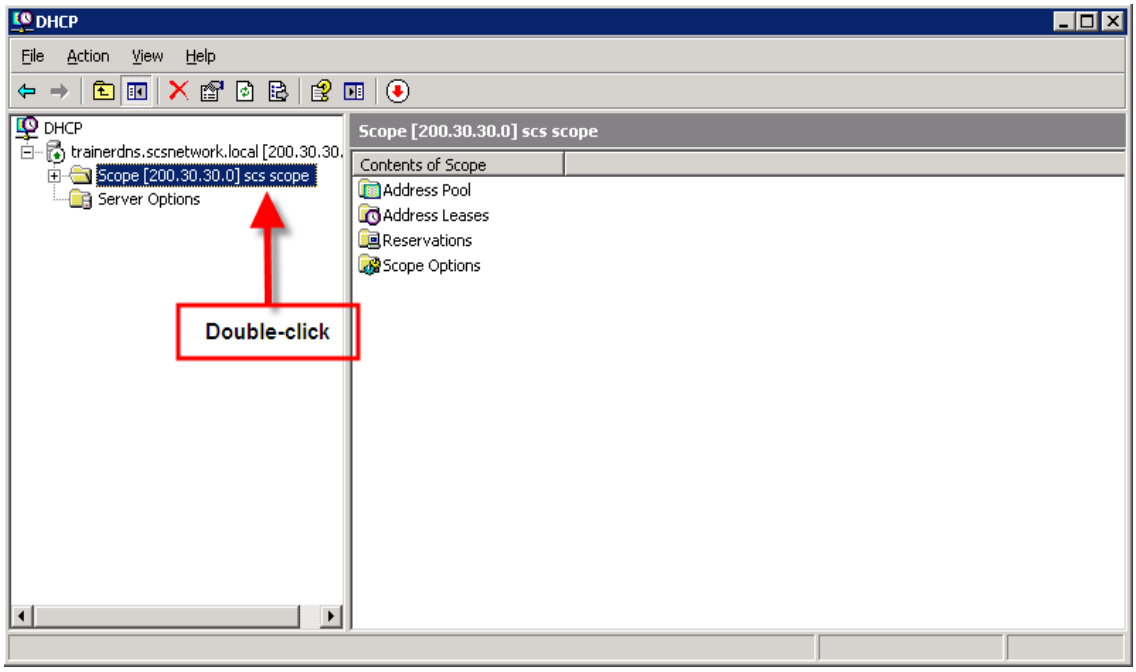
Option 66 can be configured on the DHCP server to direct IP phones to the SCS server for user profile information, so that when the phone picks up its IP address during boot-up, it will also automatically connect to the SCS for its user profile. This information *can* be configured manually on the phone itself in the absence of a DHCP server or Option 66, but for speed and efficiency purposes you may wish to configure this option on the DHCP server. On a large network with many users it would make sense to be able to simply plug phones in and have them gather all the information they require automatically, rather than having to set the download address (or TFTP server address) on each phone individually.

To configure Option 66:

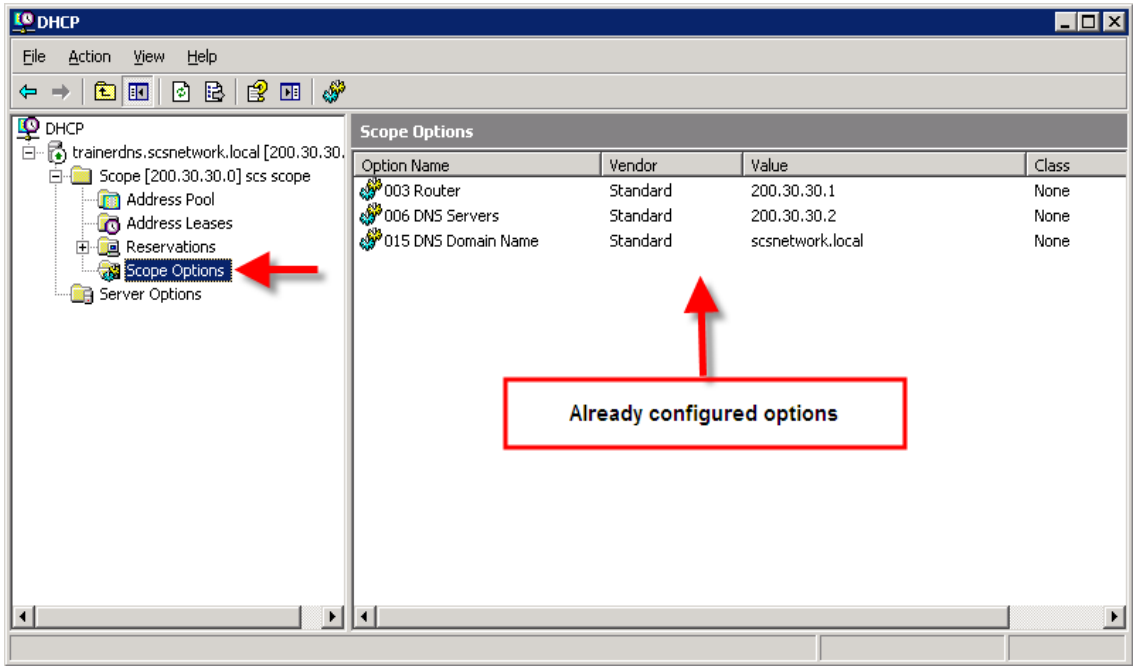
1. On the Windows Server, open the DHCP server application, either by double-clicking on the desktop icon, or by navigating through the **Start** menu.



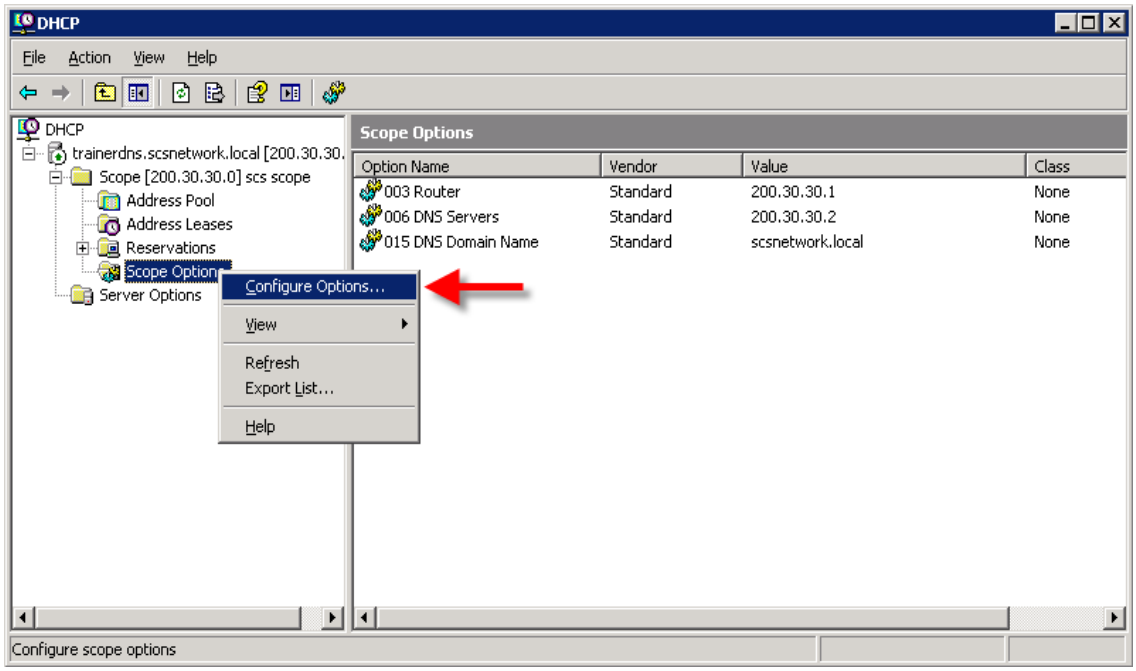
2. In the left-hand pane, double-click on the ‘Scope’ in which the SCS is situated – a scope is merely a range of IP addresses to which devices can be assigned.



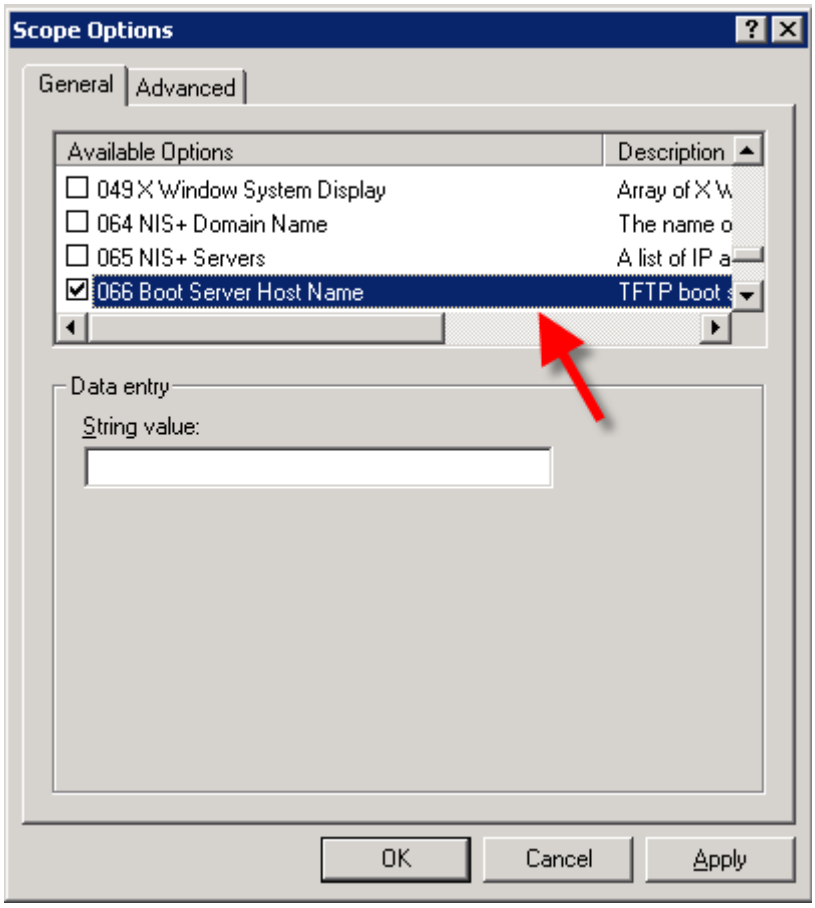
3. Click on **Scope Options** to call up a list of configured DHCP options in the right-hand pane – if Option 66 is already configured you will not be able to configure another instance, in which case the TFTP address will have to be set on phones on an individual basis. Check with the site administrator.



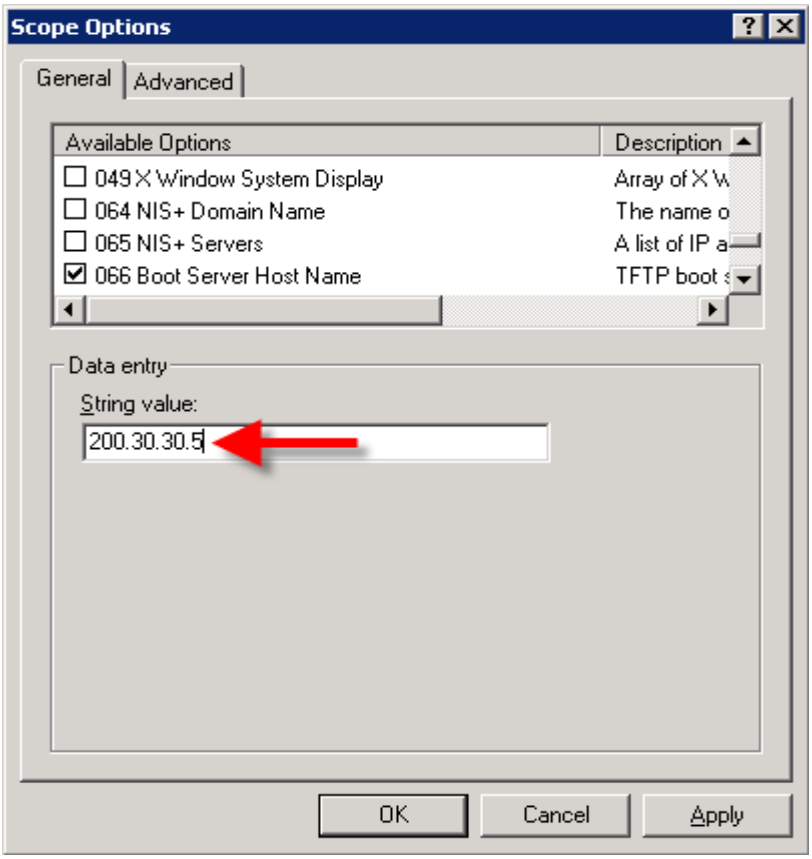
4. Right-click on **Scope Options** in the left-hand pane, and select **Configure Options**.



5. Scroll down the list of available options and select **066 Boot Server Host Name** by placing a tick in its check-box.

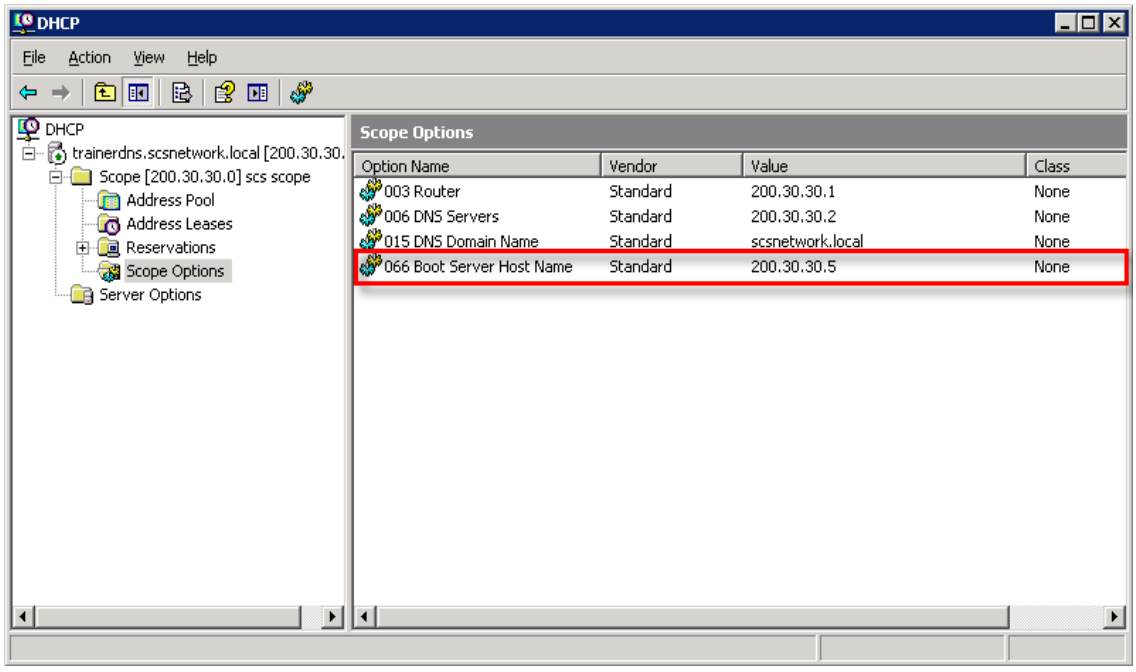


6. In the **String Value** text box, enter the IP address of the SCS server – if installing an HA system, enter the address of the primary server.



7. Click **Apply** followed by **OK**.

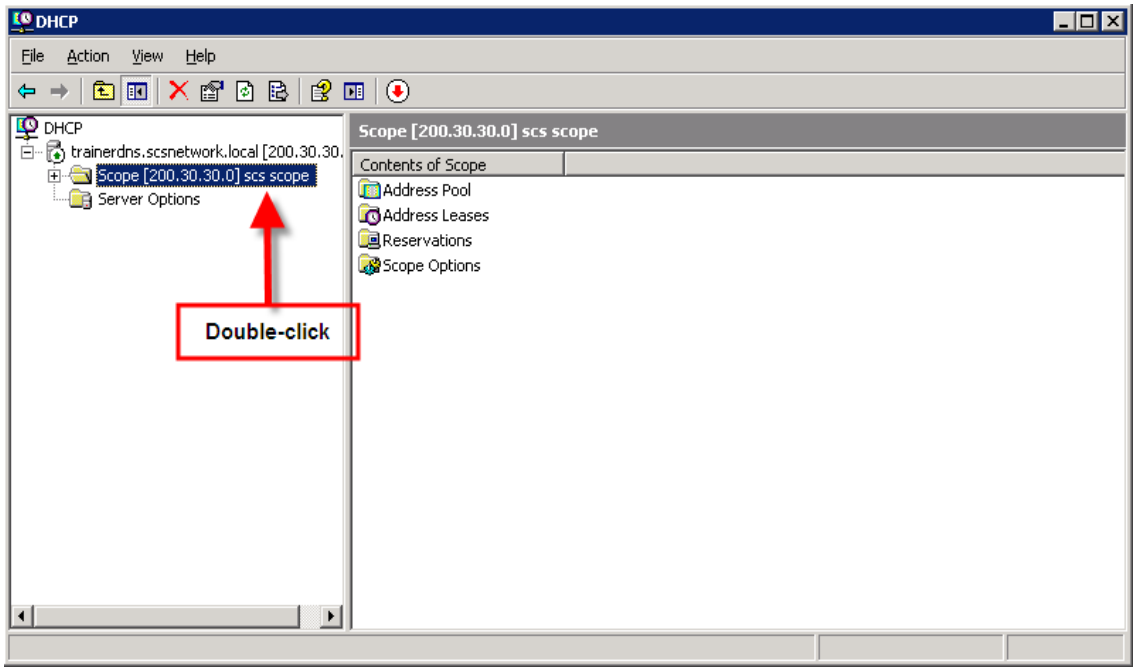
8. The new option is displayed in the right-hand pane. Option 66 configuration is complete.



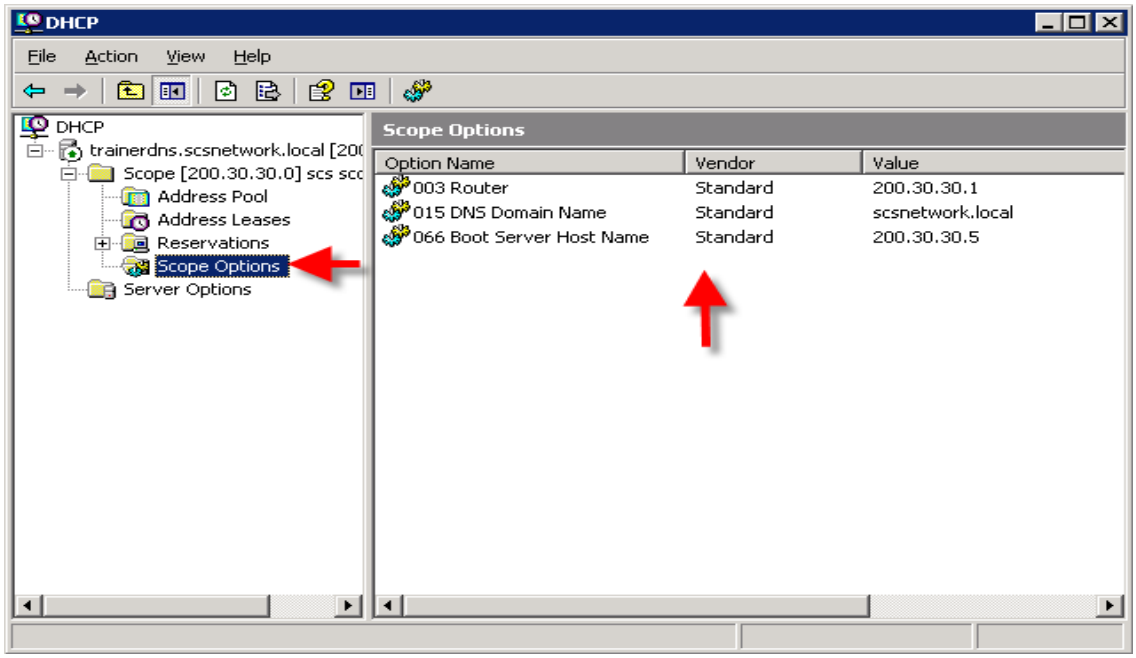
Setting Option 6 (When Utilizing SCS Onboard DNS)

In circumstances where you find it necessary to use the SCS's own onboard DNS service along side a third party DHCP server, you will need to specify the address of the SCS DNS. This is done in the following way:

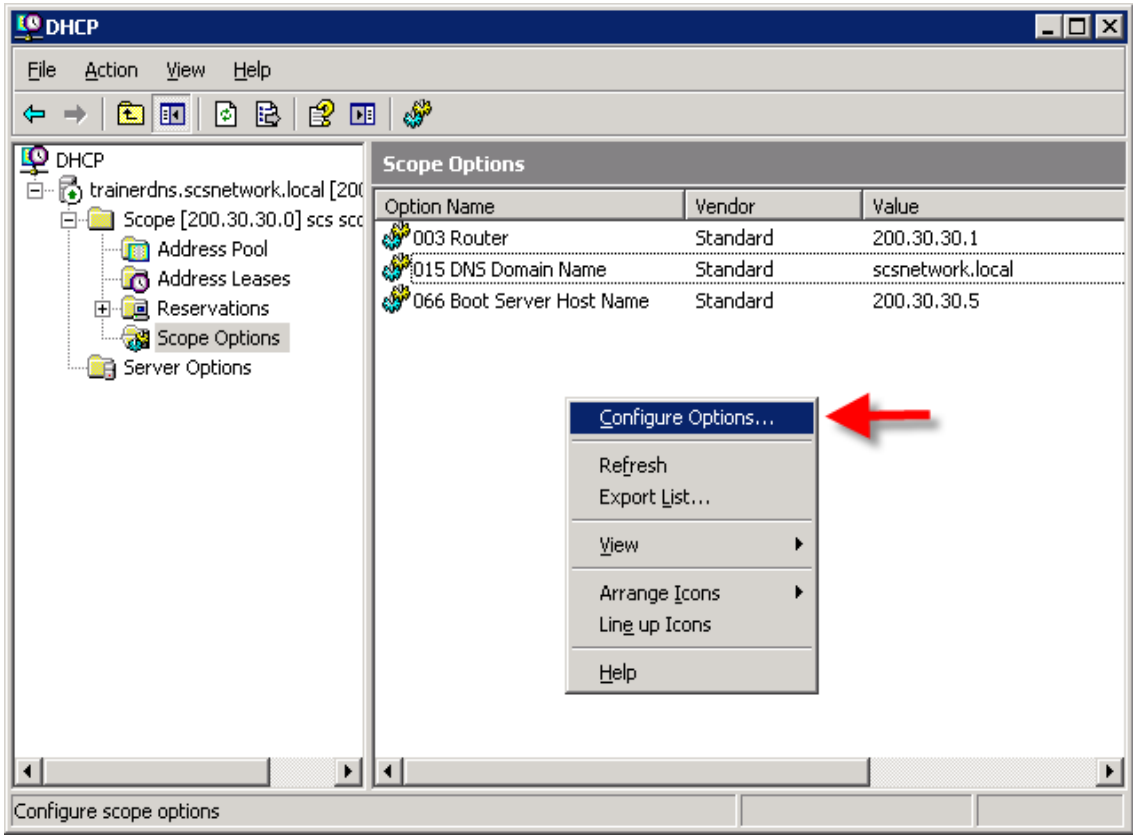
1. In the left-hand pane, double-click on the 'Scope' in which the SCS is situated – a scope is merely a range of IP addresses to which devices can be assigned.



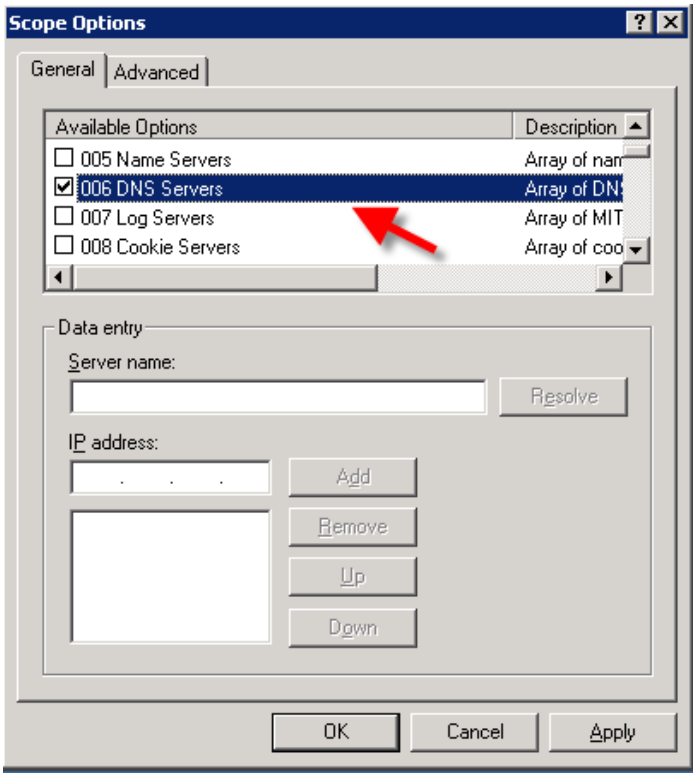
2. Click on **Scope Options** to call up a list of configured DHCP options in the right-hand pane.



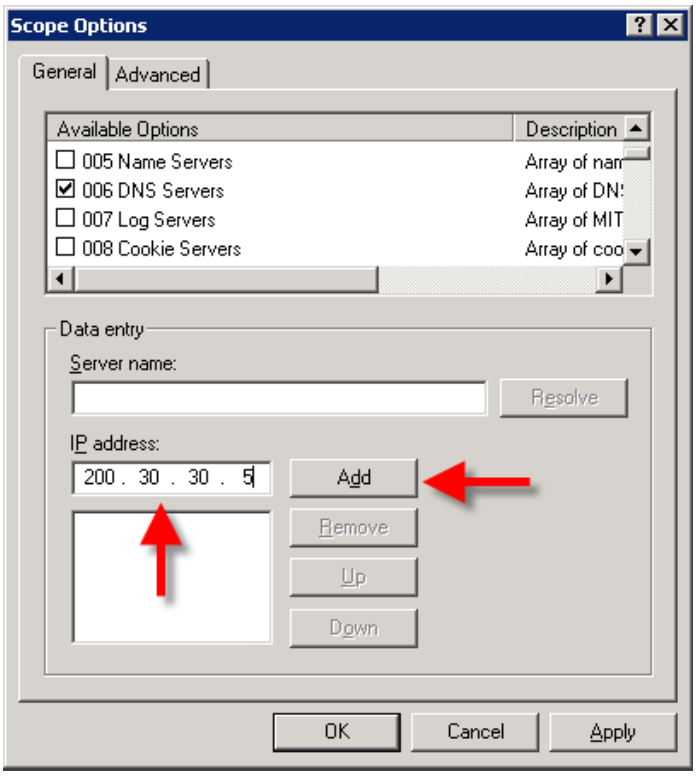
3. Right-click in the right-hand pane and select **Configure Options**.



4. Scroll through the list of available options and select **006 DNS Servers** by placing a tick in its check-box.

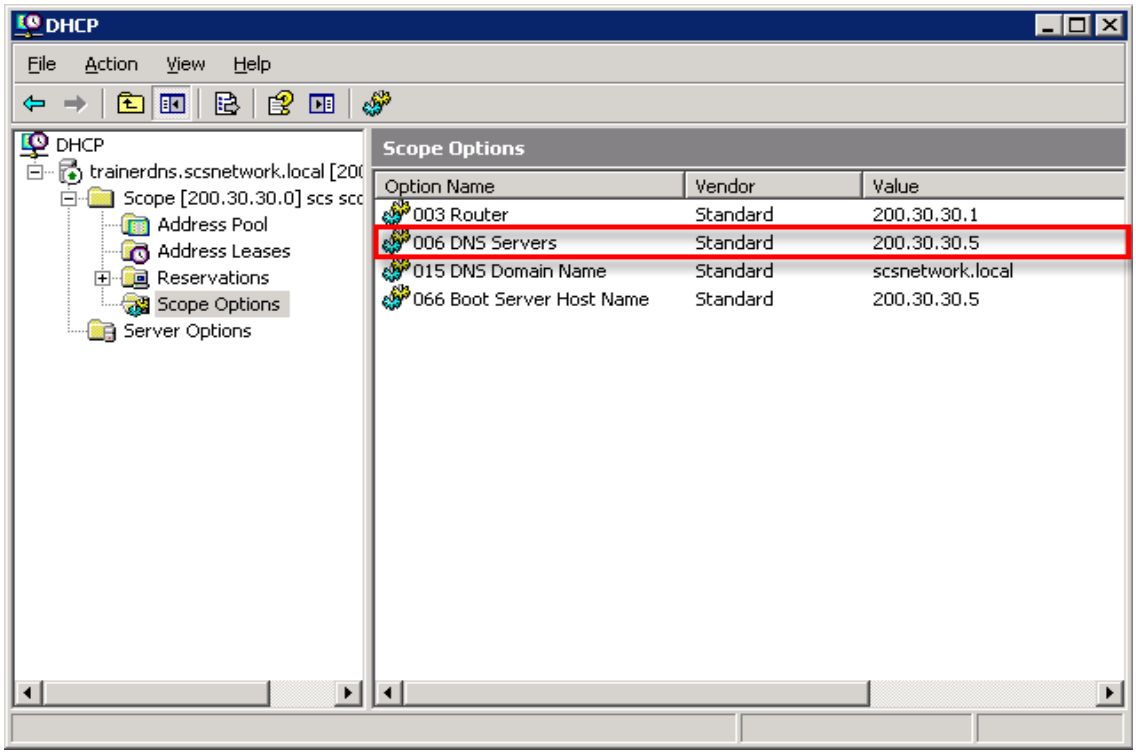


5. Enter the **IP address** of the SCS and click **Add** (if installing an HA system in which both SCS servers will provide DNS add the secondary server's address too).



6. Click **Apply** followed by **OK**.

7. The new option is shown in the Options pane.



Other DHCP Options

Other DHCP options can be configured to aid in the configuration and running of your IP telephony devices. For example, **Option 2** can be used to configure the UCT (Universal Coordinated Time) offset in seconds.

Option 42 can be used to specify a range of servers that can be used to supply a client with NTP (Network Time Protocol) data.

Configuring Windows Server 2003 DNS

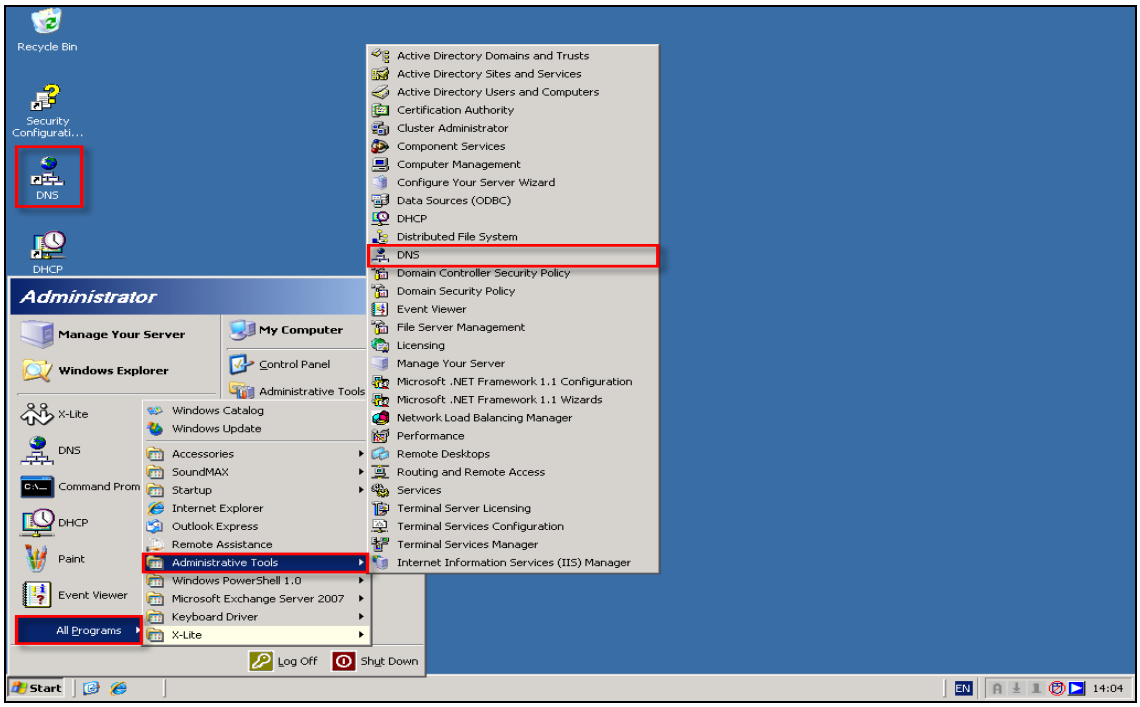
Single Server System – A Records

A single server installation can be configured to utilize DNS A Records or a combination of A Records and SRV Records. In this short section we'll look at creating A Records for a single server, non-HA system.

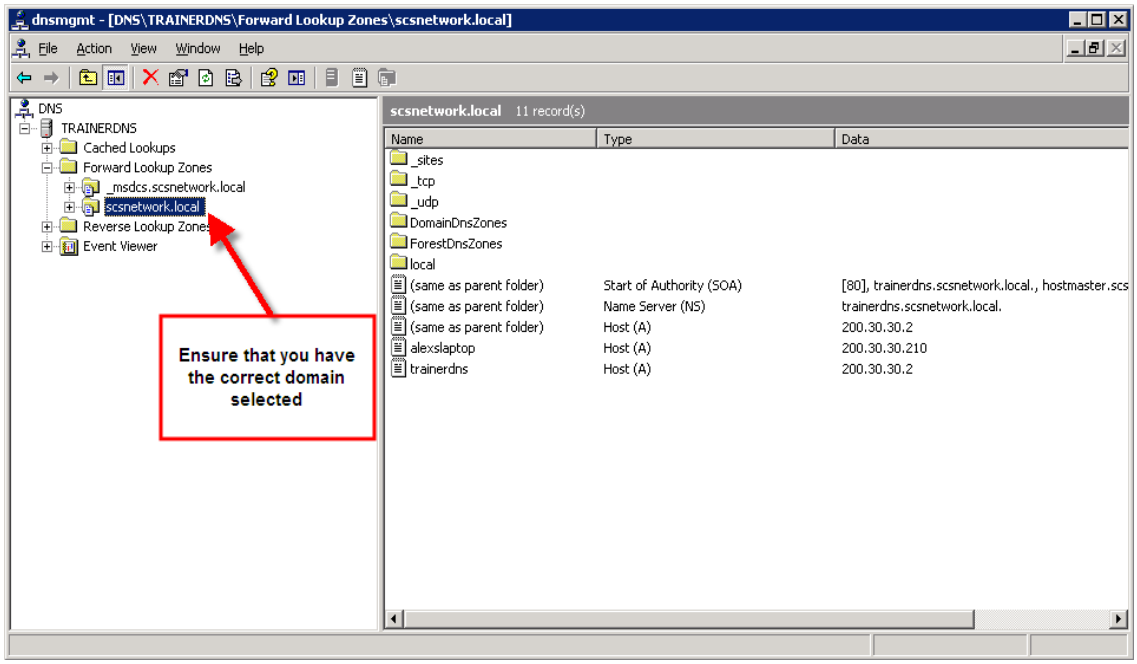
Remember: In circumstances where only A Records are present on the DNS, the SCS SIP domain should always be set to the server's **fully qualified domain name** – i.e., the host and domain name: *scshost.scsdomain.com*.

To create an A Record:

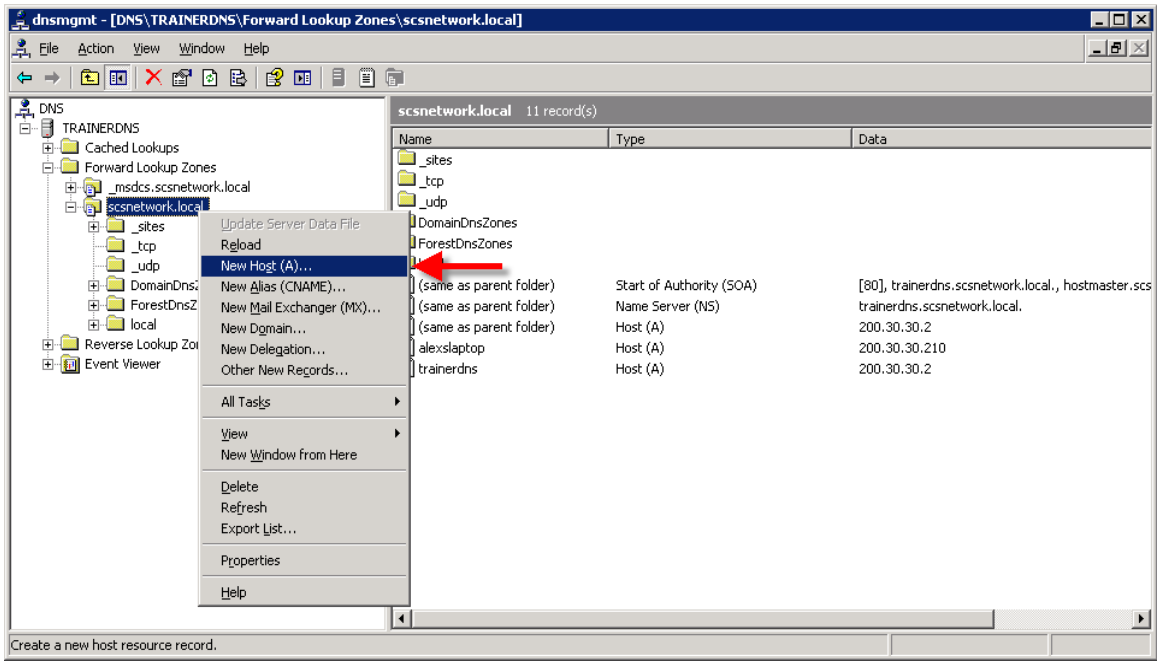
1. Open the DNS service on the Windows Server, either by double-clicking on the desktop icon, or by navigating to it via the **Start** menu.



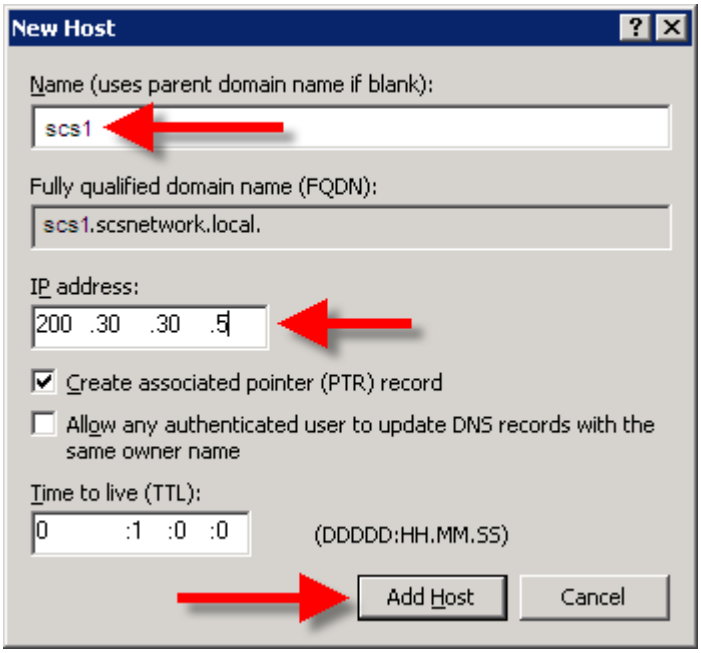
2. In the left-hand pane, single-left-click on the domain into which the SCS will be installed, in the example below the target domain for the SCS is *scsnetwork.local*.



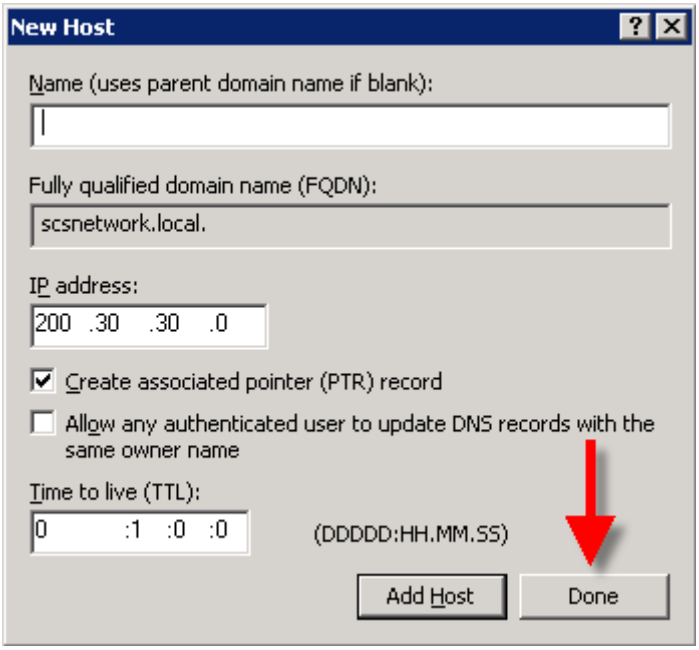
3. Right-click on the domain and select **New Host (A)**.



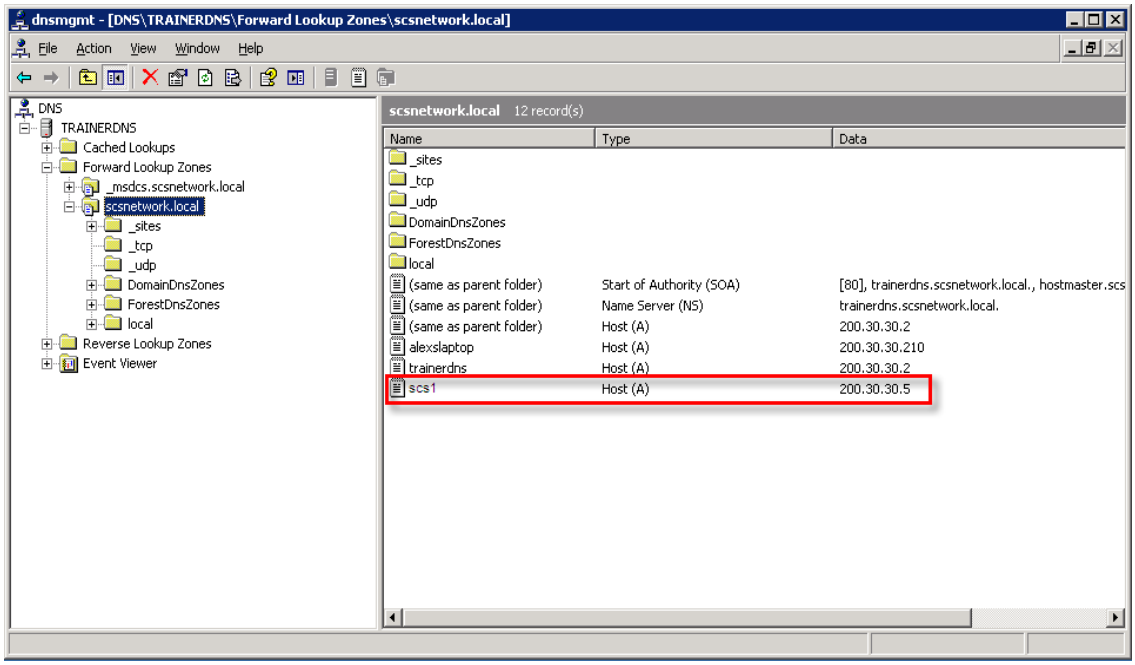
4. In the dialogue box that appears, enter the name of the server (the fully qualified domain name field will populate automatically) and its IP address, and then click **Add Host**.



5. Click **Done**.



6. The newly added A Record is displayed in the right-hand pane along with any other records already configured.

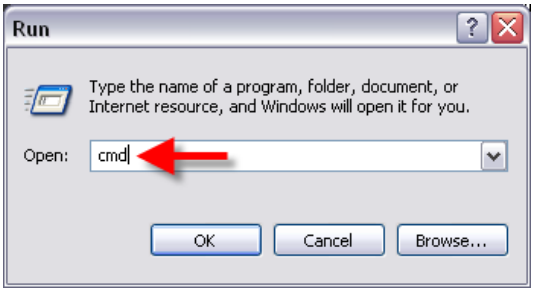


A Record creation is now complete. Don't forget to set the SIP domain to the server's fully qualified domain name during SCS configuration.

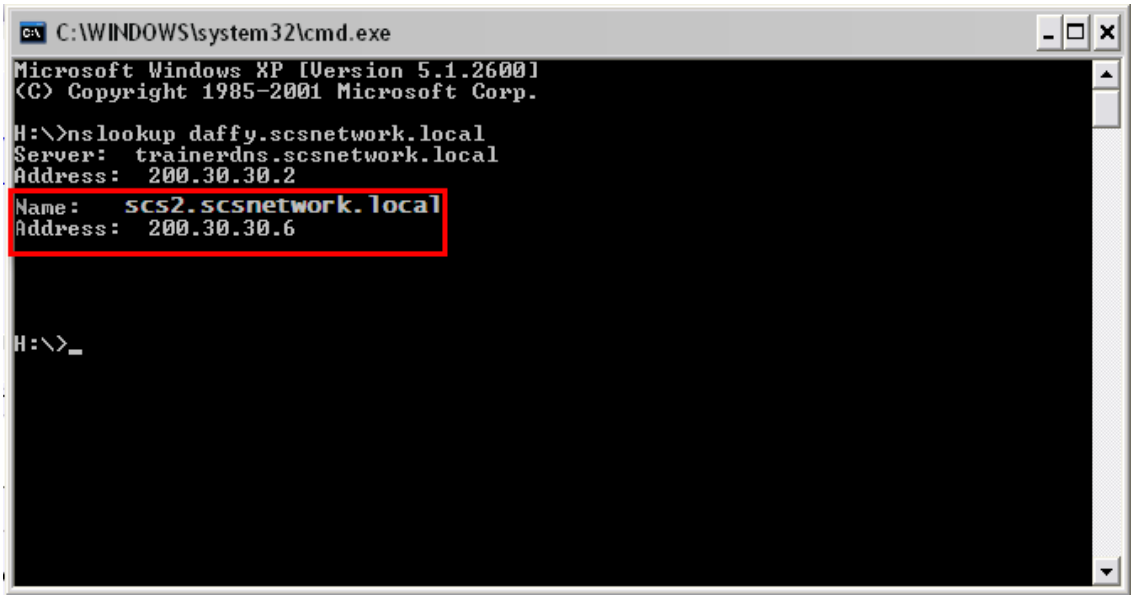
Testing DNS

You can run a simple test to determine whether DNS is working correctly:

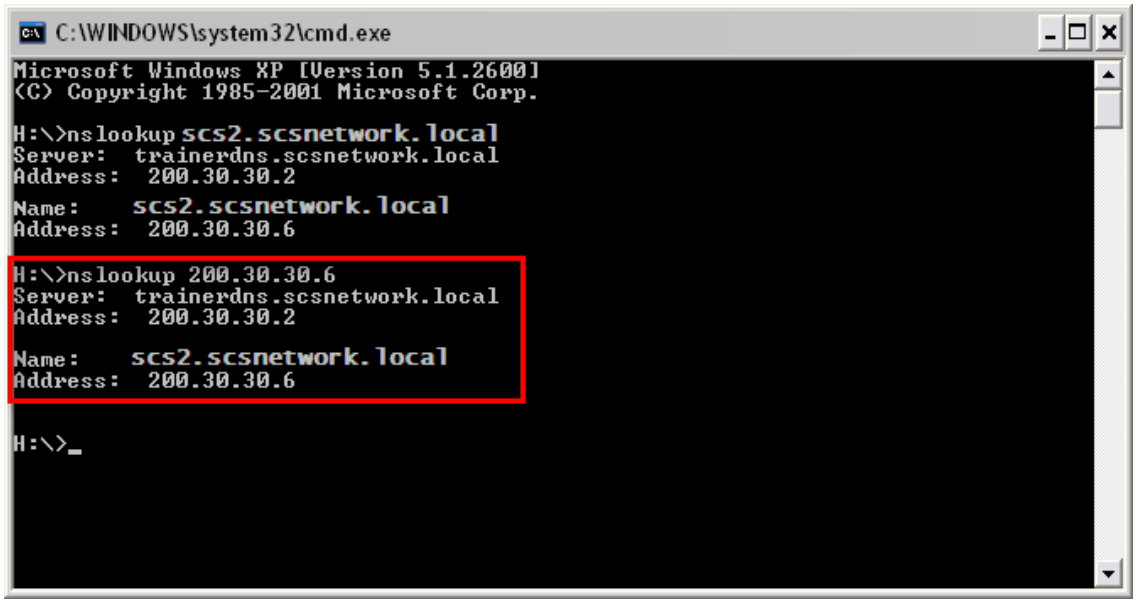
1. On a network connected PC, open the command prompt window by opening the **Start** menu and selecting **Run**.
2. In the box that opens, type **cmd** and press the **Enter** key.



3. At the prompt, type **`nslookup servername.serverdomain.com`** (enter the host name and domain name of your server) and press **Enter**.
4. If DNS is behaving properly the query should return the server's name and IP address.



5. To double-check that your records are functioning properly, run the command again, but this time lookup the IP address instead of the server name.



Single Server System – A Records & SRV Records

A single server installation can be configured to utilize DNS A Records or a combination of A Records and SRV Records. In this short section we'll look at creating A Records and SRV Records for a single server, non-HA system.

Remember: In circumstances where SRV records are present in the DNS, the SIP domain should be configured as just the domain name – e.g., *scsdomain.com*.

During this process, you will create the following records:

Configuration Type	No. of A Records	No. of SRV Records
1 server	1	2

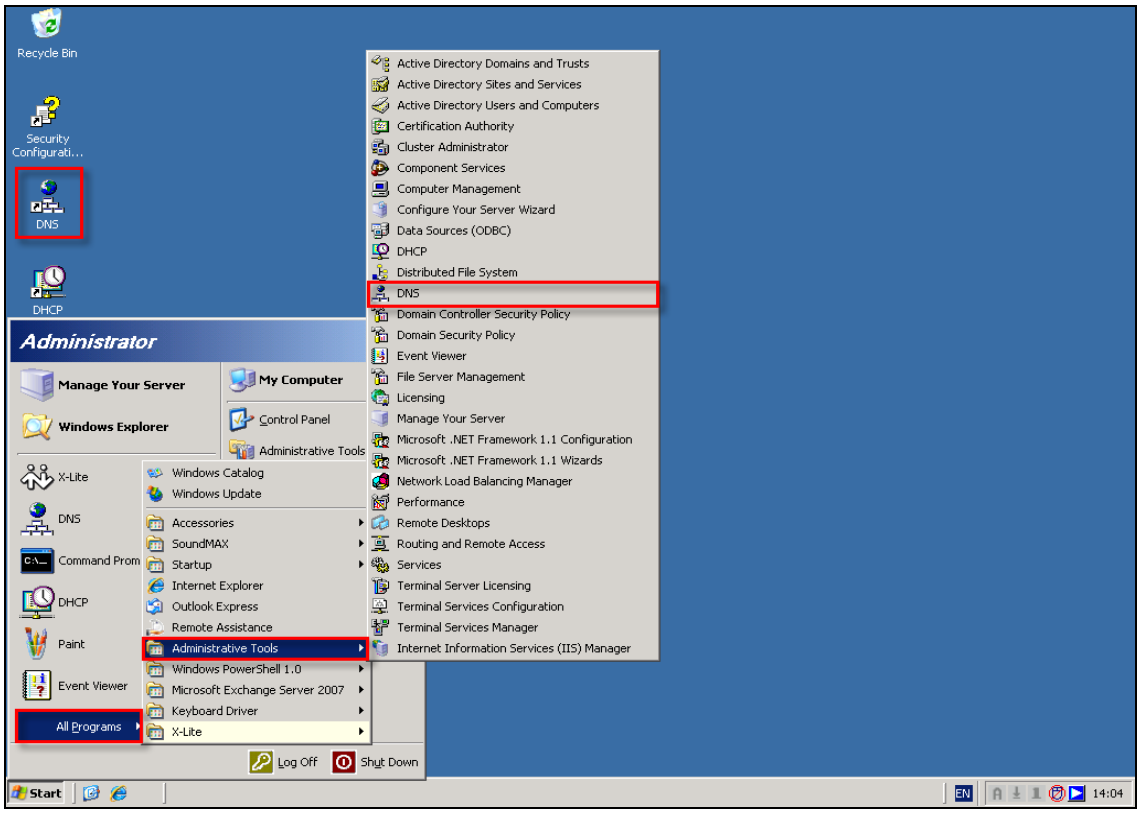
The following SRV records will need to be created:

SRV Record	Service	Protocol	Priority	Weight	Port	Host offering the service
1	_sip	_tcp	2	0	5060	servername.domain.com
2	_sip	_udp	1	0	5060	servername.domain.com

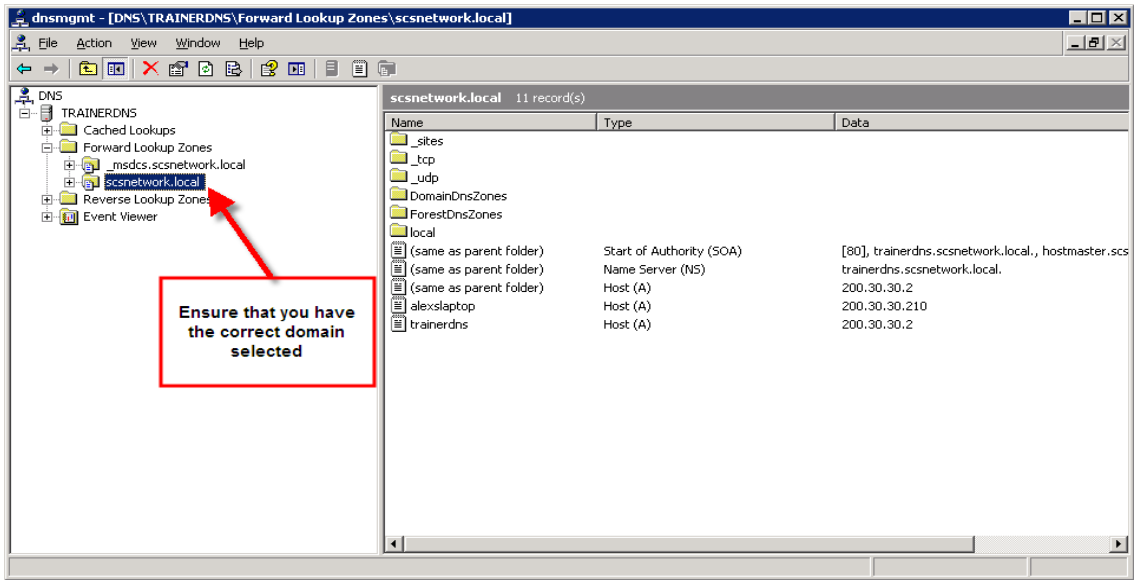
The following instructions will show you how to create each of these records.

Creating an A Record

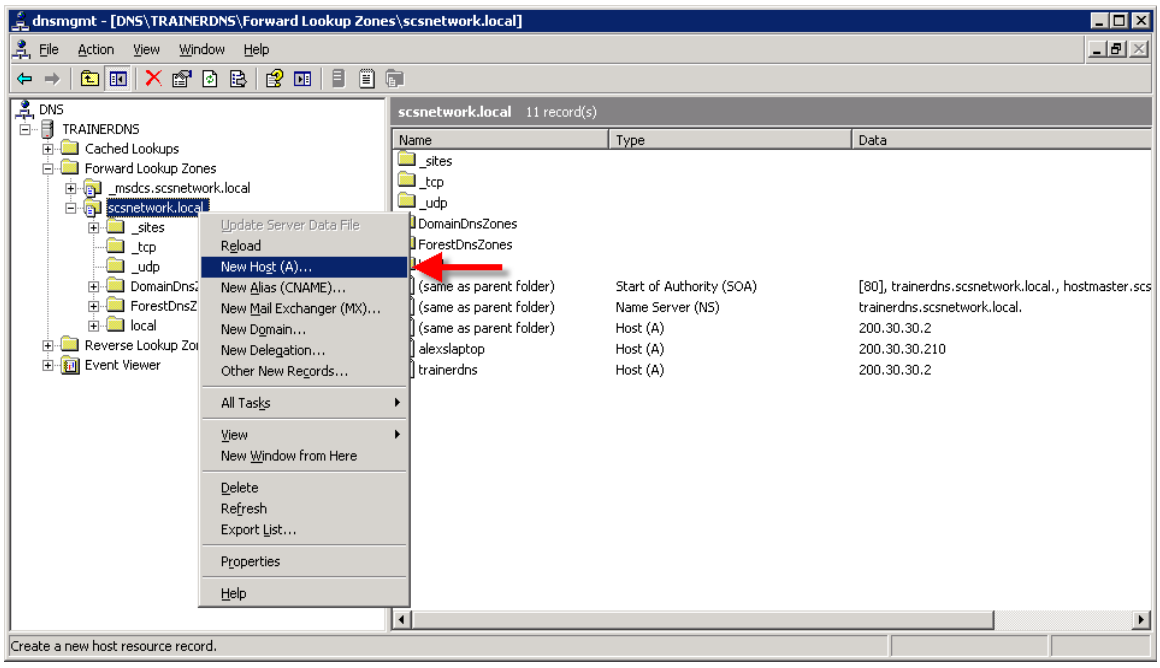
1. Open the DNS service on the Windows Server, either by double-clicking on the desktop icon, or by navigating to it via the **Start** menu.



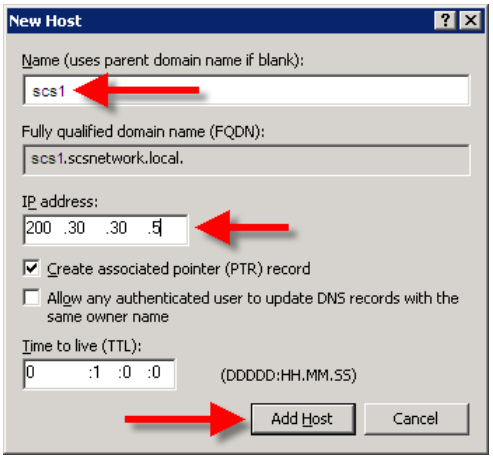
2. In the left-hand pane, single-left-click on the domain into which the SCS will be installed, in the example below the target domain for the SCS is *scsnetwork.local*.



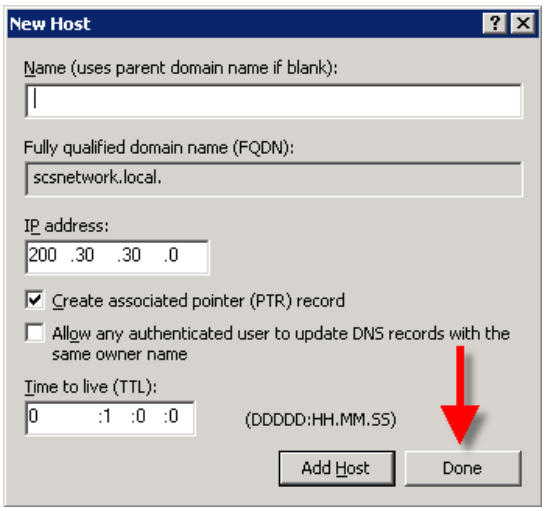
3. Right-click on the domain and select **New Host (A)**.



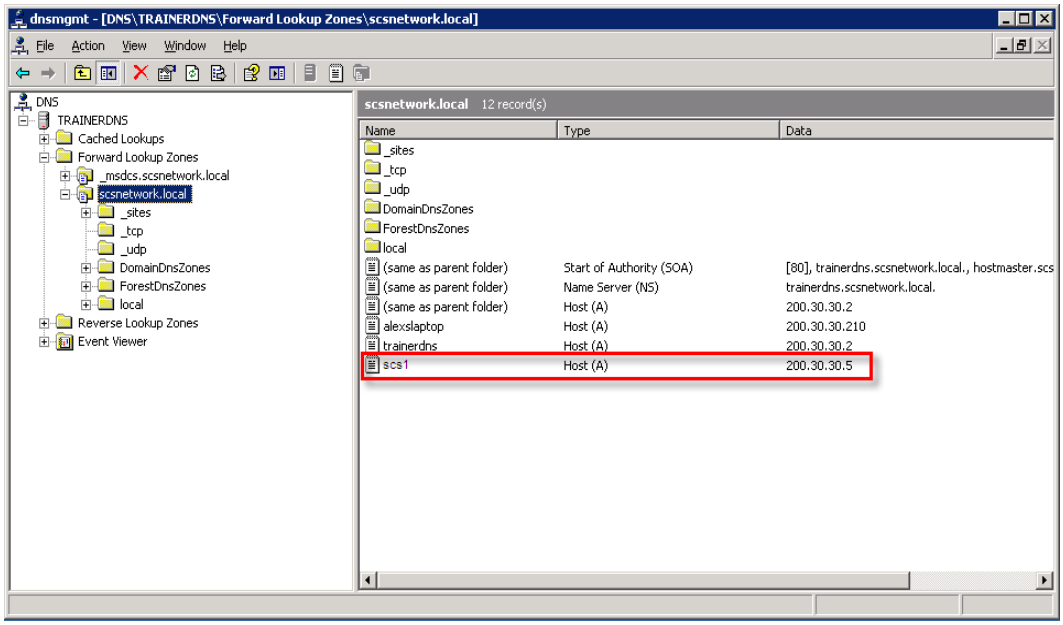
4. In the dialogue box that appears, enter the name of the server (the fully qualified domain name field will populate automatically) and its IP address, and then click **Add Host**.



5. Click **Done**.

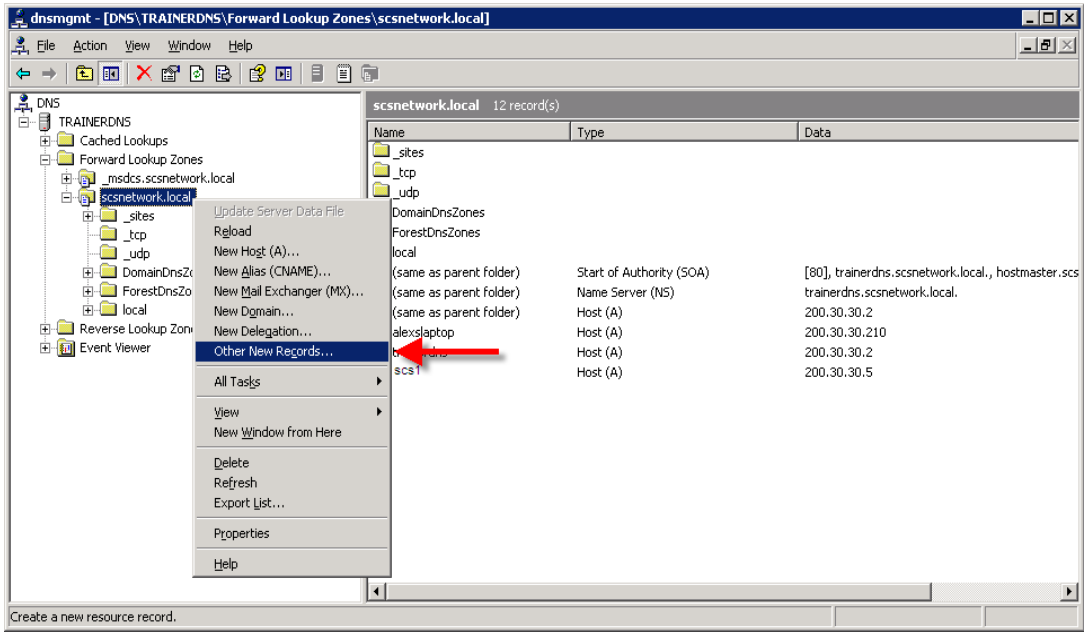


6. The newly added A Record is displayed in the right-hand pane along with any other records already configured.

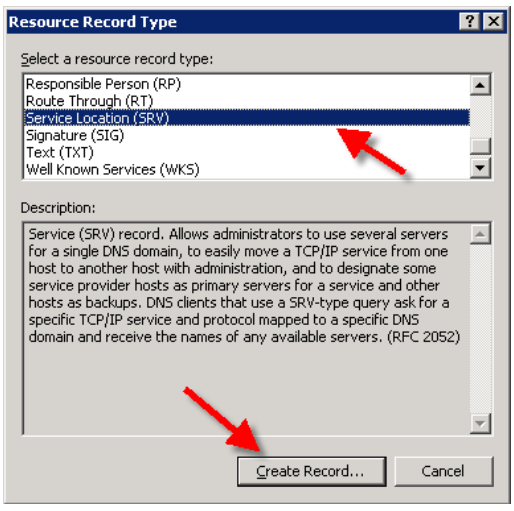


Creating SRV Records

1. Right-click on the target domain in the left-hand pane and select **Other New Records**.

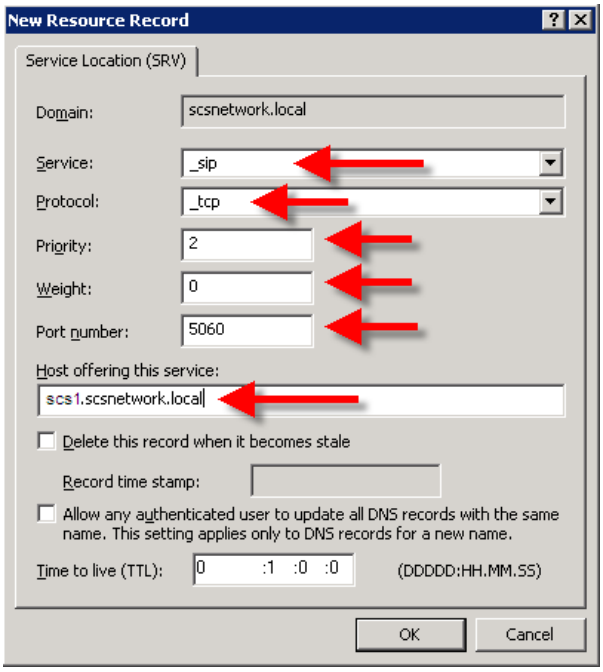


2. In the window that opens, scroll down the list and select **Service Location (SRV)** and then click on **Create Record**.



3. Enter the following values:

Service	**_sip**
Protocol	_tcp
Priority	2
Weight	0
Port number	5060
Host offering this service	*scsservername.domain.com*



4. Click **OK**.

5. You are returned to the record type selection screen again. Select **Service Location (SRV)** again and click **Create Record**.

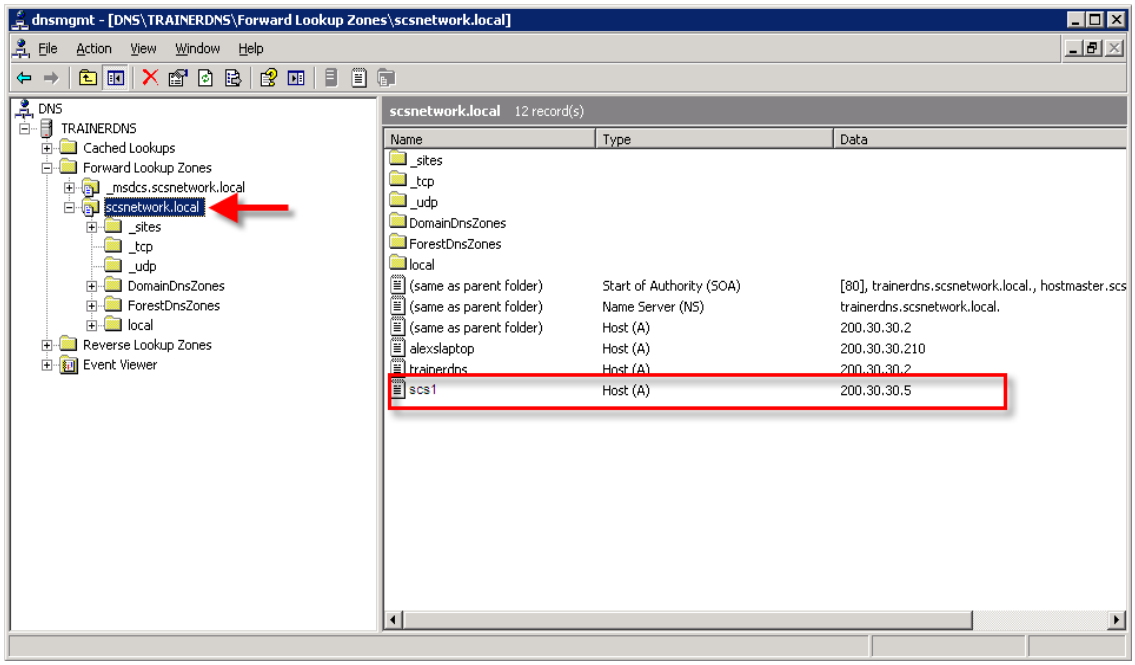
6. Enter the following values for the second SRV record:

Service	**_sip**
Protocol	_udp
Priority	1
Weight	0
Port number	5060
Host offering this service	*scsservername.domain.com*

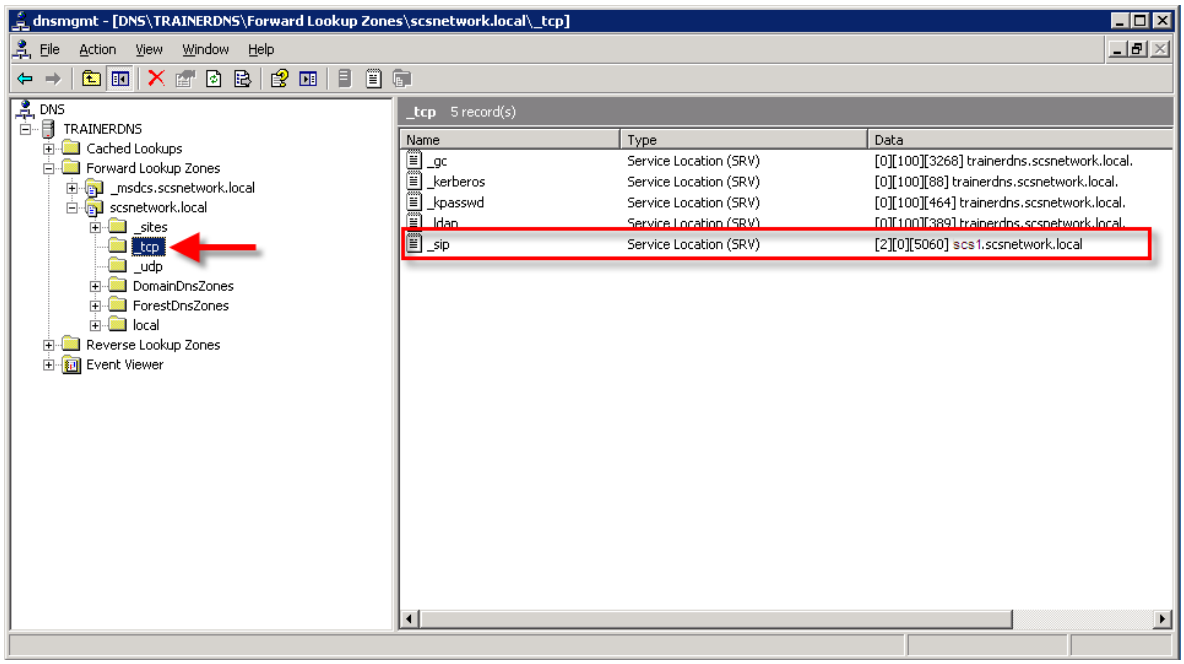
7. Click **OK**.

8. Click **Done**.

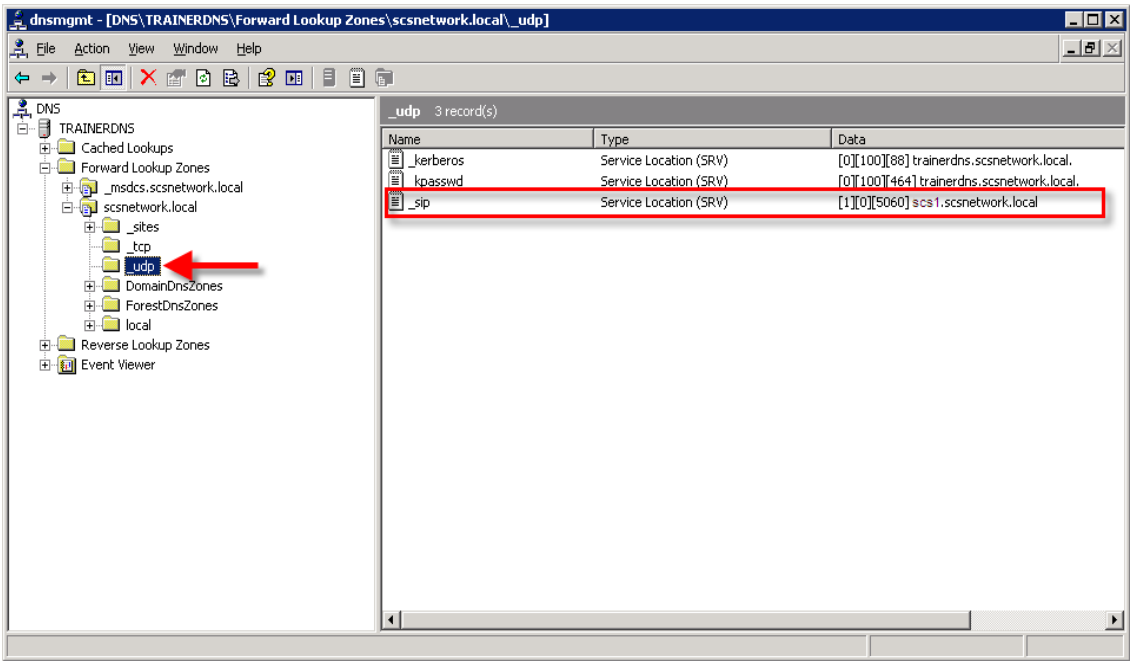
9. You should now be able to see your A Record in the domain folder . . .



. . . a SIP SRV record in the **_tcp** folder . . .



. . . and a SIP SRV record in the **_udp** folder.

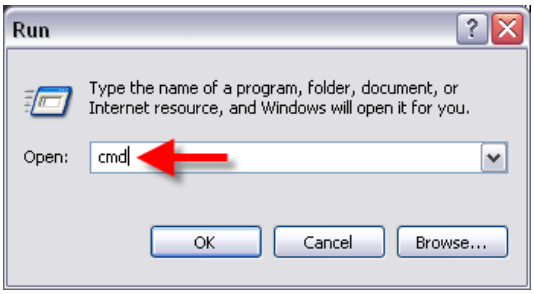


A Record and SRV Record creation is now complete. Don't forget to set the SIP domain to *domain.com* when configuring the SCS server.

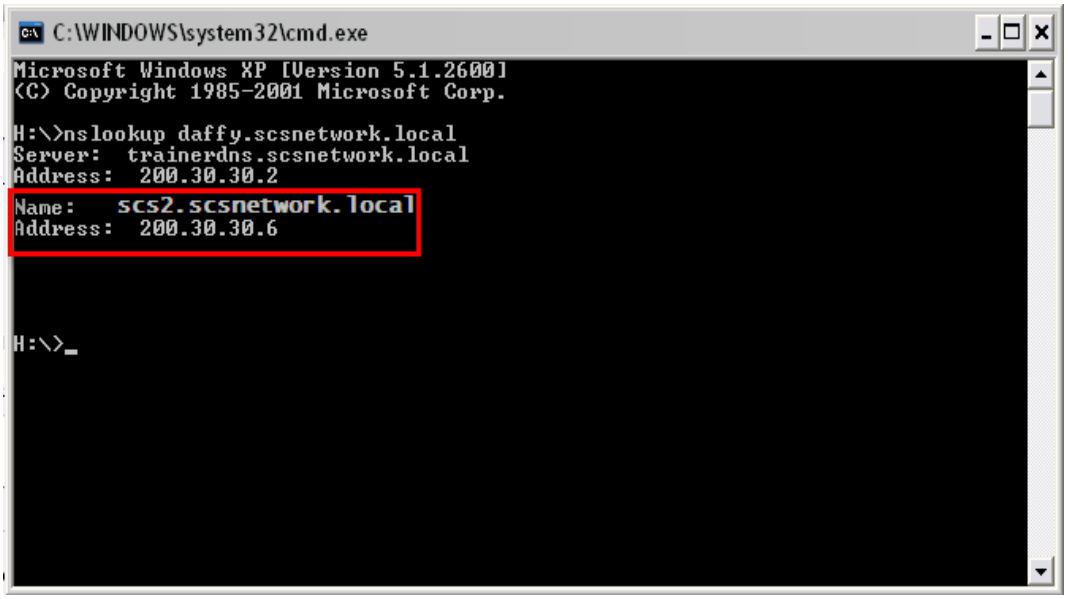
Testing DNS

You can run a simple test to determine whether DNS is working correctly:

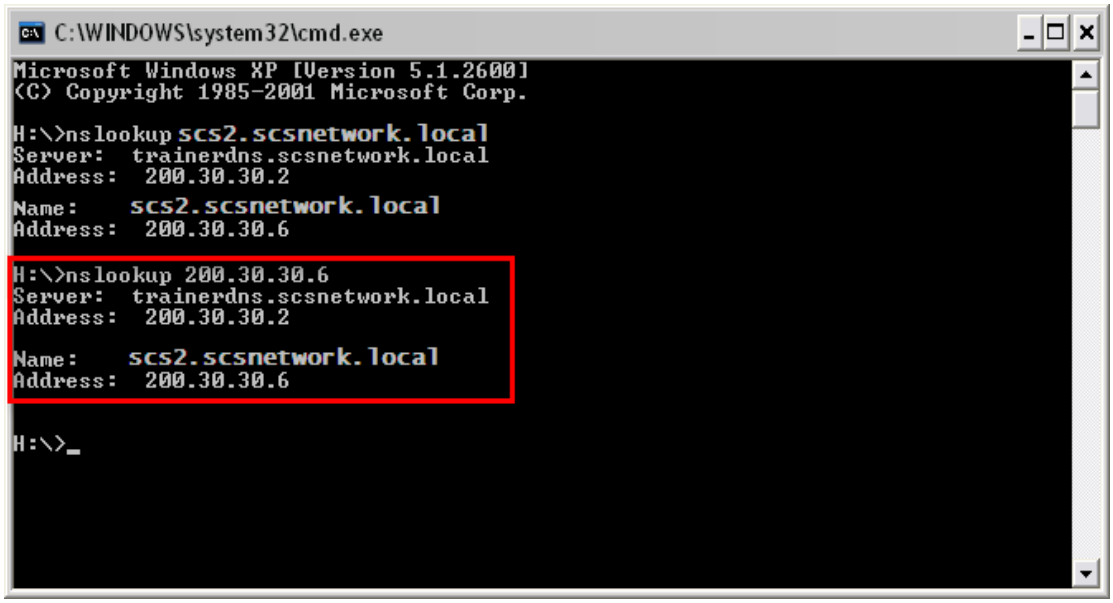
1. On a network connected PC, open the command prompt window by opening the **Start** menu and selecting **Run**.
2. In the box that opens, type **cmd** and press the **Enter** key.



3. At the prompt, type **`nslookup servername.serverdomain.com`** (enter the host name and domain name of your server) and press **Enter**.
4. If DNS is behaving properly the query should return the server's name and IP address.



5. To double-check that your records are functioning properly, run the command again, but this time lookup the IP address instead of the server name.



Dual Server (HA) System – A Records & SRV Records

As discussed earlier in this document, High Availability (HA) systems only function if SRV records are present in the DNS. This section will show you how to create all necessary A Records and SRV Records for the successful implementation of an HA SCS.

During this process, you will create the following DNS records:

No. of sub-domains	*No. of A records*	*No. of A records in sub-domain1*	*No. of A records in sub-domain2*	*No. of SRV records*	*No. of SRV in root*	*No. of SRV in sub-domain1*	*No. of SRV in sub-domain2*
2	2	*1*	*1*	12	*4*	*4*	*4*

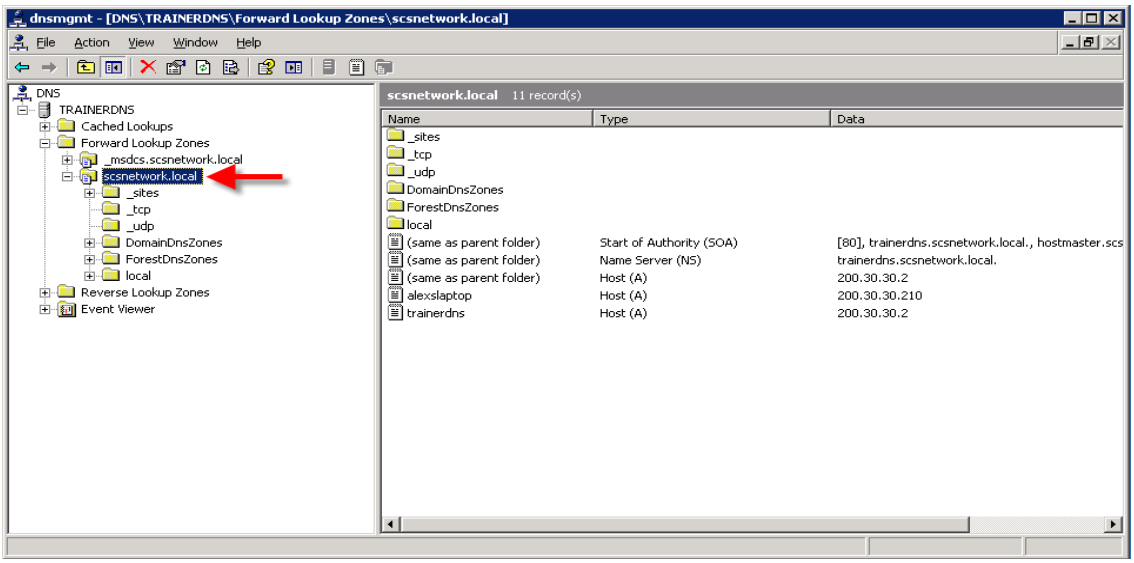
The following SRV records will be created (substitute italicised values for your own domain and server names):

SRV record	*Domain*	*Service*	*Protocol*	*Priority*	*Weight*	*Port*	*Host offering this service*
1	*root*	_sip	_udp	1	0	5060	*server1.domain.com*
2	*root*	_sip	_tcp	3	0	5060	*server1.domain.com*
3	*root*	_sip	_udp	2	0	5060	*server2.domain.com*
4	*root*	_sip	_tcp	4	0	5060	*server2.domain.com*
5	*server1*	_sip	_tcp	1	0	5070	*server1.domain.com*
6	*server1*	_sip	_udp	3	0	5070	*server1.domain.com*
7	*server1*	_sip	_tcp	2	100	5070	*server2.domain.com*
8	*server1*	_sip	_udp	4	100	5070	*server2.domain.com*
9	*server2*	_sip	_tcp	1	0	5070	*server2.domain.com*
10	*server2*	_sip	_udp	3	0	5070	*server2.domain.com*
11	*server2*	_sip	_tcp	2	100	5070	*server1.domain.com*
12	*server2*	_sip	_udp	4	100	5070	*server1.domain.com*

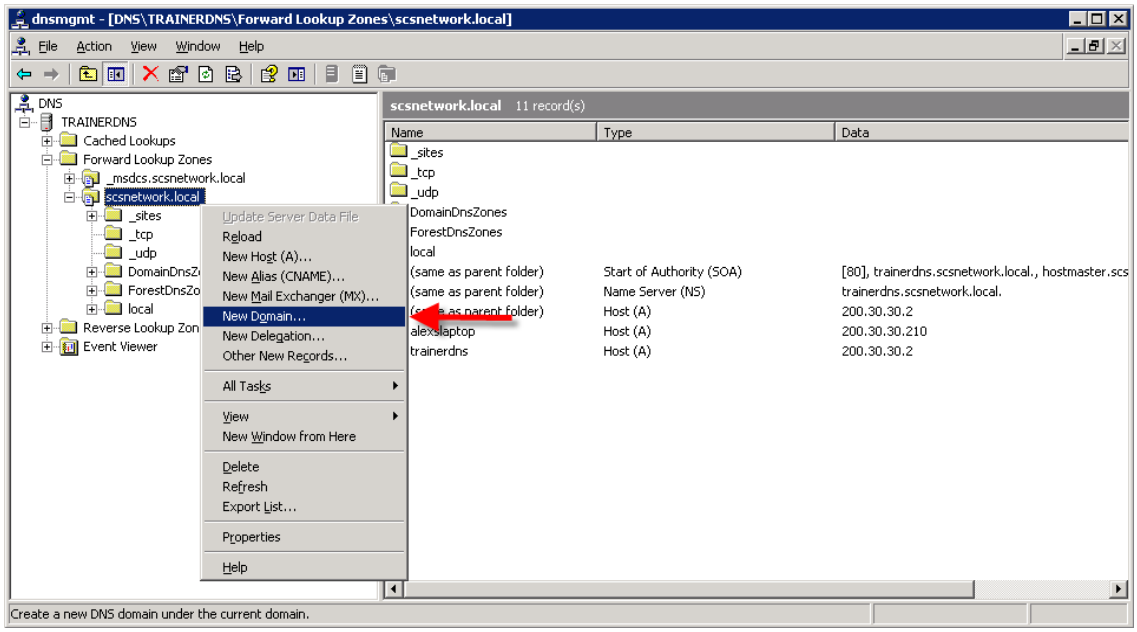
The following instructions will show you how to create each of these records in the correct locations.

Creating a sub-domain and A Record for each server

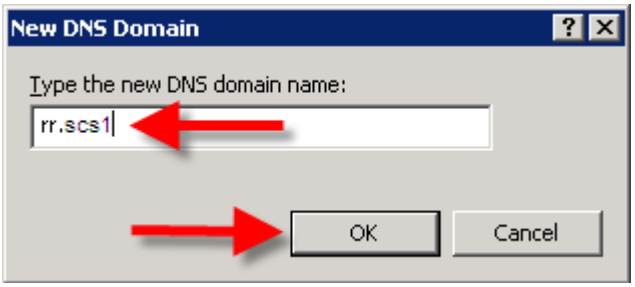
1. Ensure that you are working within the correct domain. In the coming sections we will be working with *scsnetwork.local*.



2. Right-click on the selected domain and click on **New Domain**.

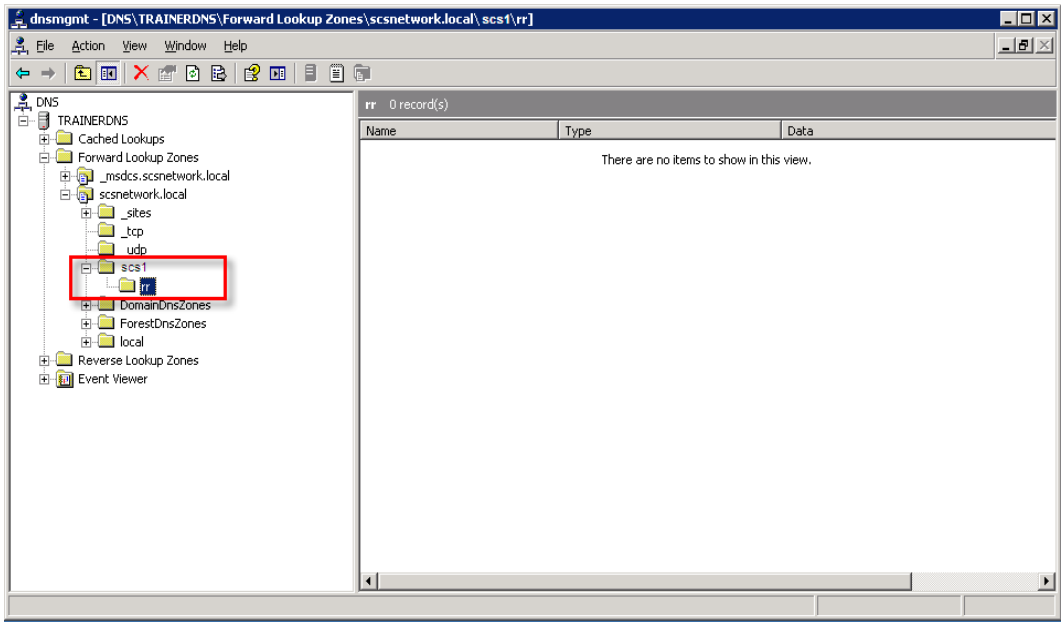


3. Name the new domain *rr.server1name*. In this document the primary server will be called *scs1* while the secondary will be known as *scs2*. In the example below the sub-domain has been named *rr.scs1.*

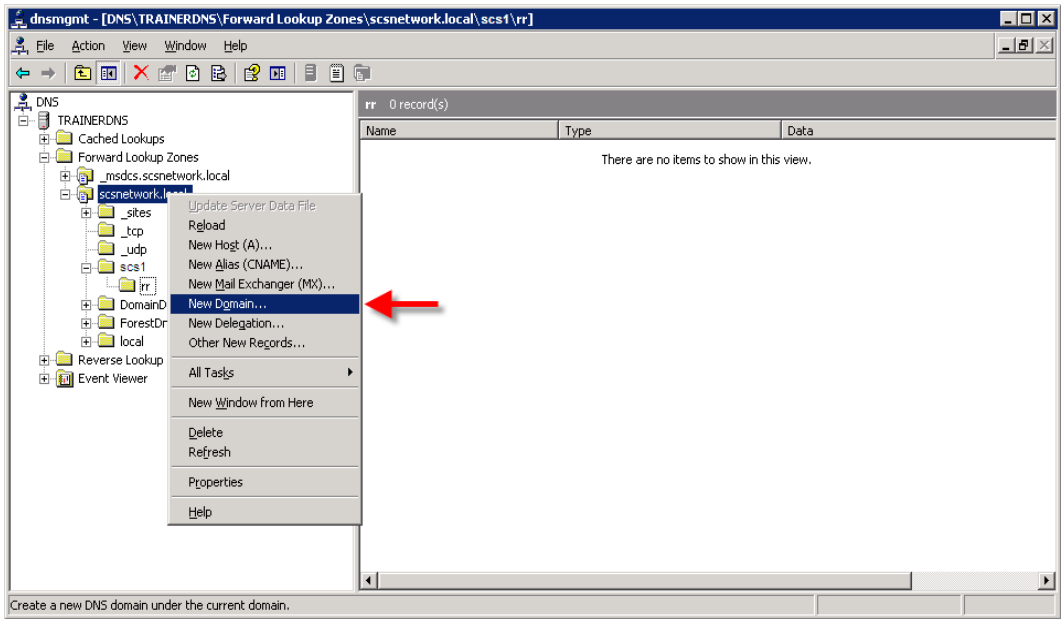


4. Click **OK**.

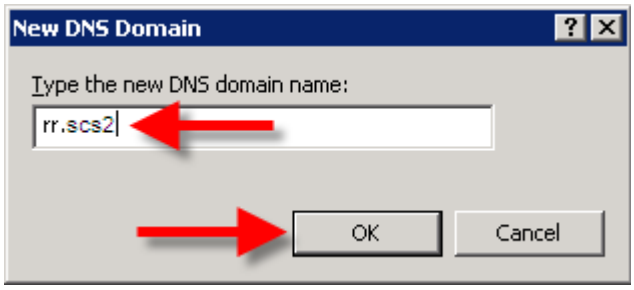
5. The new sub-domain and its ‘rr’ folder are displayed in the left-hand pane. SRV records will be created here later.



6. Right-click on the target domain again and select **New Domain**.

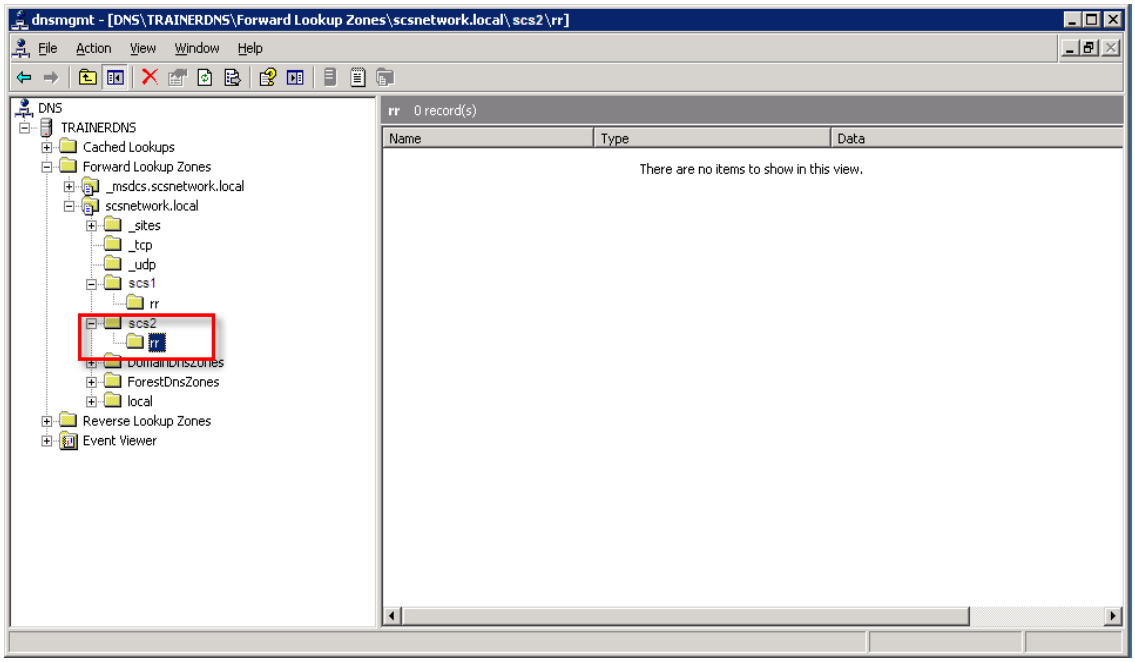


7. Name the second sub-domain *rr.server2name*. In the illustration I have created *rr.scs2*.

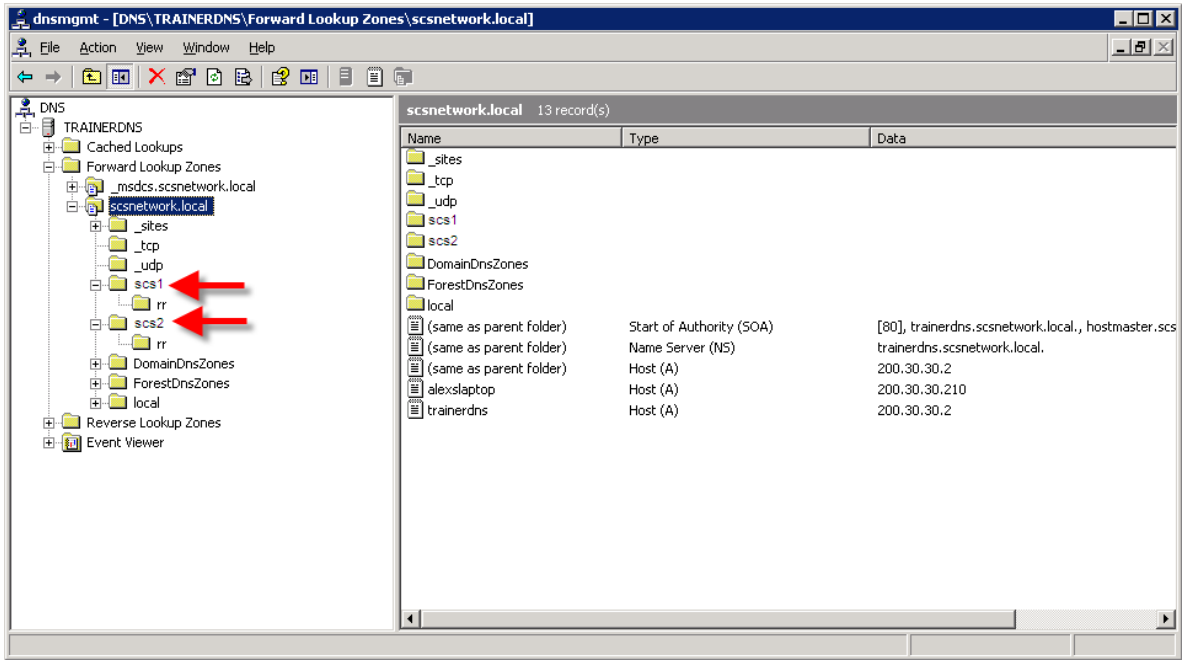


8. Click **OK**.

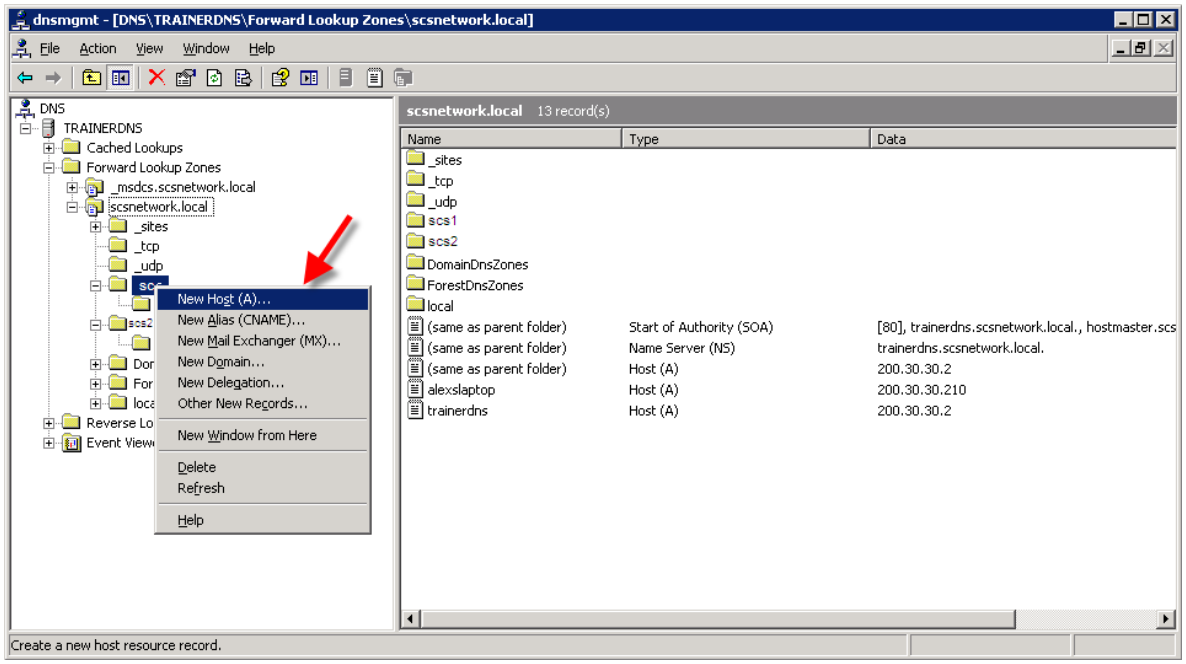
9. The second sub-domain is displayed in the tree on the left-hand side.



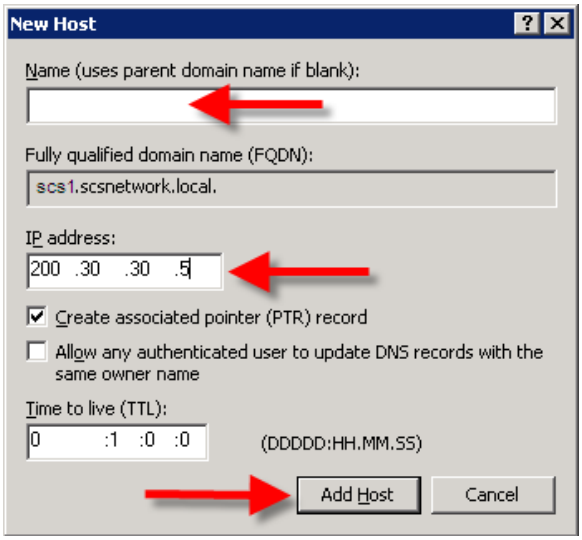
10. You now have two sub-domains, each containing its own ‘rr’ folder. These will be populated with SRV records relevant to each server.



11. Now create A Records for each server. Right-click on the first sub-domain and select **New Host (A)**.



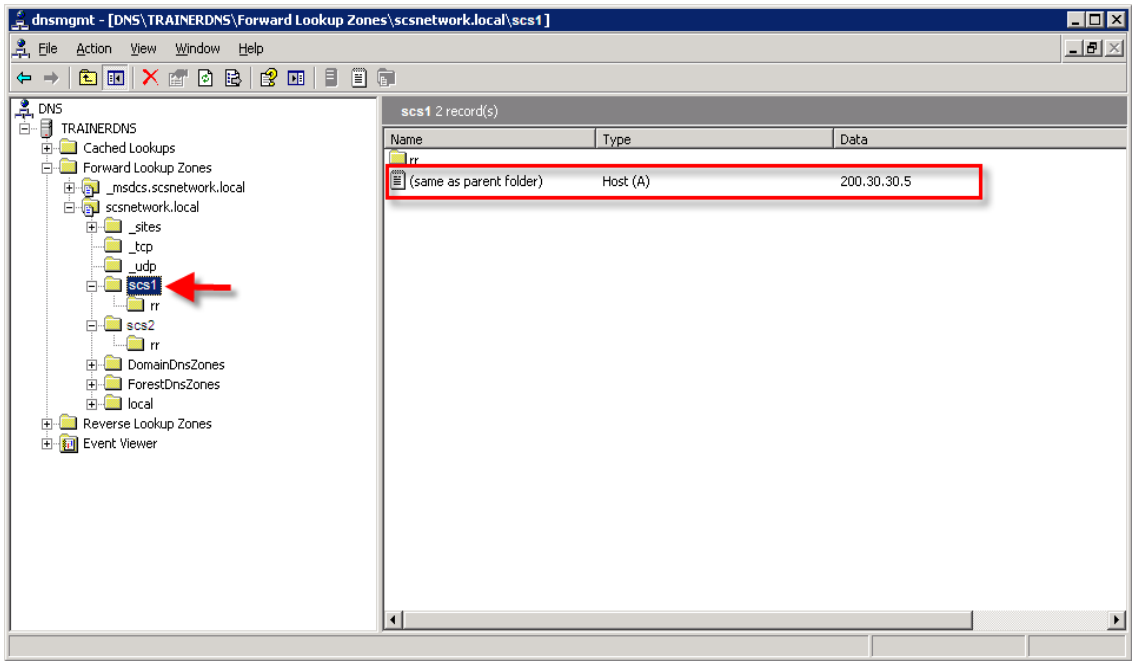
12. Leave the **Name** field blank. Enter the IP address of the primary server and then click **Add Host**.



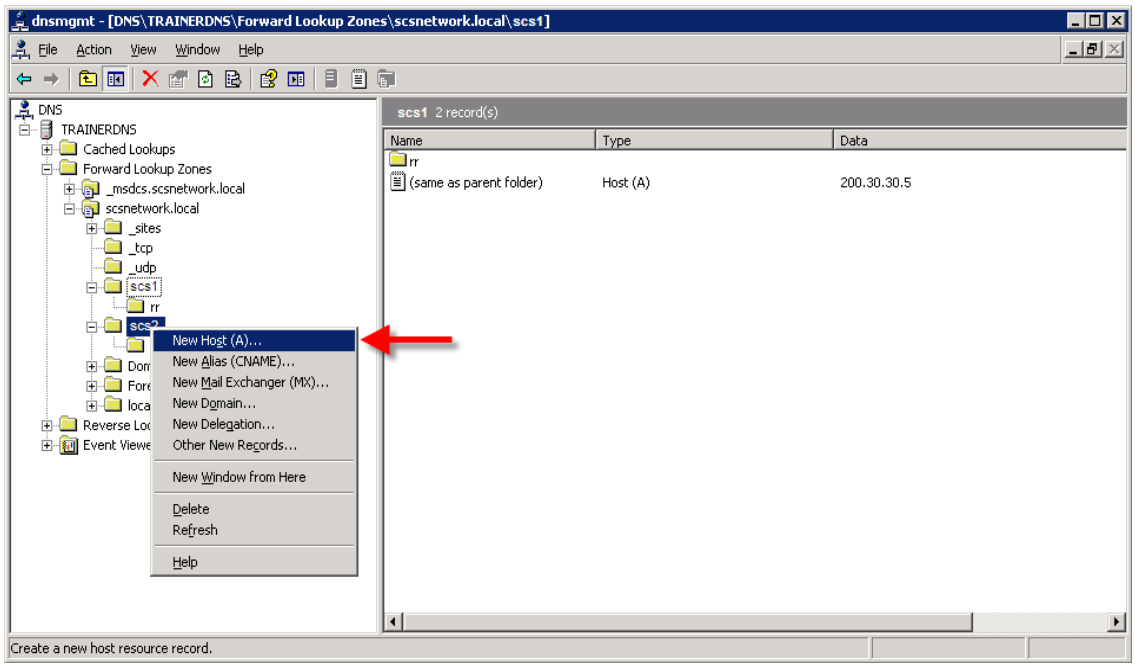
13. Click **OK** when the success message appears.

14. Click **Done**.

15. An A Record is now displayed in server 1's sub-domain.



16. Right-click on the second sub-domain and click on **New Host (A)**

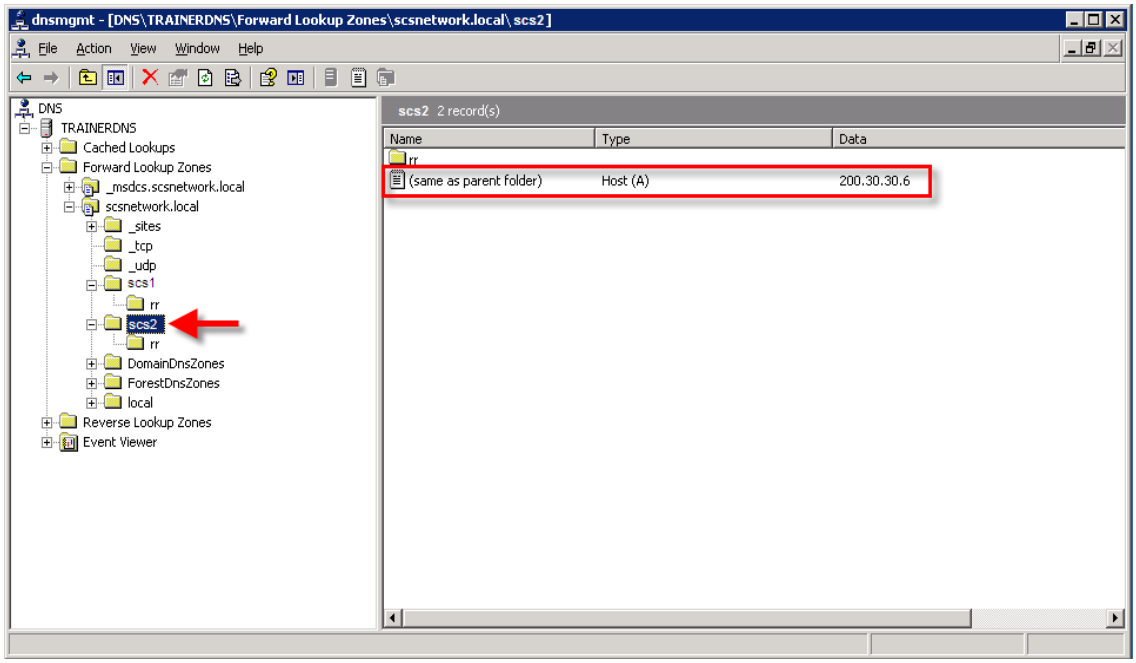


17. Leave the **Name** field blank and then enter the second server's IP address. Click **Add Host** to continue.

18. Click **OK** when the success message is displayed.

19. Click **Done** to complete record configuration.

20. The second server's sub-domain now contains an A Record.

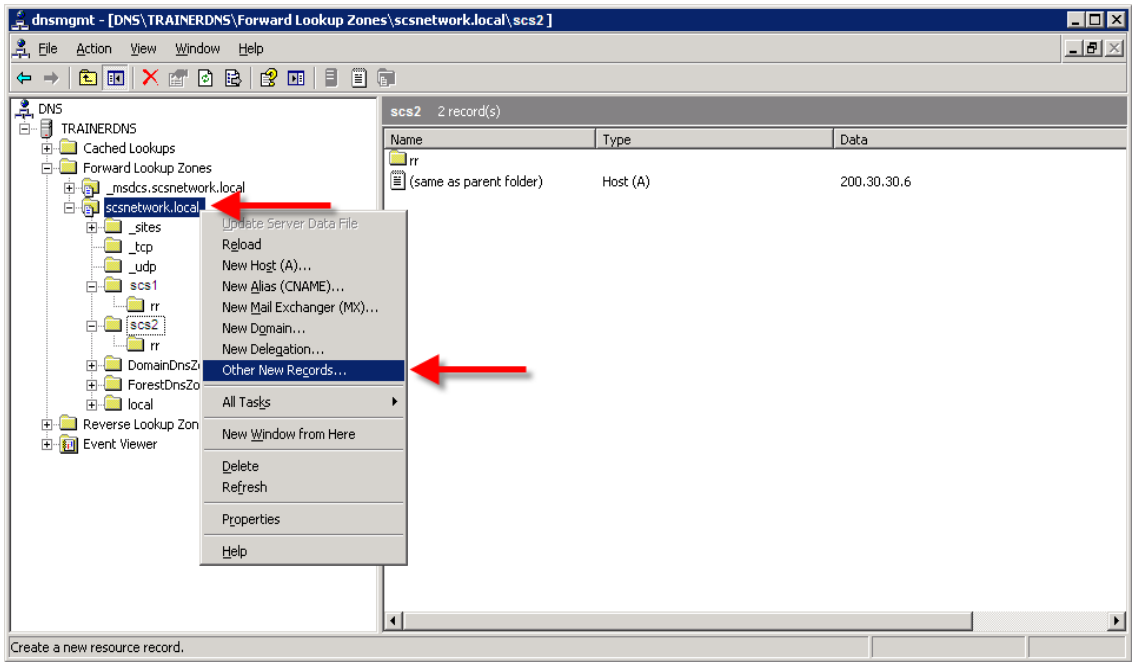


Creating SRV Records

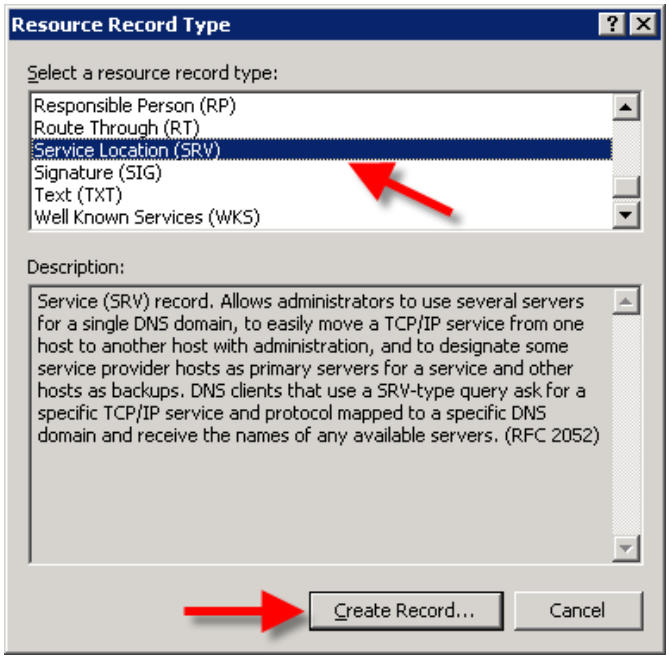
With A Records in place, you are now ready to begin creating SRV records:

Note: It is important that SRV values are entered exactly as listed for each record.

1. Right-click on the target domain and select **Other New Records**.

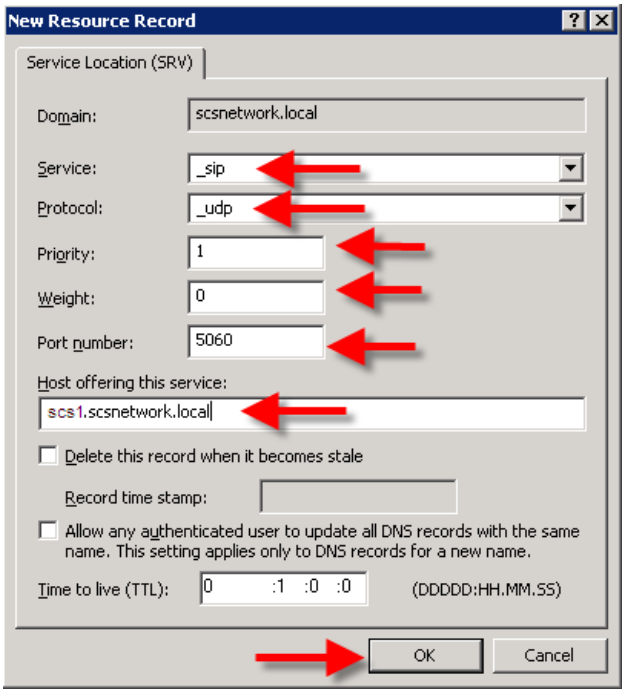


2. Scroll down the list of record types and select **Service Location (SRV)** and then click **Create Record**.



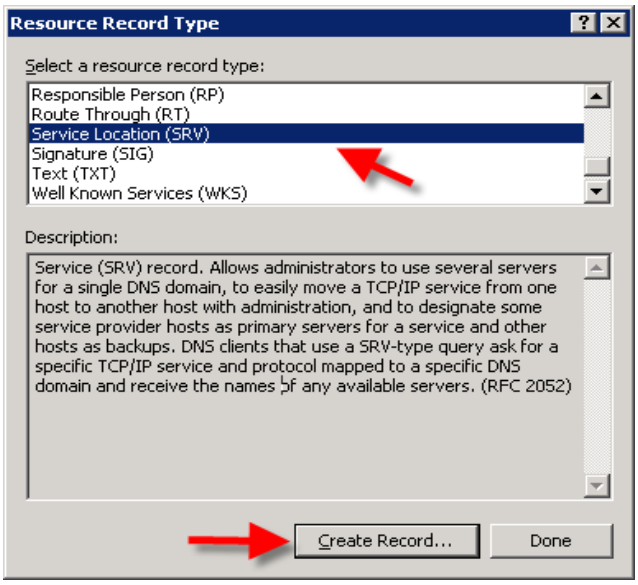
3. Create the first record with the following values:

Service	**_sip**
Protocol	_udp
Priority	1
Weight	0
Port number	5060
Host offering this service	*scsserver1.domain.com*



4. Click **OK**.

5. Select **Service Location (SRV)** and click **Create Record** again.

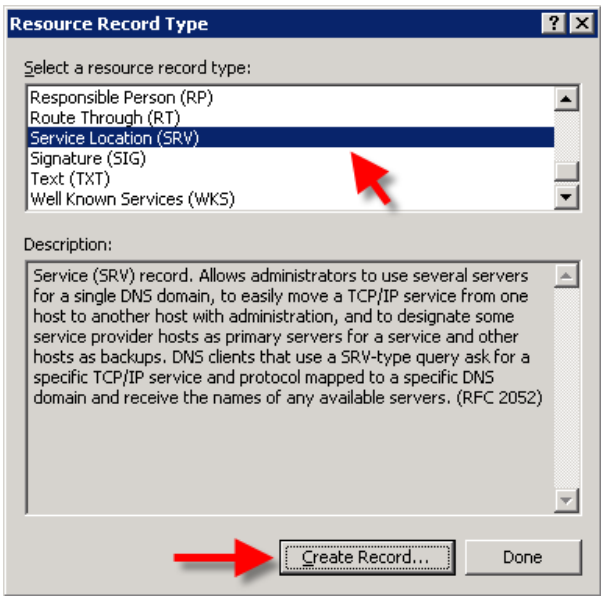


6. Create the next record with the following values:

Service	**_sip**
Protocol	_tcp
Priority	3
Weight	0
Port number	5060
Host offering this service	*scsserver1.domain.com*

7. Click **OK**.

8. Highlight **Service Location (SRV)** and click on **Create New Record**.

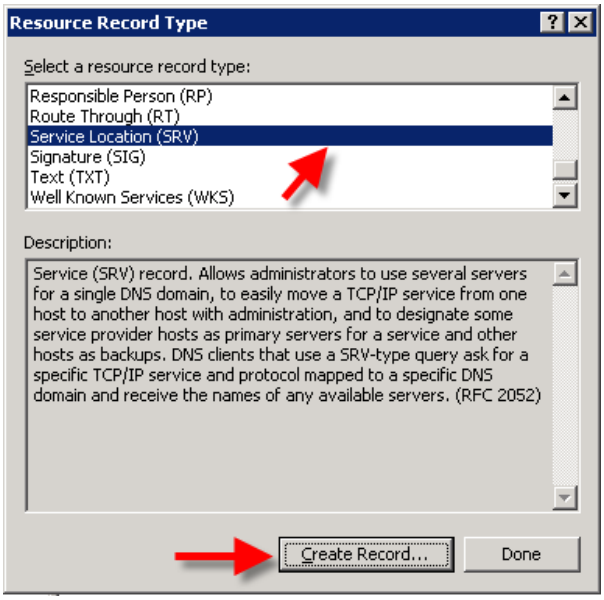


9. Enter the following values for the SRV record:

Service	**_sip**
Protocol	_udp
Priority	2
Weight	0
Port number	5060
Host offering this service	*scsserver2.domain.com*

10. Click **OK**.

11. Select **Service Location (SRV)** and click **Create Record**.

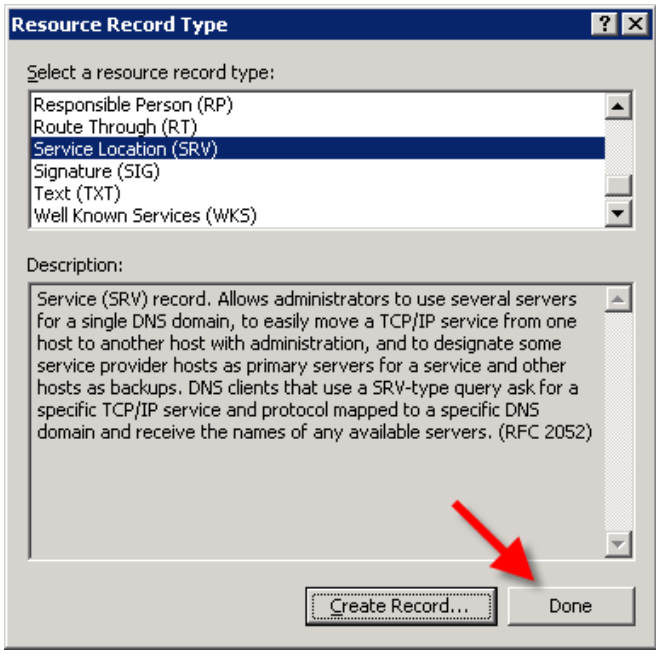


12. Enter the following values for the SRV record:

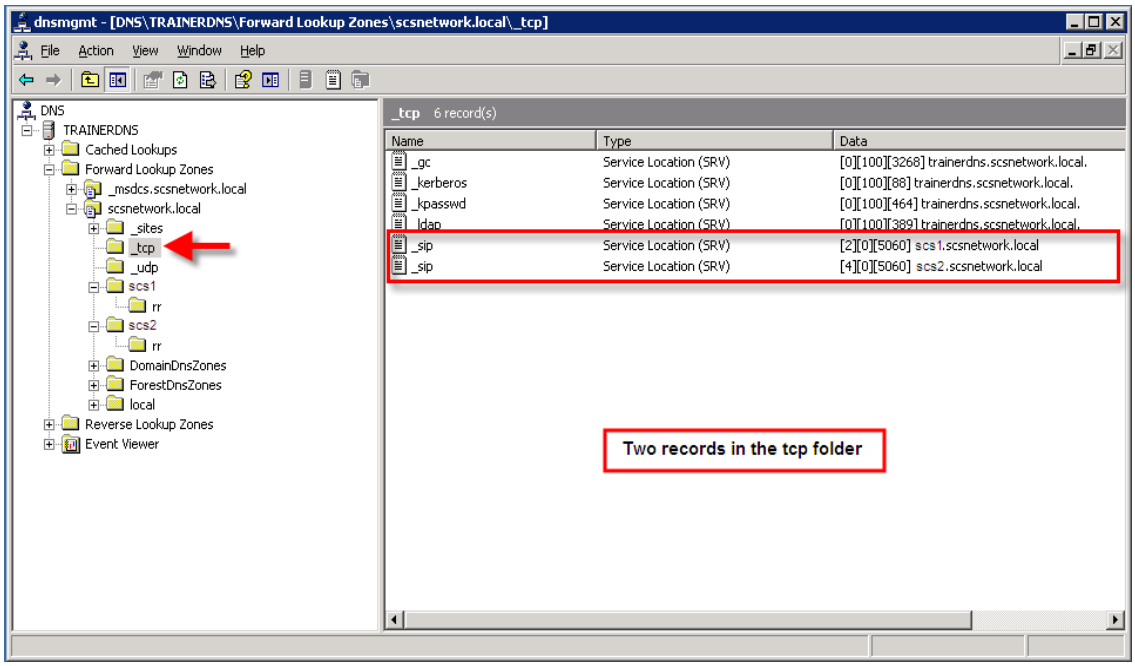
Service	**_sip**
Protocol	_tcp
Priority	4
Weight	0
Port number	5060
Host offering this service	*scsserver2.domain.com*

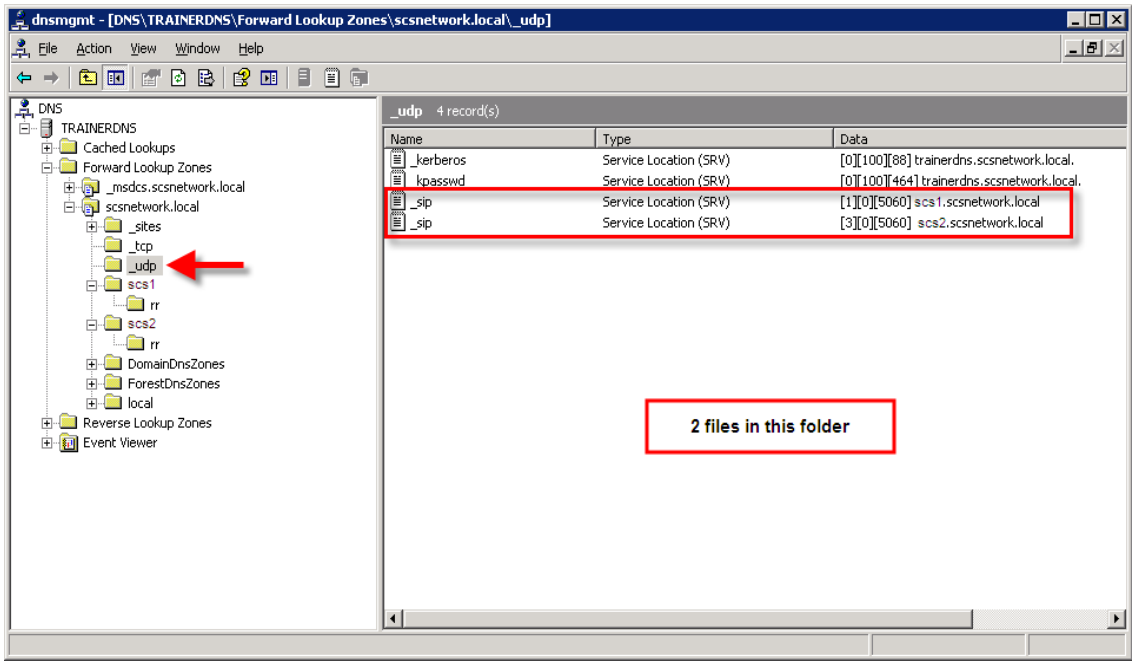
13. Click **OK**.

14. Click **Done**.



15. You should now have 2 SRV records in the **_tcp** folder and 2 SRV records in the **_udp** folder.



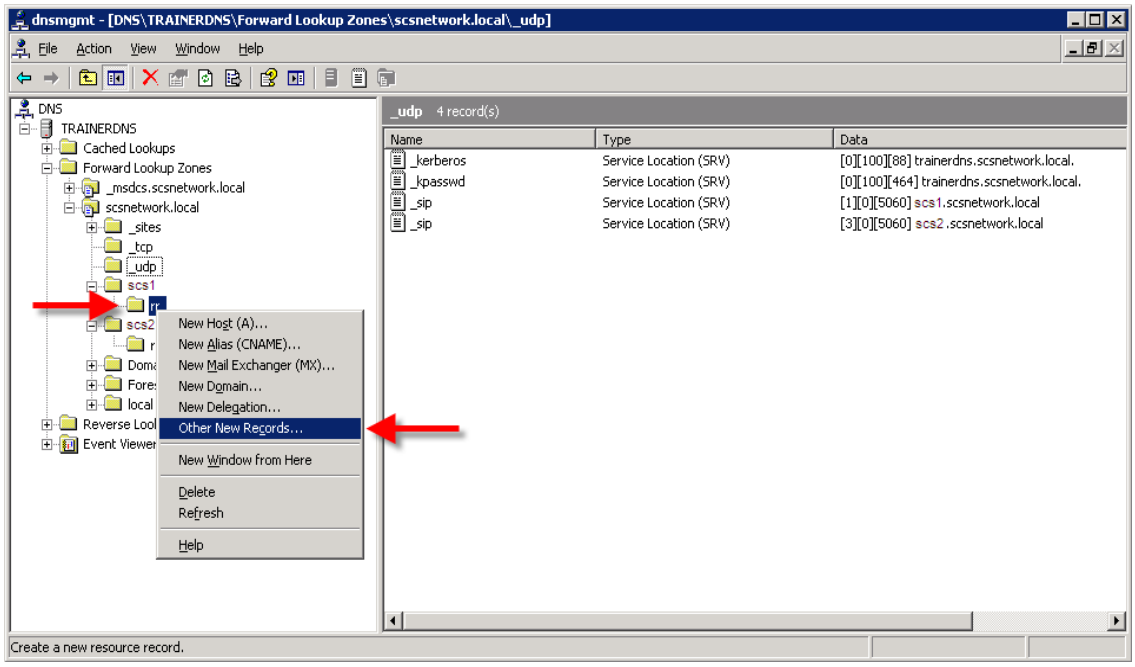


Creating Redirect SRV Records

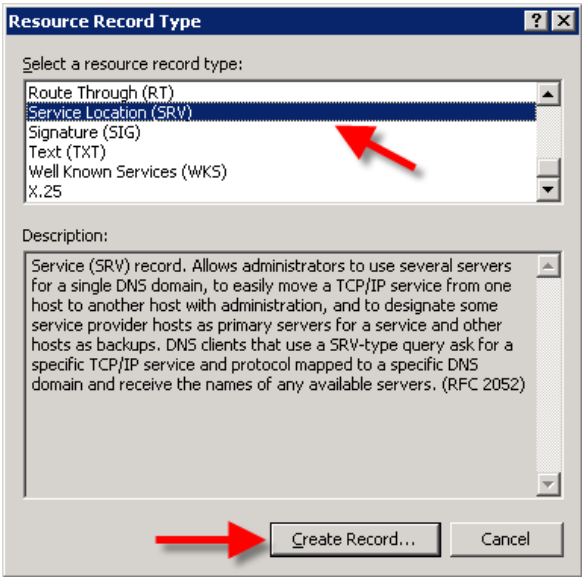
You now need to create a series of records that prioritise the flow of traffic in the event that redirection occurs. These records will be created in the sub-domains you created earlier, specifically in the '**rr**' folders attached to each sub-domain.

Note: It is important that SRV values are entered exactly as listed for each record.

1. Right-click on the '**rr**' folder of your primary server and select **Other New Records**. In this example *scs1* is my primary server, I have therefore selected *scs1/rr*.

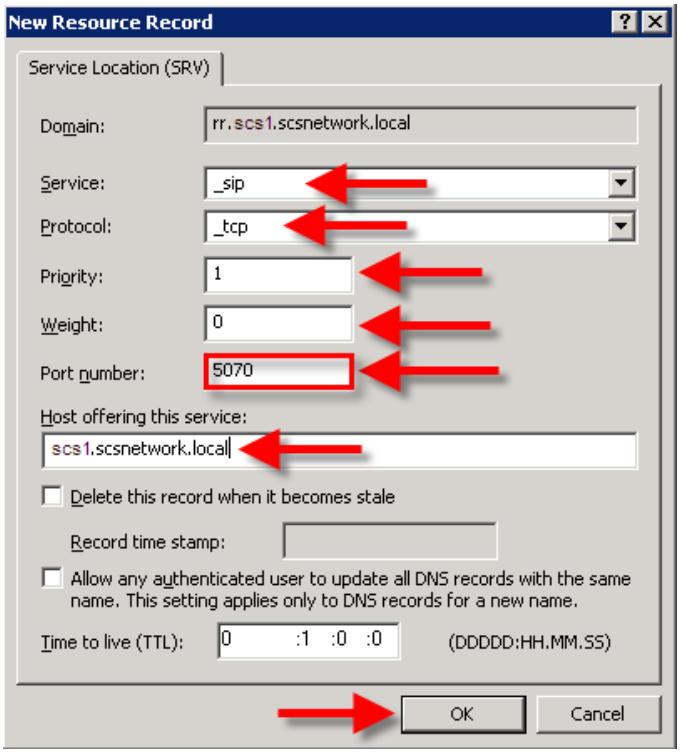


2. Select **Service Location (SRV)** and then click **Create Record**.



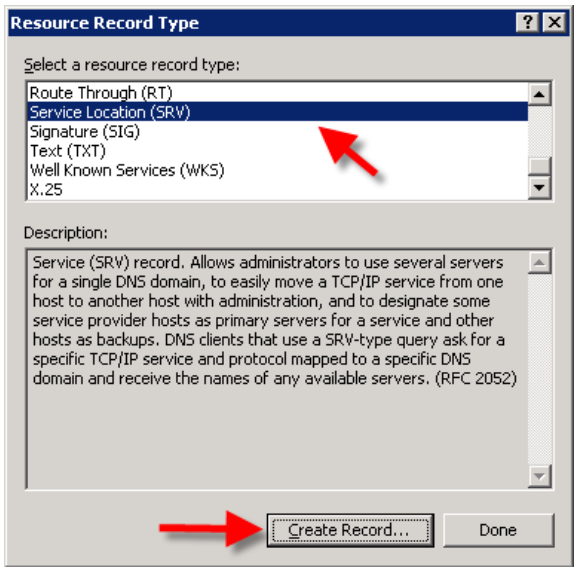
3. Create your first redirect SRV record with the following records (pay attention to the fact that the port number has changed to 5070 now):

Service	**_sip**
Protocol	_tcp
Priority	1
Weight	0
Port number	5070
Host offering this service	*scsserver1.domain.com*



4. Click **OK**

5. Click on **Service Location (SRV)** and then click **Create Record**.

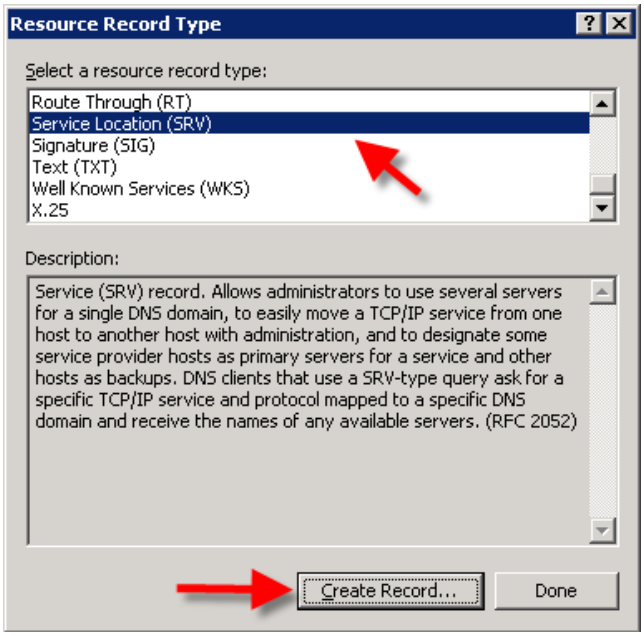


6. Enter the following values for the SRV record:

Service	**_sip**
Protocol	_udp
Priority	3
Weight	0
Port number	5070
Host offering this service	*scsserver1.domain.com*

7. Click **OK**.

8. Click on **Service Location (SRV)** and then click **Create Record**.

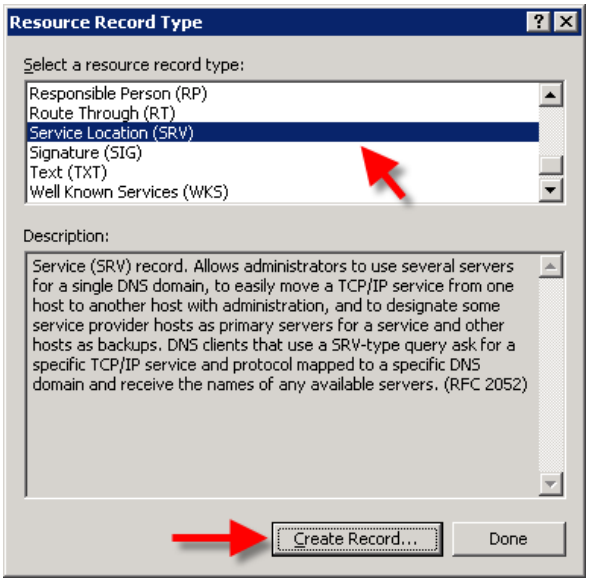


9. Enter the following SRV record values:

Service	**_sip**
Protocol	_tcp
Priority	2
Weight	100
Port number	5070
Host offering this service	*scsserver2.domain.com*

10. Click **OK**.

11. Select **Service Location (SRV)** and then click **Create Record**.

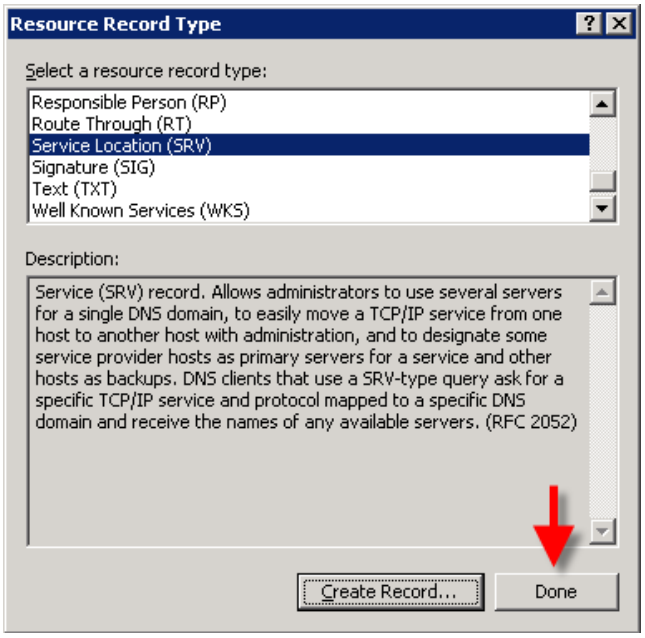


12. Enter the following values:

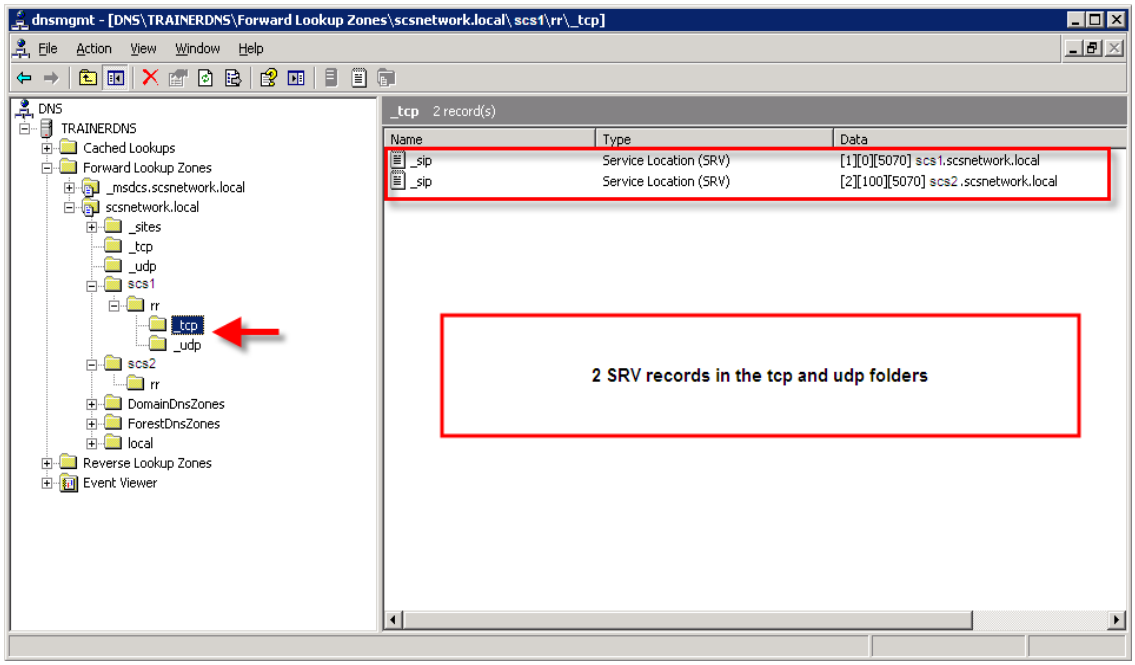
Service	**_sip**
Protocol	_udp
Priority	4
Weight	100
Port number	5070
Host offering this service	*scserver2.domain.com*

13. Click **OK**.

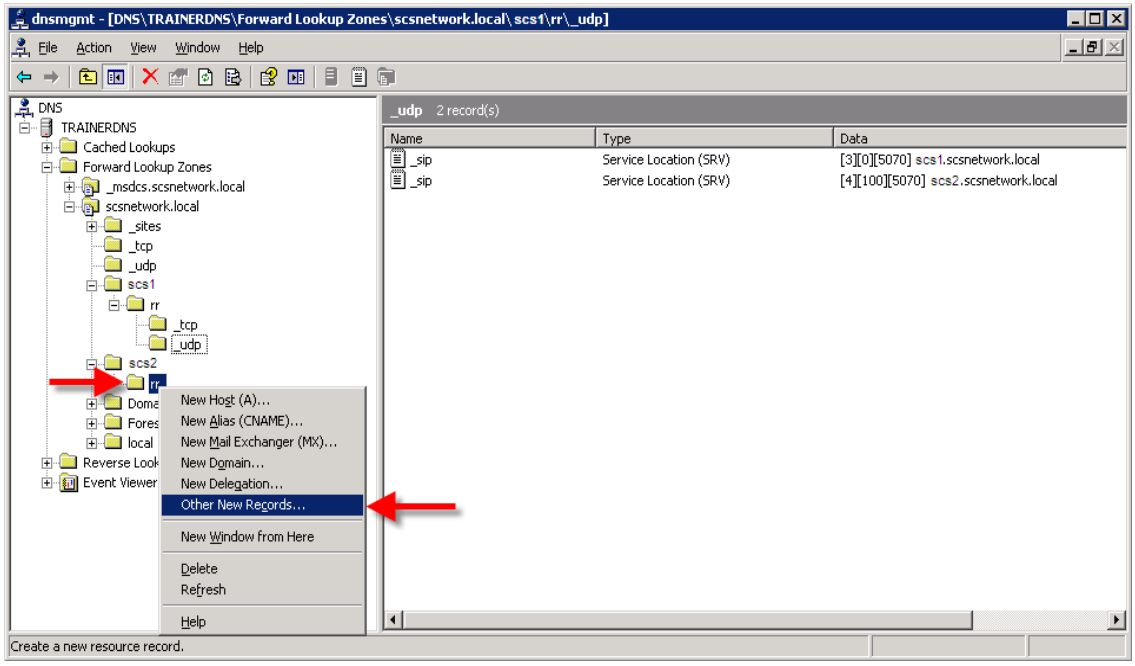
14. Click **Done**



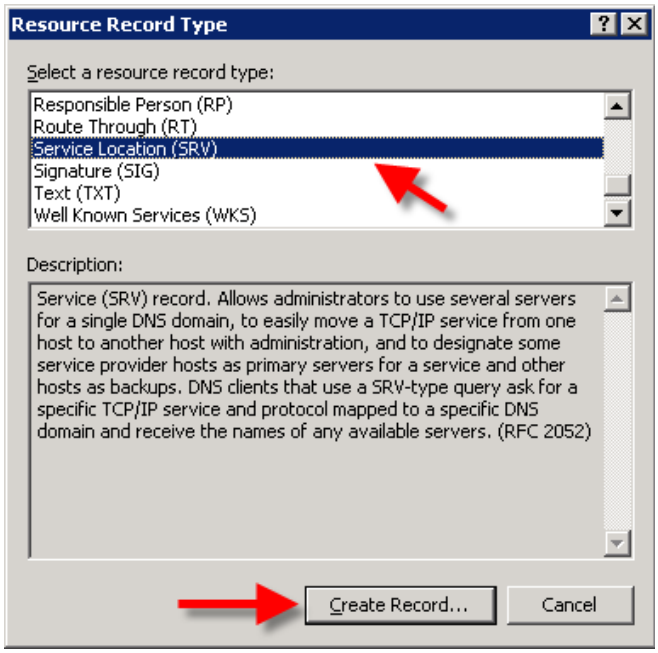
15. You should now have a **_tcp** and **_udp** folder within the '**rr'** folder of your primary server. Both folders should contain 2 records each.



16. Now configure redirect SRV records for the secondary server. Right-click on the '**rr**' folder in the secondary server sub-domain and select **Other New Records**.



17. Scroll down the list of record types and select **Service Location (SRV)** and click on **Create Record**.

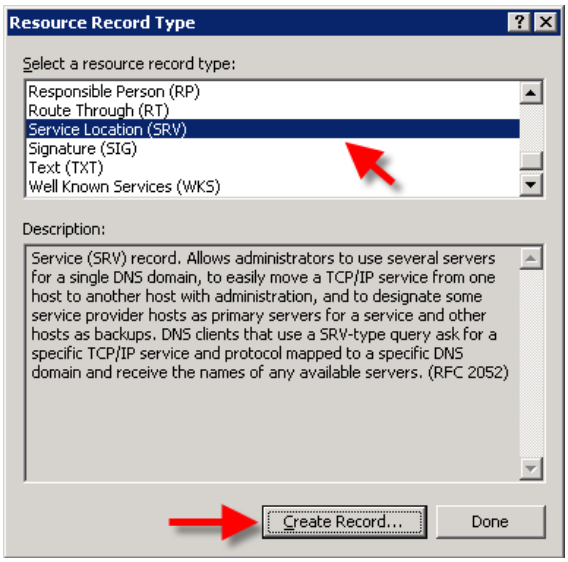


18. Enter the following values for the SRV record:

Service	**_sip**
Protocol	_tcp
Priority	1
Weight	0
Port number	5070
Host offering this service	*scsserver2.domain.com*

19. Click **OK**.

20. Select **Service Location (SRV)** and click **Create Record** to create the next record.

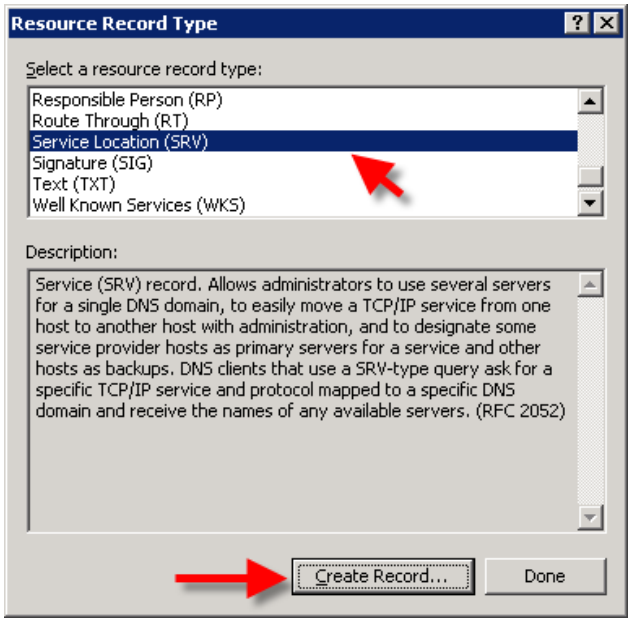


21. Enter the following values:

Service	**_sip**
Protocol	_udp
Priority	3
Weight	0
Port number	5070
Host offering this service	*scsserver2.domain.com*

22. Click **OK**.

23. Highlight **Service Location (SRV)** and then click **Create Record**.

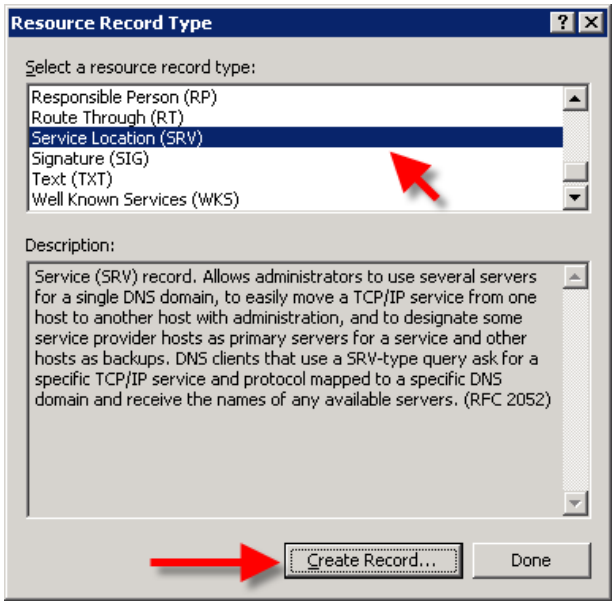


24. Enter the following values:

Service	**_sip**
Protocol	_tcp
Priority	2
Weight	100
Port number	5070
Host offering this service	*scsserver1.domain.com*

25. Click **OK**.

26. Select **Service Location (SRV)** and click **Create Record**.

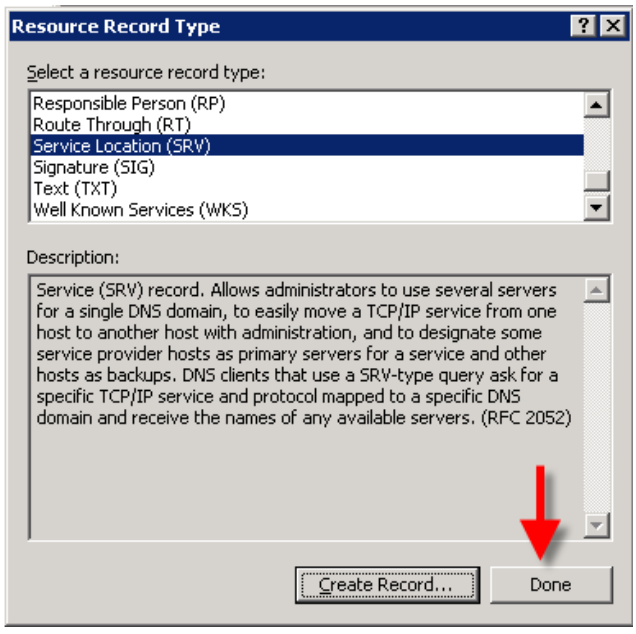


27. Enter the following values:

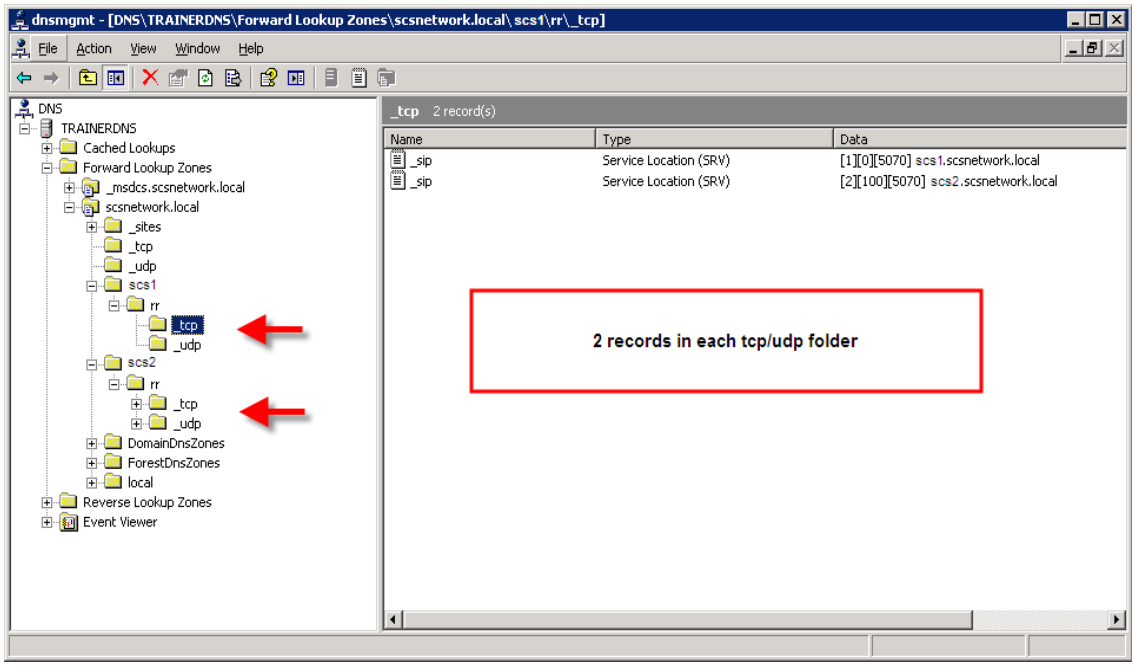
Service	**_sip**
Protocol	_udp
Priority	4
Weight	100
Port number	5070
Host offering this service	*scserver1domain.com*

28. Click **OK**.

29. Click **Done**.



30. You should now have two sub-domains containing **rr/tcp** and **rr/udp** folders. Each folder should contain two SRV records.

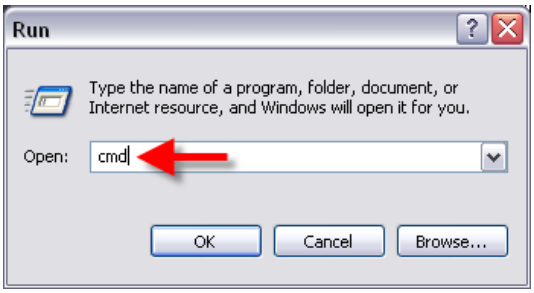


31. SRV record creation is complete.

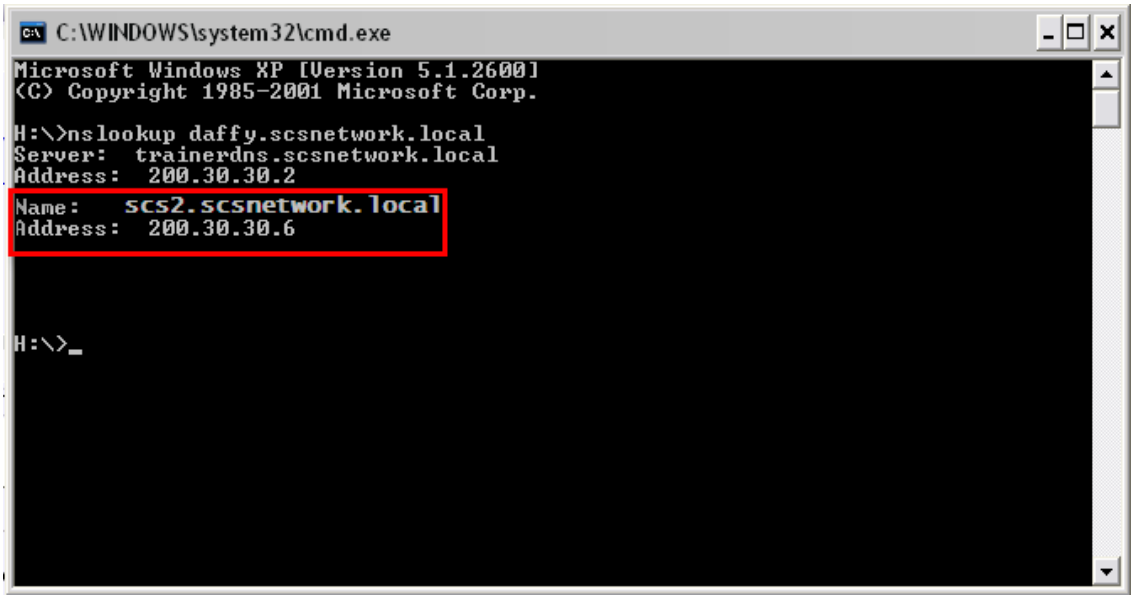
Testing DNS

You can run a simple test to determine whether DNS is working correctly:

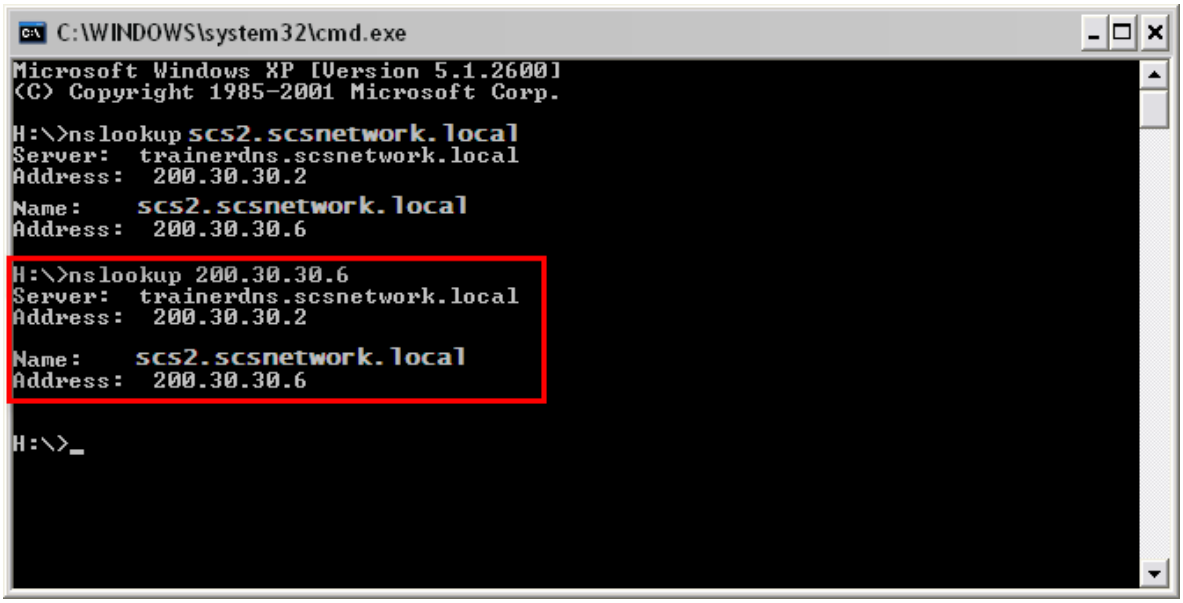
1. On a network connected PC, open the command prompt window by opening the **Start** menu and selecting **Run**.
2. In the box that opens, type **cmd** and press the **Enter** key.



3. At the prompt, type **`nslookup servername.serverdomain.com`** (enter the host name and domain name of your server) and press **Enter**.
4. If DNS is behaving properly the query should return the server's name and IP address.



5. To double-check that your records are functioning properly, run the command again, but this time lookup the IP address instead of the server name.

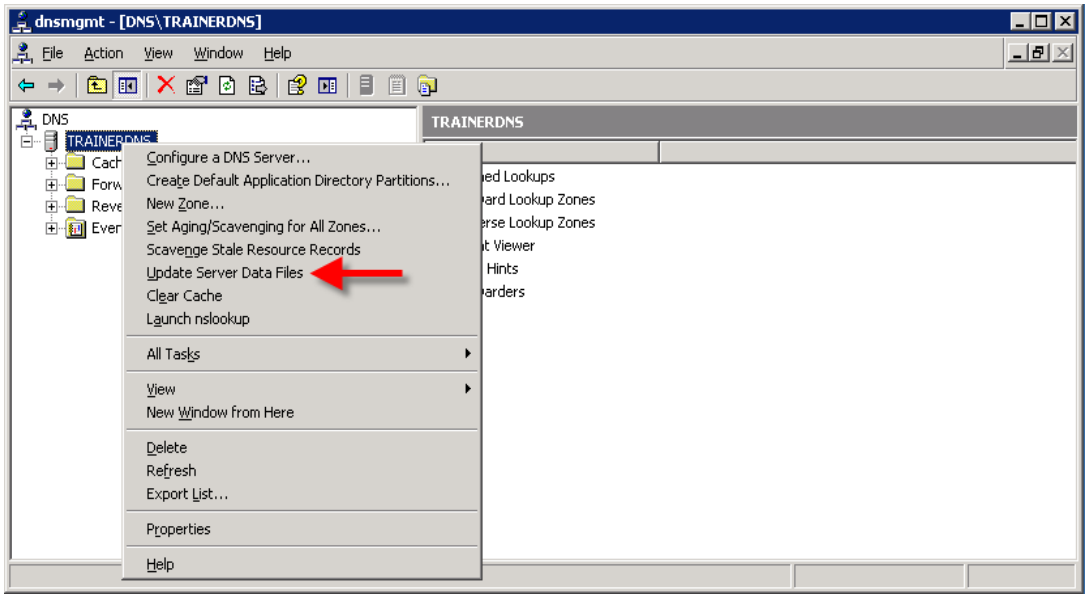


Concluding Setup

Once DNS is configured you can configure the SCS servers. If you configured the SCS servers before creating DNS entries you may need to update the DNS Data files and reboot the SCS servers.

Updating DNS Data Files

1. Right-click on the DNS server name and select **Update Server Data Files**.



Rebooting the SCS Server

If you configured LAN settings on the SCS server prior to creating DNS entries it is worth rebooting it to ensure that all services start properly. To reboot your SCS server (or servers):

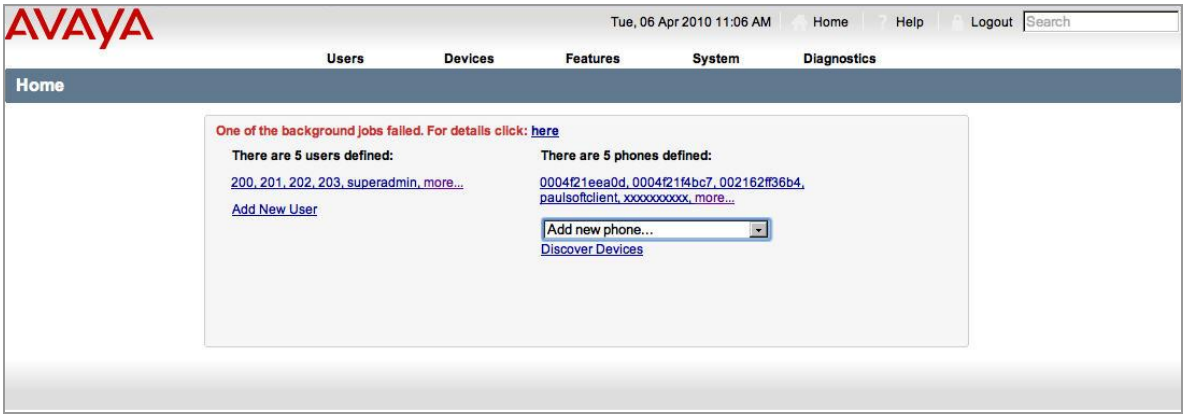
1. Log in to the server using the user name ‘root’ followed by the password you set during the configuration process.

2. At the prompt, type **`reboot`** and then press the **Enter** key.

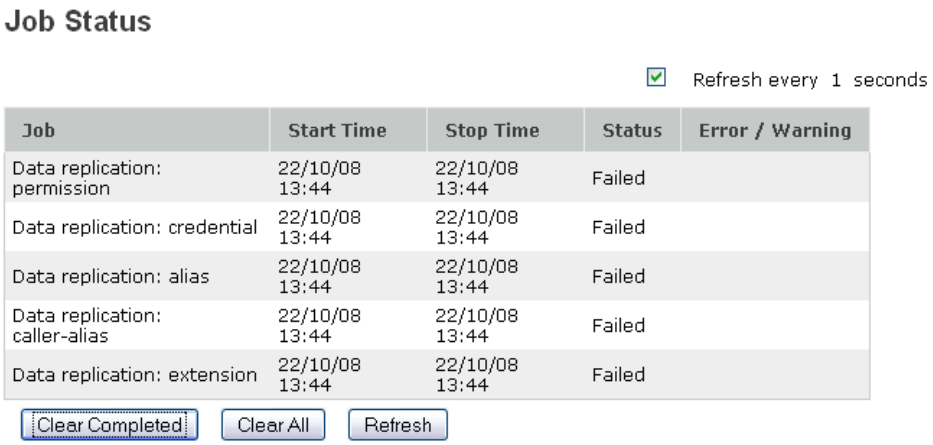
3. The server will reboot. Once reboot is complete the system will be ready for further configuration.

Data Replication Error

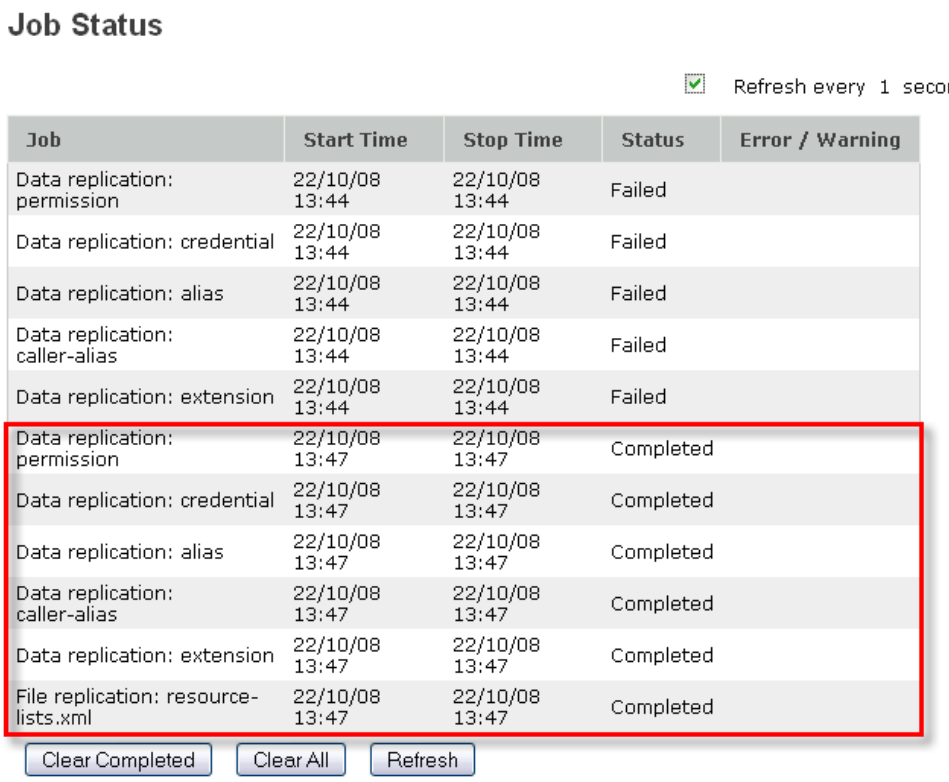
When you access the GUI for the first time after reboot, there is a good chance you will see the following message displayed on the screen:



This is perfectly normal and is usually caused by the fact that the secondary server boots up and connects later than the primary. If the primary attempts to replicate data to the secondary and the secondary is not ready then this error is produced in the **Job Status** screen (accessed from the **Diagnostics** menu):



Once the distributed server is connected to the network data replication should occur with no problems – often there is a delay in the time stamps between **Failed** messages and the **Completed** messages:



However, to clear the log and remove the red error message from the home screen you will have to click the **Clear All** button to restart the log.

Avaya Documentation Links

- SCS 4.0 Initial Installation
- SCS 4.0 Configuring the SCS with High Availability (HA)