



CompTIA Network+® Lab Series Network Concepts

Lab 9: Network Troubleshooting

Objective 1.7: Summarize DNS concepts and components
Objective 1.8: Given a scenario, implement network troubleshooting methodology
Objective 2.3: Explain the purpose and properties of DHCP
Objective 4.3: Given a scenario, use appropriate software tools to troubleshoot connectivity

Document Version: 2015-09-18



This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the [Creative Commons Attribution 3.0 Unported License](https://creativecommons.org/licenses/by/3.0/).

Development was funded by the Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48; The National Information Security, Geospatial Technologies Consortium (NISGTC) is an entity of Collin College of Texas, Bellevue College of Washington, Bunker Hill Community College of Massachusetts, Del Mar College of Texas, Moraine Valley Community College of Illinois, Rio Salado College of Arizona, and Salt Lake Community College of Utah.

This workforce solution was funded by a grant awarded by the U.S. Department of Labor's Employment and Training Administration. The solution was created by the grantee and does not necessarily reflect the official position of the U.S. Department of Labor. The Department of Labor makes no guarantees, warranties or assurances of any kind, express or implied, with respect to such information, including any information on linked sites, and including, but not limited to accuracy of the information or its completeness, timeliness, usefulness, adequacy, continued availability or ownership.

Contents

1	Troubleshoot a Suspected DNS Issue Using CLI Utilities.....	7
1.1	Using the Problem-Solving Process Troubleshoot a Suspected DNS Issue	7
1.2	Conclusion.....	11
1.3	Review Questions.....	11
2	Configure an Operational DHCP Scope of Addresses	12
2.1	Configure a DHCP Server Scope.....	12
2.2	Conclusion.....	23
2.3	Review Questions.....	23
3	Observe the Effects of a Deactivated Scope and Resolve the Configuration	24
3.1	Deactivate the DHCP Scope, Observe the Effects and Resolve the Problem	24
3.2	Conclusion.....	25
3.3	Review Questions.....	25



Introduction

This lab is part of a series of lab exercises designed to supplement coursework and provide students with a hands-on training experience based on real world applications. This series of lab exercises is intended to support courseware for CompTIA Network+® certification.

Networks are important to business processes and when they are not fully operational it is costly and frustrating to the users. Network administrators need to understand not just how to keep the network functional, but also how to approach troubleshooting problems when a network is not fully operational. This lab will review troubleshooting and a methodology that will provide ideas on where to start in the problem-solving effort. This methodology will be used as a guide in troubleshooting two protocols widely used in networks and it is important to be able to diagnose issues with them. DNS and DHCP will be the two protocols focused on in this exercise.

This lab includes the following tasks:

1. Using the Problem Solving Process Troubleshoot a Suspected DNS Issue using CLI utilities and Resolve the Issue
2. Configure an Operational DHCP Scope of Addresses
3. Observe the Effects of a Deactivated DHCP Scope and Resolve the Problem

Objective: Network Troubleshooting

Successful troubleshooting requires a logical and methodical process. The following are steps for troubleshooting and problem solving network problems as recommended by CompTIA. You should be familiar with these steps to demonstrate Network+ mastery:

- Identify the problem.
- Gather Information
- Consider Possible Causes
- Devise a Solution
- Implement the Solution
- Test the Solution
- Document the Solution

Key terms for this lab:

Domain Name Service (DNS) – the protocol used to resolve and map hostnames and domain names into IP addresses on the Internet. DNS uses UDP port 53 for initiating requests. Name servers, or DNS servers are servers that contain databases of associated names and IP addresses and provide this information to resolvers (hosts) on request.



Nslookup: a utility used to perform query testing of DNS servers and obtain detailed responses at the command prompt. This information can be useful for diagnosing and solving name resolution problems.

Dynamic Host Configuration Protocol (DHCP) – protocol used to automatically assign network configuration parameters to devices on a network. Parameters include IP address, subnet mask, default gateway, server addresses such as DNS, and lease time. DHCP uses port number 67 to communicate from client to server and port 68 from server to client.

DHCP Scope – the consecutive range of possible IP addresses that the DHCP server can lease to clients on a network or subnet. Scopes typically define a single physical subnet on your network to which DHCP services are offered. Scopes are the primary way for the DHCP server to manage distribution and assignment of IP addresses and any related configuration parameters to DHCP clients on the network.

Command Line Interface (CLI) – a text-based method of accessing the shell of an operating system. Usually CLI provides a more powerful, direct way of executing programs and utilities.

Universal Resource Locator (URL) – the named address of a resource on the Internet.

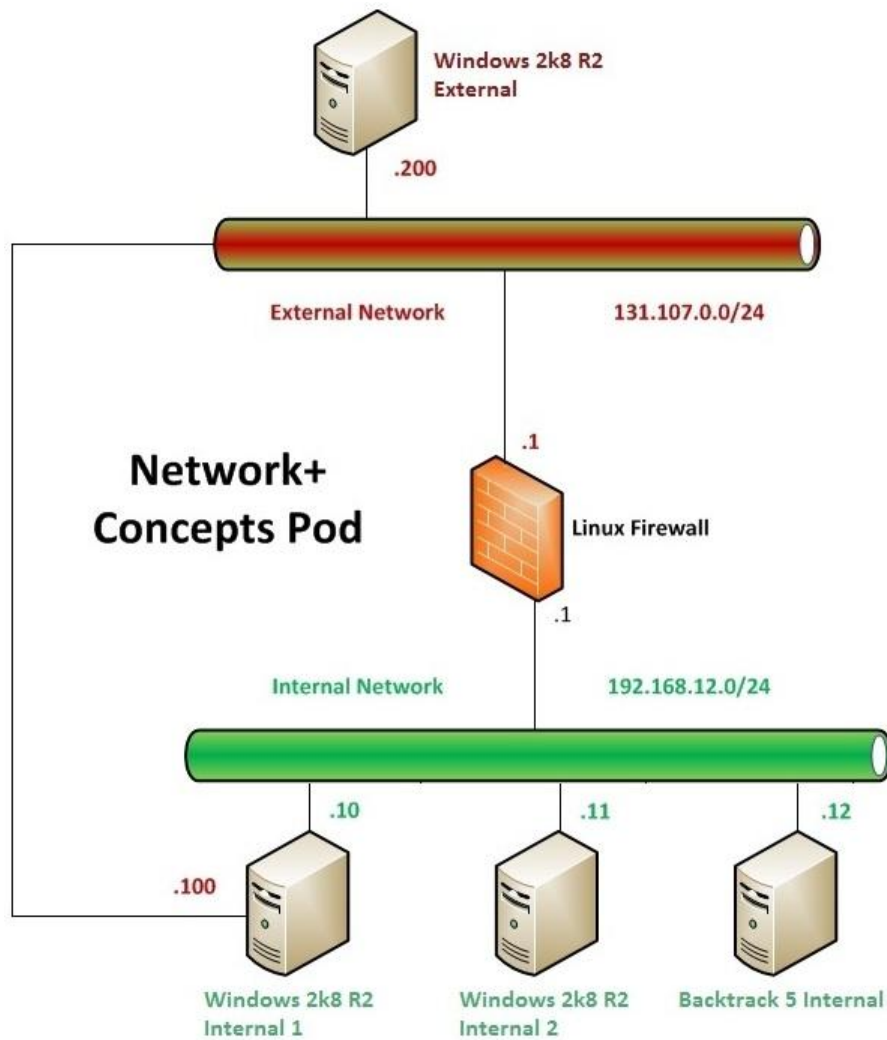
Fully Qualified Domain Name – the complete domain name for a specific computer, or host, on the Internet. The FQDN consists of two parts: the hostname and the domain name.

ipconfig – The ipconfig command is used to view or modify a computer's IP addresses, to release and then renew the IP address, and flush the DNS resolver cache.

Ping – used to verify basic TCP/IP connectivity to a network host.

APIPA (Automatic Private IP Addressing) – A Microsoft Windows feature used when there is a failure in DHCP servers, allowing DHCP clients to obtain IP addresses. APIPA allocates IP addresses in the private range 169.254.0.1 to 169.254.255.254 and are displayed in ipconfig /all as autoconfiguration IPv4 addresses. When the DHCP server is operational clients correctly update their addresses automatically.

Lab Topology



Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

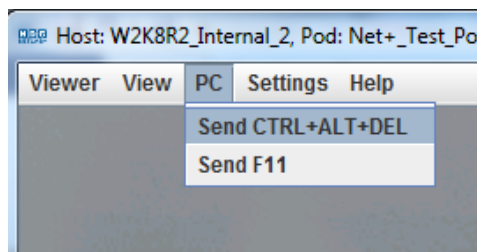
Required Virtual Machines and Applications

Log in to the following virtual machines before starting the tasks in this lab:

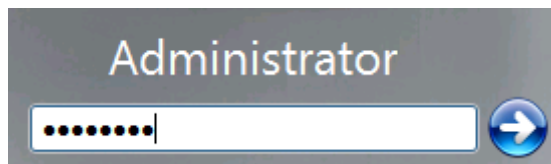
Windows 2k8 R2 Internal 1	192.168.12.10
Windows 2k8 R2 Internal 1 password	P@ssw0rd
Windows 2k8 R2 Internal 2	192.168.12.11
Windows 2k8 R2 Internal 2 Password	P@ssw0rd

Windows 2k8 R2 Login (applies to all Windows machines)

1. Click on the Windows 2k8 R2 icon on the topology that corresponds to the machine you wish to log into.
2. Use the PC menu in the NETLAB+ Remote PC Viewer to send a **Ctrl-Alt-Del** (version 2 viewer), or click the **Send Ctrl-Alt-Del** link in the bottom right corner of the viewer window (version 1 viewer).



3. In the password text box, type **P@ssw0rd** and press Enter to log in.



4. If the Initial Configuration Tasks and/or Server Manager windows appear, close them by clicking on the "X" in the top-right corner of the window.

1 Troubleshoot a Suspected DNS Issue Using CLI Utilities

Scenario: Users are complaining that the new company website at <http://www.ips.com> cannot be accessed. They were informed of the new website in a company memo. As a member of the IT support group you are tasked with troubleshooting and resolving the issue.

1.1 Using the Problem-Solving Process Troubleshoot a Suspected DNS Issue

Through your training, you know the first thing you need to do is isolate the problem. Based on your experience, this appears to be a DNS problem, but to be sure you will use a logical and methodical process of problem-solving to resolve the issue.

You begin gathering information by speaking with one of the users experiencing the access problem, asking the user questions and based on the information received you consider possible causes. Problems with network connectivity and DNS are two possibilities that you suspect as causes.

You remember that DNS is a protocol that is part of the TCP/IP suite of protocols. It is used to resolve the URL or website addresses that are readable to people into numerical IP addresses that are readable by computers. The DNS server keeps records of the addresses that are readable to people to IP address resolutions. The local computer will also build a cache of addresses that have been previously resolved by the DNS server. The user's computer accesses the correct DNS server by its configured TCP/IP settings. DNS is implemented in two software components; the DNS server and the DNS client. Your user's machine is the DNS client. Using utilities such as `ipconfig /all`, `ping`, and `nslookup`, you will troubleshoot to find a solution the problem. Once solved, you will implement the solution, document it, and explain the situation to the user.

You start the investigation by checking to see if there are any other network connectivity issues.

1. Use the instructions provided in the Lab Settings section to log onto the Windows 2k8 R2 Internal 1 machine, if you are not logged in already. If the Server Manager window appears, please close it.
2. Go to **Start > Search box** and type **cmd** and then press **Enter**.
3. Issue the **ping** command to the **loopback address 127.0.0.1** to verify the TCP socket on the local machine. It is successful.

- Issue the ping command to the host IP address to test the IP configurations of the local host (the user's computer). Refer to the table in the Lab Settings section to find the IP address of the Windows 2k8 R2 Internal 1 machine (192.168.12.10). It is successful.

```

Administrator: Command Prompt
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping 192.168.12.10

Pinging 192.168.12.10 with 32 bytes of data:
Reply from 192.168.12.10: bytes=32 time<1ms TTL=128
Reply from 192.168.12.10: bytes=32 time<1ms TTL=128
Reply from 192.168.12.10: bytes=32 time<1ms TTL=128
Reply from 192.168.12.10: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.12.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
  
```

The previous tests have helped to determine that the computer has its TCP/IP setting configured and the stack is functioning properly.

Next, the tests will determine that the TCP/IP setting on the host computer are correct in relation to the network it is configured for, particularly those settings that are used for DNS name resolution since that is one of the potential causes of the existing problem.

- At the command prompt, type **ipconfig /all**. This will display the full TCP/IP configuration for all NICs on the system, including DNS, DHCP, and WINS settings.

```

Administrator: C:\Windows\system32\cmd.exe

C:\Users\Administrator>ipconfig /all

Windows IP Configuration

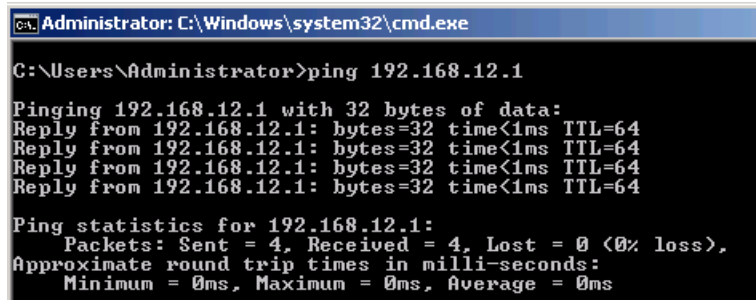
    Host Name . . . . . : W2K8R2Internal1
    Primary Dns Suffix . . . . . :
    Node Type . . . . . : Hybrid
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No
    DNS Suffix Search List. . . . . : netplus.com

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . : netplus.com
    Description . . . . . : Intel(R) PRO/1000 MT Network Connection
    Physical Address. . . . . : 00-50-56-90-29-A0
    DHCP Enabled. . . . . : No
    Autoconfiguration Enabled . . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::5501:2c24:fb0a:daa%11(Preferred)
    IPv4 Address. . . . . : 192.168.12.10(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.12.1
    DHCPv6 Iaid . . . . . : 234901590
    DHCPv6 Client DUID. . . . . : 00-01-00-01-18-D2-A7-35-00-50-56-9C-27-3B

    DNS Servers . . . . . : 192.168.12.10
    NetBIOS over Tcpip. . . . . : Enabled
  
```


6. Locate the **default gateway IP address** from the ipconfig /all output. **Ping the default gateway** to verify the router that takes you outside your local LAN is accessible. It is successful. This will help you narrow down what could be causing the original problem of not being able to access the new website at <http://www.ips.com> by eliminating lack of network connectivity.



```

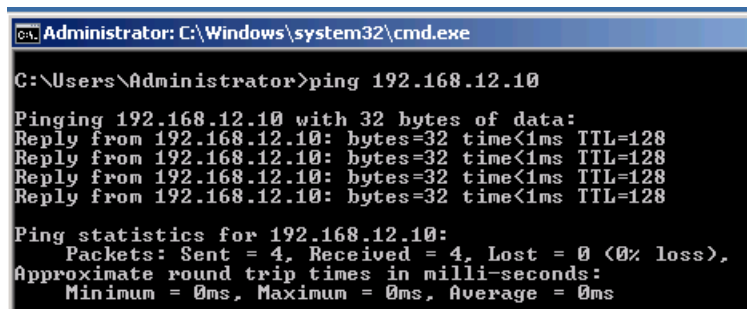
C:\Users\Administrator>ping 192.168.12.1

Pinging 192.168.12.1 with 32 bytes of data:
Reply from 192.168.12.1: bytes=32 time<1ms TTL=64
Reply from 192.168.12.1: bytes=32 time<1ms TTL=64
Reply from 192.168.12.1: bytes=32 time<1ms TTL=64
Reply from 192.168.12.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.12.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
  
```

You have eliminated loss of network connectivity within the LAN as the cause of the problem by proving connectivity to local hosts. Now it is time to test connectivity to the DNS server to be sure that the user's computer can access it.

7. Locate the **DNS server IP address** from the ipconfig /all output. At the command prompt, **ping the DNS server** to make sure it is accessible from the user's computer. It is successful. This proves that the DNS server is accessible, but that does not mean that DNS is functioning properly because you are still using an IP address in your testing.



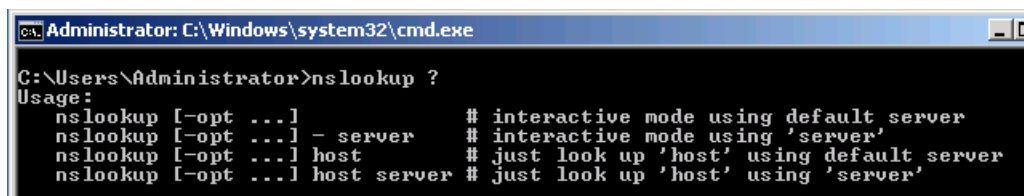
```

C:\Users\Administrator>ping 192.168.12.10

Pinging 192.168.12.10 with 32 bytes of data:
Reply from 192.168.12.10: bytes=32 time<1ms TTL=128
Reply from 192.168.12.10: bytes=32 time<1ms TTL=128
Reply from 192.168.12.10: bytes=32 time<1ms TTL=128
Reply from 192.168.12.10: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.12.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
  
```

8. At the command prompt, type **nslookup ?**. Nslookup is a command-line utility for testing and troubleshooting DNS servers. Nslookup ? shows available commands in the utility.



```

C:\Users\Administrator>nslookup ?

Usage:
  nslookup [-opt ...]           # interactive mode using default server
  nslookup [-opt ...] - server  # interactive mode using 'server'
  nslookup [-opt ...] host      # just look up 'host' using default server
  nslookup [-opt ...] host server # just look up 'host' using 'server'
  
```

9. Nslookup can be used to test DNS failures. At the command prompt, type **nslookup** followed by the **IP address of the user's computer**.

```

Administrator: Command Prompt
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>nslookup 192.168.12.11
Server: w2k8r2internal1.netplus.com
Address: 192.168.12.10

Name: w2k8r2internal12.netplus.com
Address: 192.168.12.11

```

Nslookup is useful in this situation because it has allowed you to verify that name resolution is working. The output has returned the name and IP address of the DNS server that resolved the name. It also shows you the fully qualified domain name and the IP address of the host you specified in the command that is that of the user's computer.

10. You have now determined that network connectivity is functional and DNS is working properly. Now, type **nslookup www.ips.com** to learn if the DNS server is resolving the name to an IP address. Based on your findings, it can be concluded that the URL provided may be incorrect.

```

Administrator: C:\Windows\system32\cmd.exe

C:\Users\Administrator>nslookup www.ips.com
Server: w2k8r2internal1.netplus.com
Address: 192.168.12.10

DNS request timed out.
timeout was 2 seconds.
DNS request timed out.
timeout was 2 seconds.
DNS request timed out.
timeout was 2 seconds.
DNS request timed out.
timeout was 2 seconds.
*** Request to w2k8r2internal1.netplus.com timed-out
C:\Users\Administrator>

```

11. By contacting the department that distributed the memo and checking the URL of the new website, you learn that the correct URL is <http://www.isp.com>. Type nslookup again with the correct URL to see that DNS is now resolving it.

```

Administrator: C:\Windows\system32\cmd.exe

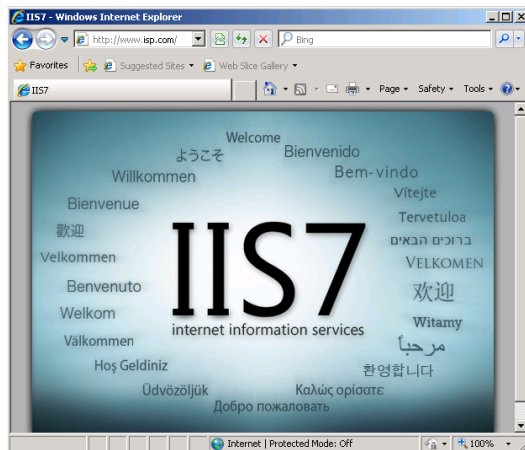
C:\Users\Administrator>nslookup www.isp.com
Server: w2k8r2internal1.netplus.com
Address: 192.168.12.10

Non-authoritative answer:
Name: w2k8r2external.isp.com
Address: 131.107.0.200
Aliases: www.isp.com

C:\Users\Administrator>

```

12. Open a web browser and try to access the new website using the corrected URL, <http://www.isp.com>. The website opens in the browser.



1.2 Conclusion

There are many useful CLI utilities that can be used for troubleshooting and problem solving on the network. Even with all the tools available, it is still important to work through solving problems using a logical and methodical process. A good starting point for troubleshooting is to identify the problem and gather information about what is wrong and who is affected. This makes it easier to come up with possible causes and work toward solutions of the problem.

1.3 Review Questions

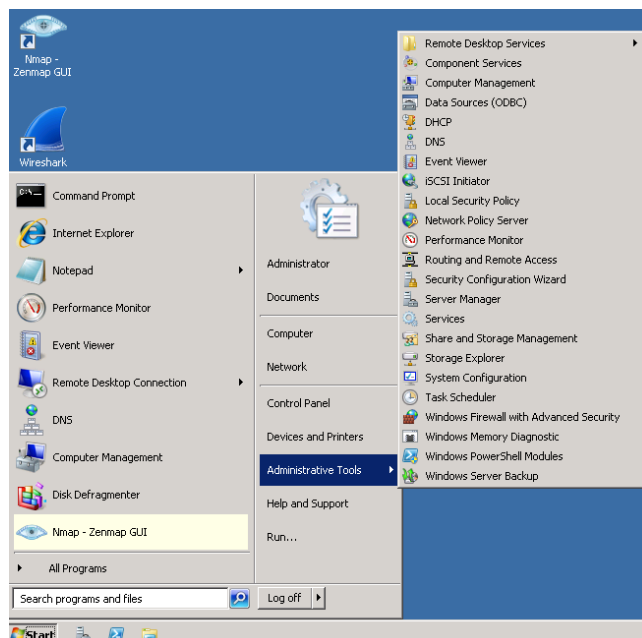
1. What does the *nslookup* command do?
2. What utility can be used to find out the IP address, subnet mask and default gateway configured on a computer?
3. What is the function of the DNS protocol?
4. If a client does not have the correct DNS server address specified in its TCP/IP properties, what will occur?

2 Configure an Operational DHCP Scope of Addresses

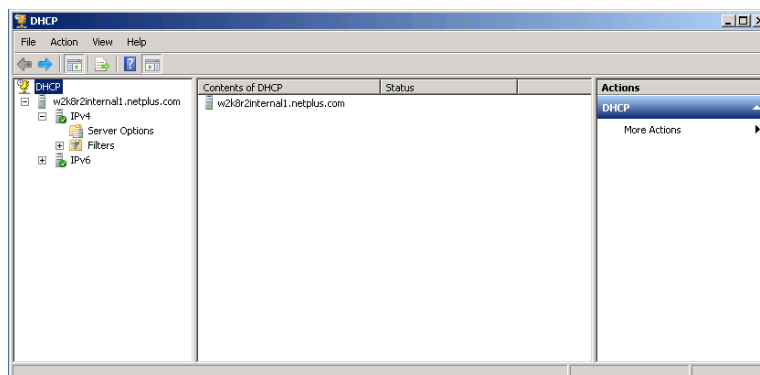
A DHCP server is used to automatically assign TCP/IP configuration parameters to devices on a network such as: IP address, subnet mask, default gateway, and server addresses such as DNS. The DHCP Scope is the consecutive range of IP addresses that the DHCP server can lease to clients on a network or subnet. In this task, you will configure DHCP on a server and test it to be sure the client is receiving the correct DHCP configurations.

2.1 Configure a DHCP Server Scope

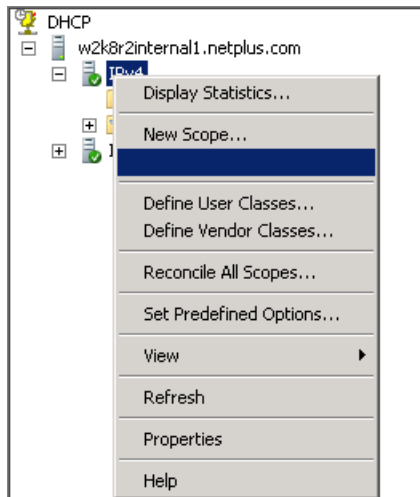
1. Use the instructions in the Lab Settings section to log into the Windows 2k8 R2 Internal 1 machine, if you are not logged in already.
2. Click **Start > Administrative Tools -> DHCP**



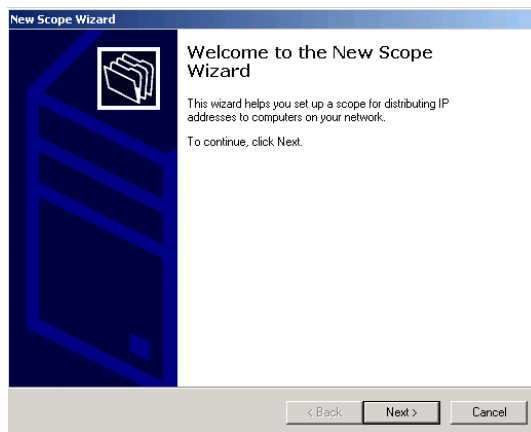
3. Click on the + next to the **w2k8r2internal1.netplus.com** machine to expand.



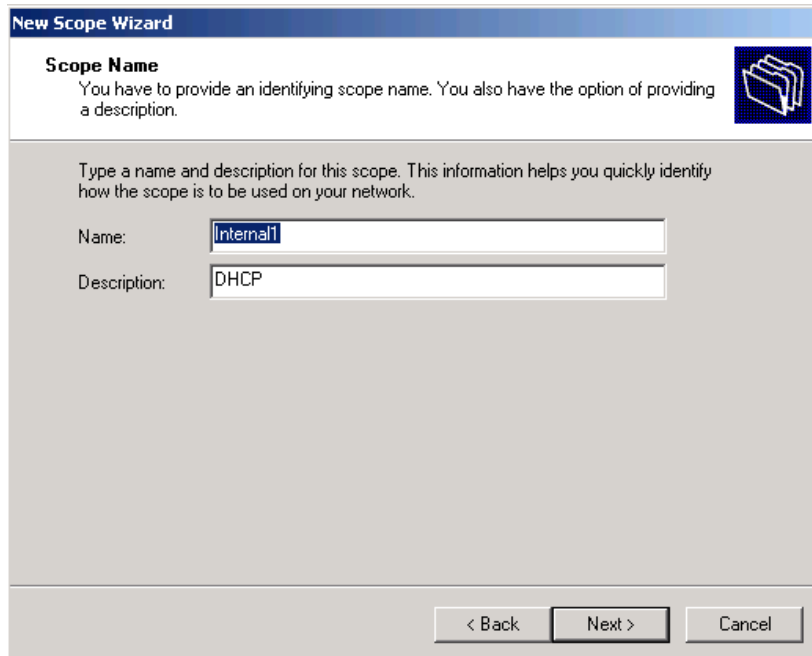
4. Right-click on **IPv4** and select **New Scope** from the shortcut menu.



5. The Welcome to the New Scope Wizard screen appears. Click **Next**.



6. On the **Scope Name** Wizard screen, type in the name, **Internal1** and a description, **DHCP**. These are just variables decided by the network administrator so a name or description would be selected according to the company conventions. Click **Next**.

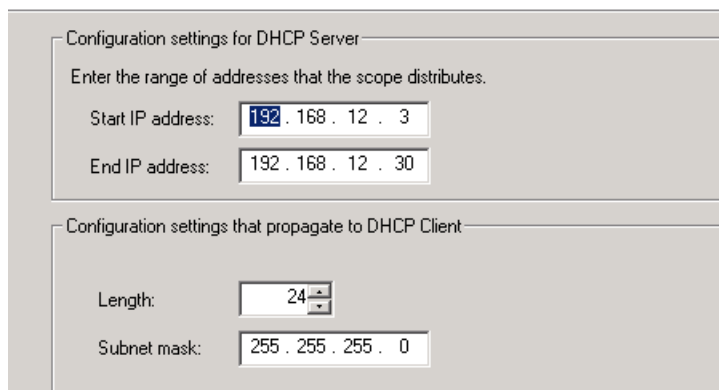


The screenshot shows the 'New Scope Wizard' window with the 'Scope Name' tab selected. The window title is 'New Scope Wizard'. Below the title bar, there's a section titled 'Scope Name' with a folder icon. The text says: 'You have to provide an identifying scope name. You also have the option of providing a description.' Below this, a larger text block says: 'Type a name and description for this scope. This information helps you quickly identify how the scope is to be used on your network.' There are two input fields: 'Name:' with the value 'Internal1' and 'Description:' with the value 'DHCP'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

7. On the IP Address Range Wizard screen, type the Start and End IP address. Use the start address, **192.168.12.3**, and the end address, **192.168.12.30**. These addresses need to be usable IP addresses within the same network/subnet as the host to which they will be assigned. You may also need to configure a length or subnet mask. The length and subnet mask are used to indicate the number of bits being used to identify the network portion of the host IP address. In this case, you will accept the default settings because that is the correct subnet for this scenario. Click **Next**.

IP Address Range

You define the scope address range by identifying a set of consecutive IP addresses.



The screenshot shows the 'IP Address Range' configuration window. It has two main sections. The first section is titled 'Configuration settings for DHCP Server' and contains the text 'Enter the range of addresses that the scope distributes.' Below this are two input fields: 'Start IP address:' with the value '192 . 168 . 12 . 3' and 'End IP address:' with the value '192 . 168 . 12 . 30'. The second section is titled 'Configuration settings that propagate to DHCP Client' and contains two input fields: 'Length:' with the value '24' and 'Subnet mask:' with the value '255 . 255 . 255 . 0'.

8. On the Add Exclusions and Delay Wizard screen, enter a valid start and end IP address. For this scope, the start IP address for excluding IP address from being dynamically assigned to hosts is **192.168.12.3** and the end address in the range is **192.168.12.14**. This range of addresses is selected to be left out of the scope because some of them are statically assigned to other devices on the network and since IP addresses need to be unique within a network excluding these from possibly being assigned again will prevent duplicate IP address problems on the network. Type the addresses into the wizard and be sure to click **Add** to save the settings. Leave the Subnet delay at the default setting. Click **Next**.

New Scope Wizard

Add Exclusions and Delay

Exclusions are addresses or a range of addresses that are not distributed by the server. A delay is the time duration by which the server will delay the transmission of a DHCP OFFER message.

Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only.

Start IP address: End IP address:

Excluded address range:

192.168.12.3 to 192.168.12.14

9. On the Lease Duration Wizard screen, accept defaults and click **Next**. DHCP allocates the IP address for specified periods of time known as a lease. The Lease duration specifies the time, in seconds, from address assignment until the client's lease on the address expires.

New Scope Wizard

Lease Duration

The lease duration specifies how long a client can use an IP address from this scope.

Lease durations should typically be equal to the average time the computer is connected to the same physical network. For mobile networks that consist mainly of portable computers or dial-up clients, shorter lease durations can be useful. Likewise, for a stable network that consists mainly of desktop computers at fixed locations, longer lease durations are more appropriate.

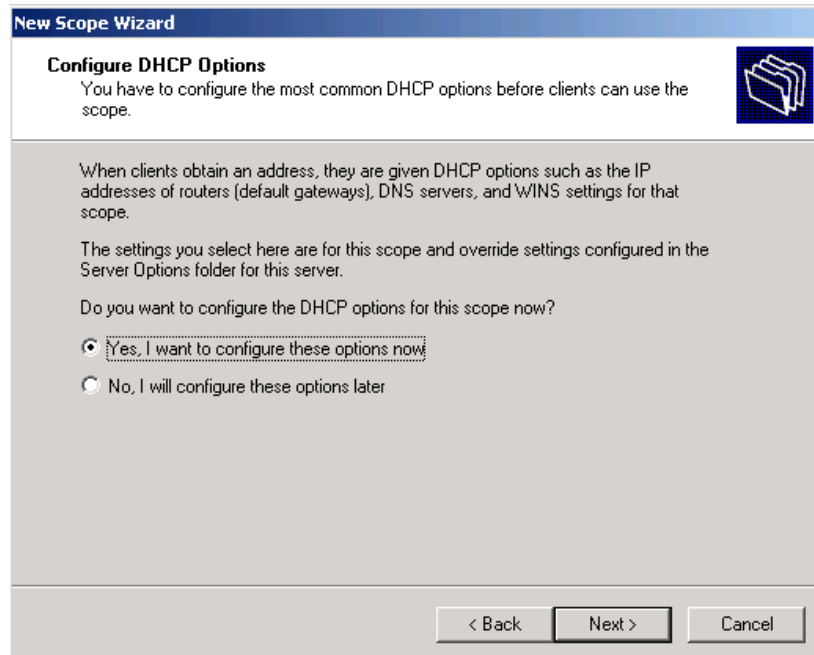
Set the duration for scope leases when distributed by this server.

Limited to:

Days: Hours: Minutes:

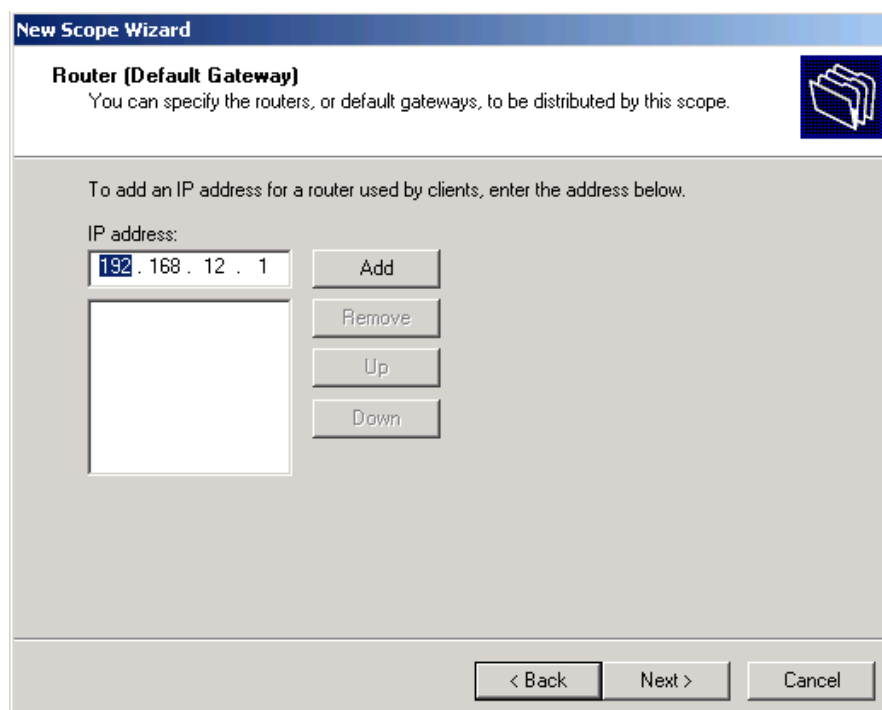
< Back Cancel

10. A host IP address, subnet mask, default gateway are the main options that need to be configured through DHCP. If a system is part of a domain or needs to connect to the Internet the domain name and DNS server options need to be configured. For Windows systems WINS can also be configured. On the Configure DHCP Options Wizard screen, click the **Yes** button and click **Next**.



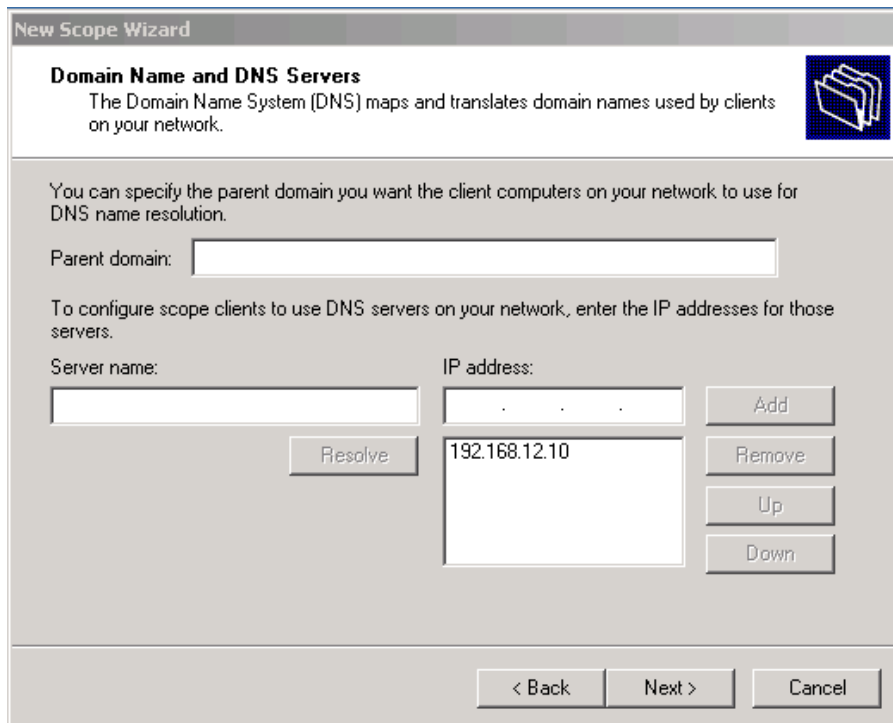
The screenshot shows the 'New Scope Wizard' window with the 'Configure DHCP Options' step. The title bar reads 'New Scope Wizard'. Below the title bar, the section is 'Configure DHCP Options' with a folder icon. The text says: 'You have to configure the most common DHCP options before clients can use the scope.' Below this, it explains: 'When clients obtain an address, they are given DHCP options such as the IP addresses of routers (default gateways), DNS servers, and WINS settings for that scope. The settings you select here are for this scope and override settings configured in the Server Options folder for this server.' Then it asks: 'Do you want to configure the DHCP options for this scope now?'. There are two radio buttons: 'Yes, I want to configure these options now' (which is selected) and 'No, I will configure these options later'. At the bottom right are three buttons: '< Back', 'Next >', and 'Cancel'.

11. On the Router (Default Gateway) Wizard screen, type in **192.168.12.1**, click **Add** and then click **Next**.



The screenshot shows the 'New Scope Wizard' window with the 'Router (Default Gateway)' step. The title bar reads 'New Scope Wizard'. Below the title bar, the section is 'Router (Default Gateway)' with a folder icon. The text says: 'You can specify the routers, or default gateways, to be distributed by this scope.' Below this, it says: 'To add an IP address for a router used by clients, enter the address below.' There is a text box labeled 'IP address:' containing '192.168.12.1'. To the right of the text box are four buttons: 'Add', 'Remove', 'Up', and 'Down'. Below the text box is an empty list box. At the bottom right are three buttons: '< Back', 'Next >', and 'Cancel'.

12. There is no domain to configure for this network. Notice the DNS server IP address has already been added to the options to be configured on the DHCP clients. On the Domain Name and DNS Servers Wizard screen, click **Next**.



New Scope Wizard

Domain Name and DNS Servers
The Domain Name System (DNS) maps and translates domain names used by clients on your network.

You can specify the parent domain you want the client computers on your network to use for DNS name resolution.

Parent domain:

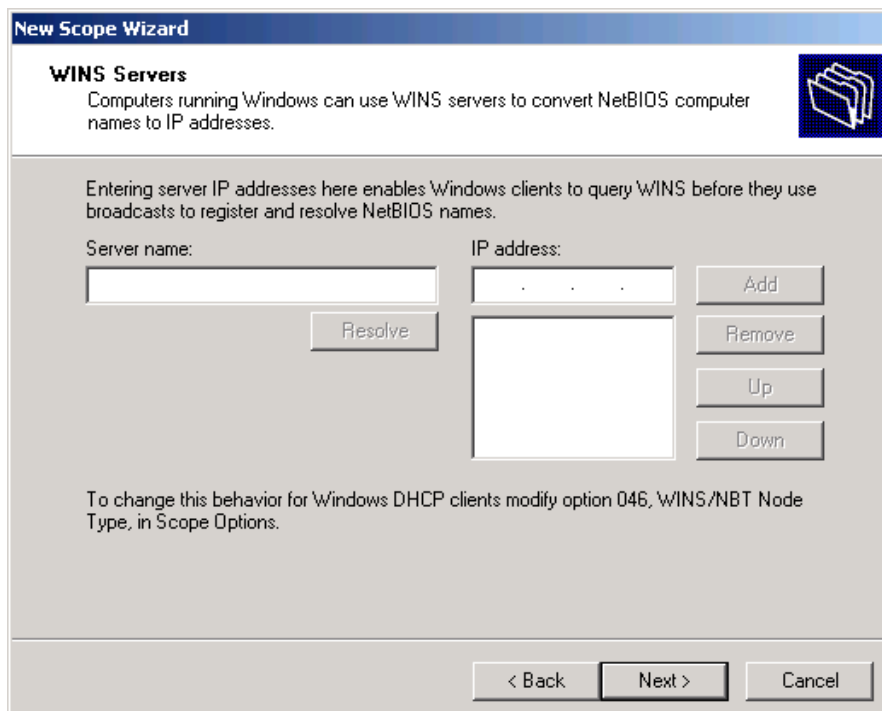
To configure scope clients to use DNS servers on your network, enter the IP addresses for those servers.

Server name:	IP address:	
<input type="text"/>	<input type="text"/>	Add
<input type="text"/>	192.168.12.10	Remove
		Up
		Down

Resolve

< Back Next > Cancel

13. You will not be configuring a WINS setting on this scope. On the WINS Servers Wizard Screen, click **Next**.



New Scope Wizard

WINS Servers
Computers running Windows can use WINS servers to convert NetBIOS computer names to IP addresses.

Entering server IP addresses here enables Windows clients to query WINS before they use broadcasts to register and resolve NetBIOS names.

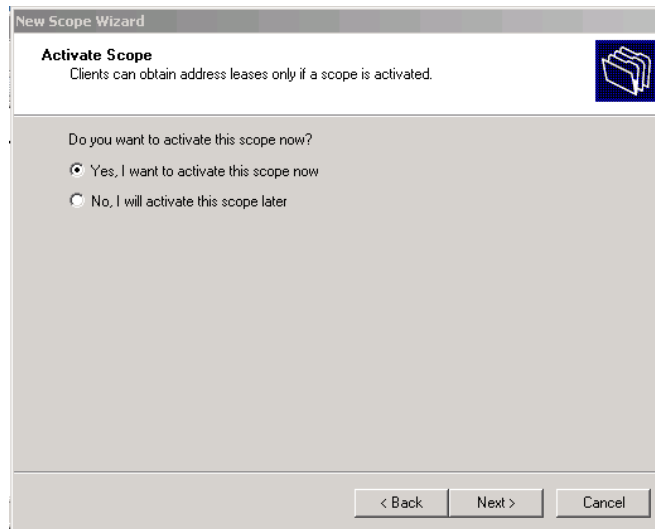
Server name:	IP address:	
<input type="text"/>	<input type="text"/>	Add
<input type="text"/>		Remove
		Up
		Down

Resolve

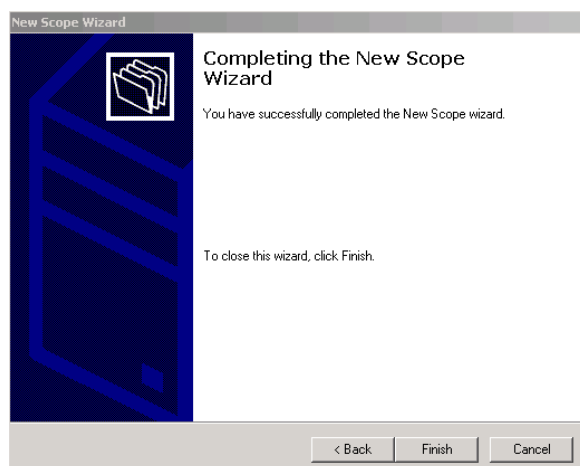
To change this behavior for Windows DHCP clients modify option 046, WINS/NBT Node Type, in Scope Options.

< Back Next > Cancel

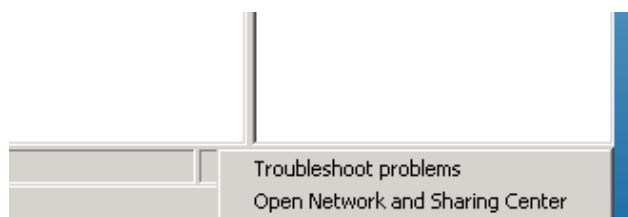
14. On the Activate Scope Wizard screen, click the **Yes** button and click **Next**.



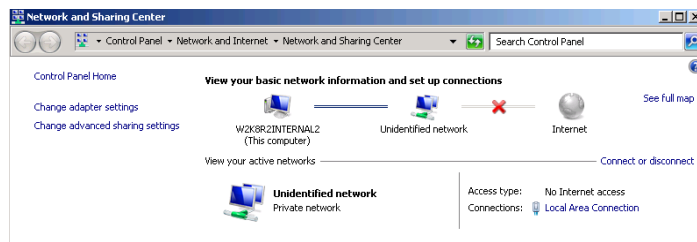
15. Click **Finish** to complete the New Scope Wizard.



16. Close the DHCP Dialog Box and all other open windows.
17. To test out the scope configuration, we will use the **Windows 2k8 R2 Internal 2** machine, enabling it as the DHCP client. Login to this machine following the steps outlined in the Lab Settings section, if you are not logged in already.
18. If the Server Manager window appears, please close it.
19. Open the **Network and Sharing Center** by right-clicking the network access icon on the bottom-right of the task bar and click **Open Network and Sharing Center**.



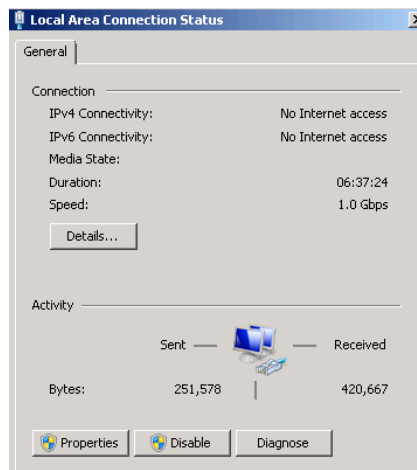
20. Click **Change adapter settings** in the left panel.



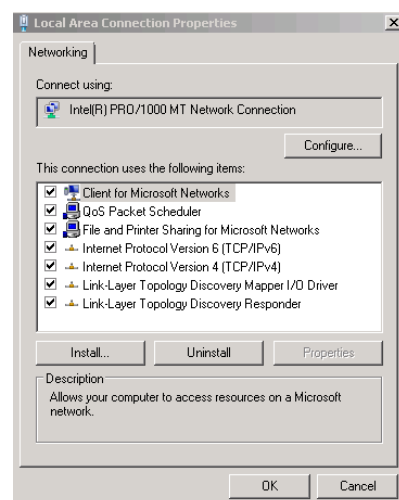
21. Double-click on the network card named **Local Area Connection**.



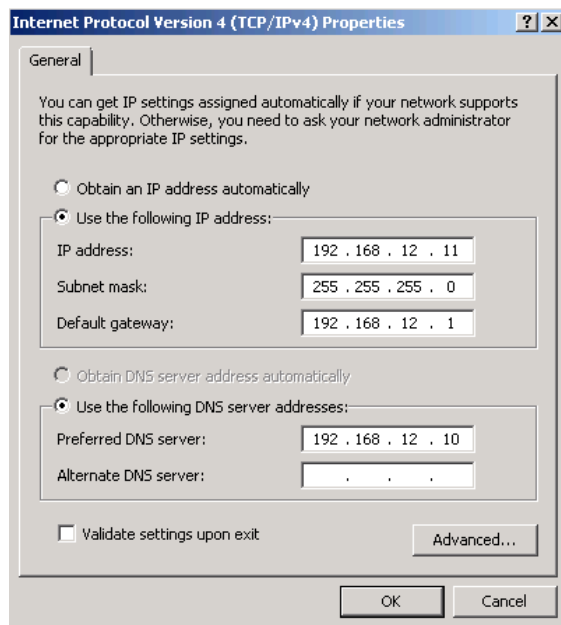
22. Click **Properties**.



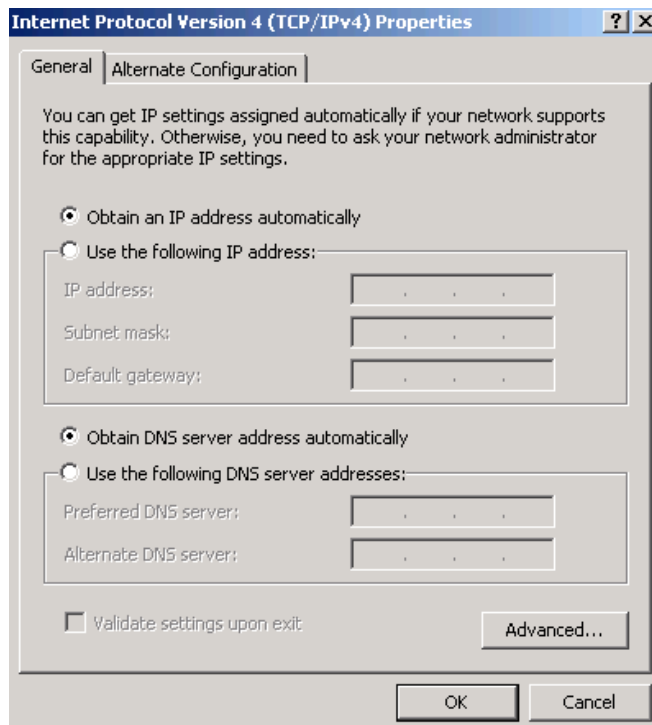
23. Click **Internet Protocol Version 4 (TCP/IPv4)** to highlight, then click **Properties**.



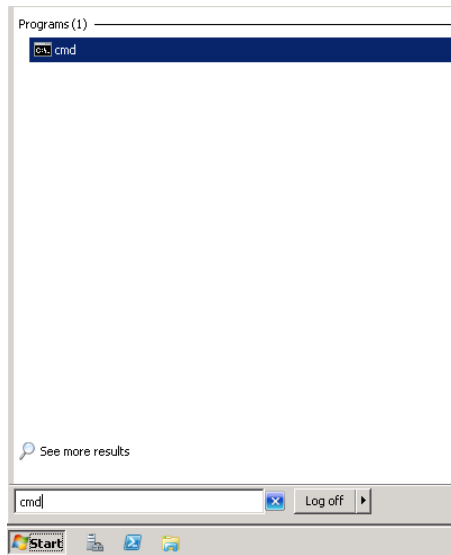
24. Notice the radio button next to **Use the following IP address:** is selected. This is how you indicate that static IP configuration settings are to be used; these are manually set by the network administrator.



25. In the **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog box, set this machine to a DHCP client by clicking the buttons **Obtain an IP address automatically** and **Obtain DNS server address automatically**. Click **OK > Close > Close**. Close all open windows.



26. Test DHCP on the client (Windows 2k8 R2 Internal 2). **Open the command prompt** by clicking **Start**, type **cmd** in the search box and press **Enter**.



27. The Command prompt dialog window opens. Type **ipconfig/all** to verify that this machine is a DHCP client. Maximize the window to see all the information. You should see something similar to the following:

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig/all

Windows IP Configuration

Host Name . . . . . : W2K8R2Internal2
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : netplus.com

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . : netplus.com
Description . . . . . : Intel(R) PRO/1000 MT Network Connection
Physical Address. . . . . : 00-50-56-90-6D-B0
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::bc91:781c:7397:6115%11(Preferred)
IPv4 Address. . . . . : 192.168.12.20(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Sunday, September 15, 2013 12:40:50 PM
Lease Expires . . . . . : Monday, September 23, 2013 12:40:50 PM
Default Gateway . . . . . : 192.168.12.1
DHCP Server . . . . . : 192.168.12.10
DHCPv6 IAD . . . . . : 234901590
DHCPv6 Client DUID. . . . . : 00-01-00-01-18-D2-A7-38-00-50-56-9C-27-3D

DNS Servers . . . . . : 192.168.12.10
NetBIOS over Tcpip. . . . . : Enabled

Tunnel adapter isatap.netplus.com:
```

The Windows 2k8 R2 Internal 2 client obtained IP configuration information such as: IPv4 Address, Subnet mask, Default Gateway, Lease information, DHCP and DNS Server information dynamically and this is indicated by looking at the **DHCP Enabled** row and seeing **Yes** as the setting. If the client was configured to use static IP addressing No would replace the Yes in that row.

28. Release and renew the IP configuration by typing **ipconfig/release** then **ipconfig/renew**.

```

Administrator: C:\Windows\system32\cmd.exe
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : netplus.com

Tunnel adapter Teredo Tunneling Pseudo-Interface:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :

C:\Users\Administrator>ipconfig/renew

Windows IP Configuration

An error occurred while releasing interface Loopback Pseudo-Interface 1 : The system cannot find the file specified.

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . : netplus.com
Link-local IPv6 Address . . . . . : fe80::bc91:781c:7397:6115%11
IPv4 Address. . . . . : 192.168.12.20
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.12.1

Tunnel adapter isatap.netplus.com:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : netplus.com

Tunnel adapter Teredo Tunneling Pseudo-Interface:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :

C:\Users\Administrator>

```

29. Verify that you still have LAN network connectivity by pinging both the Default Gateway and DHCP server addresses.

```

Administrator: C:\Windows\system32\cmd.exe
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : netplus.com

Tunnel adapter Teredo Tunneling Pseudo-Interface:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :

C:\Users\Administrator>ping 192.168.12.1

Pinging 192.168.12.1 with 32 bytes of data:
Reply from 192.168.12.1: bytes=32 time<1ms TTL=64
Reply from 192.168.12.1: bytes=32 time<1ms TTL=64
Reply from 192.168.12.1: bytes=32 time<1ms TTL=64
Reply from 192.168.12.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.12.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>ping 192.168.12.10

Pinging 192.168.12.10 with 32 bytes of data:
Reply from 192.168.12.10: bytes=32 time<1ms TTL=128
Reply from 192.168.12.10: bytes=32 time<1ms TTL=128
Reply from 192.168.12.10: bytes=32 time<1ms TTL=128
Reply from 192.168.12.10: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.12.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>

```

2.2 Conclusion

Setting up a DHCP Server is a step-by-step process requiring planning in order to provide accurate IP configuration parameters to client devices. Settings such as the size of the DHCP pool, addresses of key devices to exclude, DNS server and Default Gateway parameters are paramount to ensure proper Scope configuration. Testing and verification commands such as `ipconfig`, `ipconfig/all`, `ipconfig/release` and `ipconfig/renew` are significant in ensuring DHCP works as planned.

2.3 Review Questions

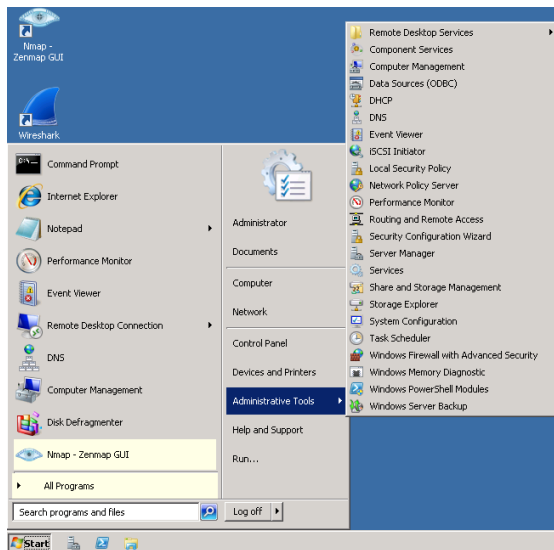
1. *What IPv4 address was assigned to the Windows 2k8 R2 Internal 2 machine by the DHCP server?*
2. *Could this machine have leased a different IP address?*
3. *According the DHCP server configurations, what range of IP addresses could this machine been assigned by DHCP?*
4. *After configuring the host as a DHCP client, was it dynamically allocated DHCP and DNS server addresses correctly?*

3 Observe the Effects of a Deactivated Scope and Resolve the Configuration

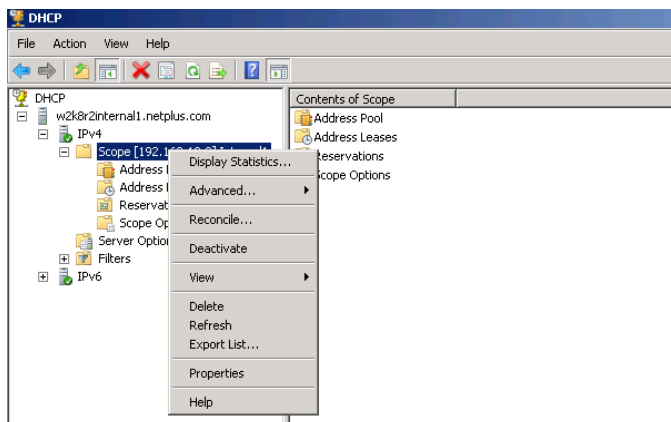
To complete this, lab you will now misconfigure the DHCP server scope and observe the effects of incorrect DHCP settings on a network.

3.1 Deactivate the DHCP Scope, Observe the Effects and Resolve the Problem

1. On the DHCP server (Windows 2k8 R2 Internal 1) machine, click **Start > Administrative Tools > DHCP**.



2. Maximize and resize the windows to suit your viewing preference. Click the + next to the **w2k8r2internal1.netplus.com** and **IPv4** to expand them. **Highlight Scope [192.168.12.0]**, right-click and select **Deactivate**. When you are asked if you are sure you want to deactivate the scope click **Yes**.



- Go back to the DHCP client machine (Windows 2k8 R2 Internal 2) and at the command prompt type **ipconfig /release**. Then, type **ipconfig /all**. Notice that DHCP Enabled is still set to **Yes** but the TCP/IP configurations are APIPA addresses (autoconfiguration IPv4 address of 169.254.x.x) because the DHCP server is unavailable.

```

C:\Users\Administrator>ipconfig /release

Windows IP Configuration

An error occurred while releasing interface Ethernet adapter Local Area Connection:
System cannot find the file specified.

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . . . . . : netplus.com
    Description . . . . . : Intel(R) PRO/1000 MT-2
    Physical Address. . . . . : 00-50-56-90-61-00
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::bc91:7811:149a:5996%1
    Autoconfiguration IPv4 Address. . . . . : 169.254.97.214
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . : 255.255.0.0
    DHCPv6 IAID . . . . . : 234901590
    DHCPv6 Client DUID. . . . . : 00-01-00-01-18-00-00-00-00-00-00-00-00-00-00-00

Tunnel adapter isatap.netplus.com:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . . . . : netplus.com
    Description . . . . . : {4} {5} {6} {7} {8} {9} {A} {B} {C} {D} {E} {F} {G} {H} {I} {J} {K} {L} {M} {N} {O} {P} {Q} {R} {S} {T} {U} {V} {W} {X} {Y} {Z} {AA} {AB} {AC} {AD} {AE} {AF} {AG} {AH} {AI} {AJ} {AK} {AL} {AM} {AN} {AO} {AP} {AQ} {AR} {AS} {AT} {AU} {AV} {AW} {AX} {AY} {AZ} {BA} {BB} {BC} {BD} {BE} {BF} {BG} {BH} {BI} {BJ} {BK} {BL} {BM} {BN} {BO} {BP} {BQ} {BR} {BS} {BT} {BU} {BV} {BW} {BX} {BY} {BZ} {CA} {CB} {CC} {CD} {CE} {CF} {CG} {CH} {CI} {CJ} {CK} {CL} {CM} {CN} {CO} {CP} {CQ} {CR} {CS} {CT} {CU} {CV} {CW} {CX} {CY} {CZ} {DA} {DB} {DC} {DD} {DE} {DF} {DG} {DH} {DI} {DJ} {DK} {DL} {DM} {DN} {DO} {DP} {DQ} {DR} {DS} {DT} {DU} {DV} {DW} {DX} {DY} {DZ} {EA} {EB} {EC} {ED} {EE} {EF} {EG} {EH} {EI} {EJ} {EK} {EL} {EM} {EN} {EO} {EP} {EQ} {ER} {ES} {ET} {EU} {EV} {EW} {EX} {EY} {EZ} {FA} {FB} {FC} {FD} {FE} {FF} {00} {01} {02} {03} {04} {05} {06} {07} {08} {09} {0A} {0B} {0C} {0D} {0E} {0F} {10} {11} {12} {13} {14} {15} {16} {17} {18} {19} {1A} {1B} {1C} {1D} {1E} {1F} {20} {21} {22} {23} {24} {25} {26} {27} {28} {29} {2A} {2B} {2C} {2D} {2E} {2F} {30} {31} {32} {33} {34} {35} {36} {37} {38} {39} {3A} {3B} {3C} {3D} {3E} {3F} {40} {41} {42} {43} {44} {45} {46} {47} {48} {49} {4A} {4B} {4C} {4D} {4E} {4F} {50} {51} {52} {53} {54} {55} {56} {57} {58} {59} {5A} {5B} {5C} {5D} {5E} {5F} {60} {61} {62} {63} {64} {65} {66} {67} {68} {69} {6A} {6B} {6C} {6D} {6E} {6F} {70} {71} {72} {73} {74} {75} {76} {77} {78} {79} {7A} {7B} {7C} {7D} {7E} {7F} {80} {81} {82} {83} {84} {85} {86} {87} {88} {89} {8A} {8B} {8C} {8D} {8E} {8F} {90} {91} {92} {93} {94} {95} {96} {97} {98} {99} {9A} {9B} {9C} {9D} {9E} {9F} {A0} {A1} {A2} {A3} {A4} {A5} {A6} {A7} {A8} {A9} {AA} {AB} {AC} {AD} {AE} {AF} {AG} {AH} {AI} {AJ} {AK} {AL} {AM} {AN} {AO} {AP} {AQ} {AR} {AS} {AT} {AU} {AV} {AW} {AX} {AY} {AZ} {BA} {BB} {BC} {BD} {BE} {BF} {BG} {BH} {BI} {BJ} {BK} {BL} {BM} {BN} {BO} {BP} {BQ} {BR} {BS} {BT} {BU} {BV} {BW} {BX} {BY} {BZ} {CA} {CB} {CC} {CD} {CE} {CF} {CG} {CH} {CI} {CJ} {CK} {CL} {CM} {CN} {CO} {CP} {CQ} {CR} {CS} {CT} {CU} {CV} {CW} {CX} {CY} {CZ} {DA} {DB} {DC} {DD} {DE} {DF} {DG} {DH} {DI} {DJ} {DK} {DL} {DM} {DN} {DO} {DP} {DQ} {DR} {DS} {DT} {DU} {DV} {DW} {DX} {DY} {DZ} {EA} {EB} {EC} {ED} {EE} {EF} {EG} {EH} {EI} {EJ} {EK} {EL} {EM} {EN} {EO} {EP} {EQ} {ER} {ES} {ET} {EU} {EV} {EW} {EX} {EY} {EZ} {FA} {FB} {FC} {FD} {FE} {FF}

DNS Servers . . . . . : fec0:0:0:ffff::1%1
                        fec0:0:0:ffff::2%1
                        fec0:0:0:ffff::3%1

NetBIOS over Tcpip. . . . . : Enabled
  
```

- On the command line, type **echo "your first and last names"**. Then press the Enter key. Take a screenshot that contains your full name and the running outputs obtained at Step 3 above.
- Now return to the DHCP server machine (Windows 2k8 R2 Internal 1). If necessary, click the + next to the **w2k8r2internal1.netplus.com** and **IPv4** to expand them. Highlight **Scope [192.168.12.0]**, right-click and select **Activate**.
- On more time, return to the DHCP client machine (Windows 2k8 R2 Internal 2) and type **ipconfig /renew** to reset the TCP/IP configuration settings.
- Ping the DHCP server machine (Windows 2k8 R2 Internal 1) to verify that the settings are correct and there is network connectivity.

3.2 Conclusion

The DHCP protocol allows a server to dynamically distribute IP addressing and configuration information to clients. Normally, the DHCP server provides the client with at least this basic information: IP Address, Subnet Mask, and Default Gateway. By using DHCP server computers to centrally manage IP addresses and other related configuration parameters, network administrators are relieved of the trouble of manually configuring TCP/IP settings on all network hosts.

3.3 Review Questions

- What is the function of the **ipconfig/release** and the **ipconfig/renew** commands?
- What type of devices would be better served to have static IP configuration?