CompTIA Network+® Lab Series
Network Concepts

Lab 5: TCP/IP Protocols – Other Key Protocols

Objective 1.5: Identify common TCP and UDP default ports
Objective 1.6: Explain the function of common networking protocols
Objective 1.7: Summarize DNS concepts and its components
Objective 2.3: Explain the purpose and properties of DHCP
Objective 4.3: Given a scenario, use appropriate software tools to troubleshoot connectivity issues

Document Version: 2015-09-18

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

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.

This lab will introduce students to additional key services and protocols used on TCP/IP networks. These services include DHCP and DNS.

This lab includes the following tasks:

1. Create and Test a DHCP Scope
2. Create and Test a DHCP Reservation
3. Create and Test DNS Records

Objective: Using Key Network Services and their Protocols

Many services exist on a network for the purpose of making the user experience easier. Many services, when operating properly, are invisible to the end-user. However, without these services, users would not have a pleasant network experience.

Key terms for this lab:

Dynamic Host Configuration Protocol (DHCP) – a protocol that allows devices to automatically obtain network settings (such as IP address, default gateway, etc.) so they can communicate on the network. DHCP uses UDP ports 67 (Server) and 68 (Client)

Reservation – with DHCP, the process where an administrator assigns an address for DHCP to give to a client

Media Access Control (MAC) address – the physical address burned into the ROM of an Ethernet network card; used by switches at the Data Link layer of the OSI model to move information between nodes on the same network

Domain Name System (DNS) – the protocol used to map hostnames and domain names to an IP address on the Internet. DNS uses UDP port 53 for initiating requests

Fully Qualified Domain Name (FQDN) – the domain name that specifies the exact location of the specified node in the DNS hierarchy

Forward Lookup Zone – the zone used by DNS clients to obtain information such as IP addresses that correspond to DNS domain names or services in the zone

Host (A) record – the DNS record that links a FQDN to an IPv4 address

Host (AAAA) record – the DNS record that links a FQDN to an IPv6 address

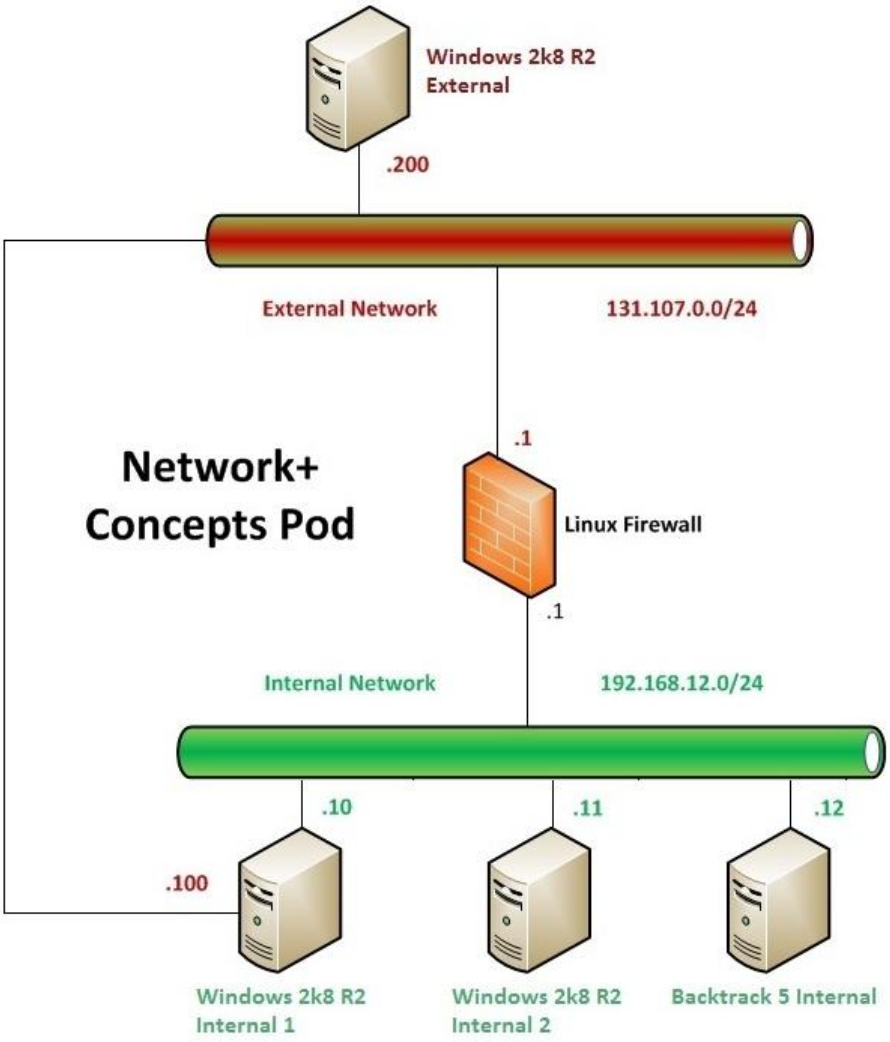
Alias – a secondary name assigned to a host within DNS – allows an administrator to provide multiple names the same host can respond to

Reverse Lookup Zone – the zone that provides mapping from IP addresses back to DNS domain names

in-addr.arpa – The reverse lookup zone used by IPv4 to map IP addresses to DNS names

Pointer (PTR) record – the DNS record that links an IP address to a FQDN – used for reverse lookups

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.

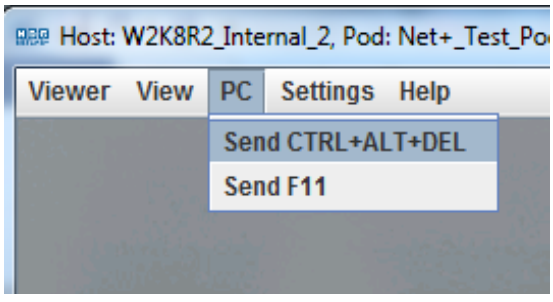
Required Virtual Machines and Applications

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

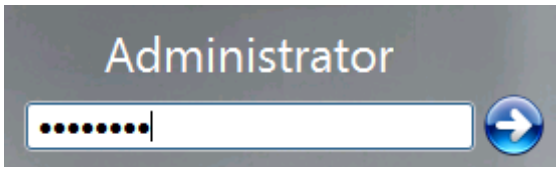
Windows 2k8 R2 Internal 1	192.168.12.10
Windows 2k8 R2 Internal 1 password	P@ssw0rd
Windows 2k8 R2 Internal 2	192.168.12.11
Windows 2k8 R2 Internal 2 password	P@ssw0rd
Backtrack 5 Internal	192.168.12.12
Backtrack 5 Internal username/password	root/toor

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 in to.
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.



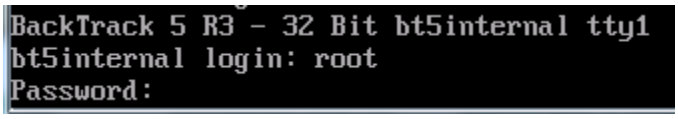
4. If the **Initial Configuration Tasks** and/or **Server Manager** windows appear, close them by clicking on the "**X**" in the top-right corner of the window.

Backtrack 5 Internal Login

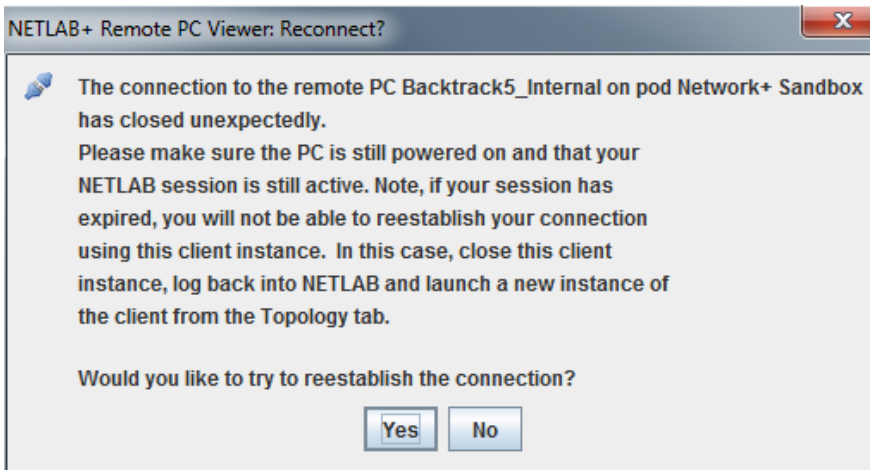
1. Click on the Backtrack 5 Internal icon on the topology.
2. At the **bt5internal login:** prompt, type the username **root** and press **Enter**.

3. At the **Password:** prompt, type the password **toor** and press **Enter**.

The password will not be displayed as you type into the prompt.



4. Once you have successfully logged in, type **startx** at the **root@bt5internal:~#** prompt and press **Enter**. This will start the GUI. (Note: if you are disconnected after typing startx, click yes on the popup message to reconnect).

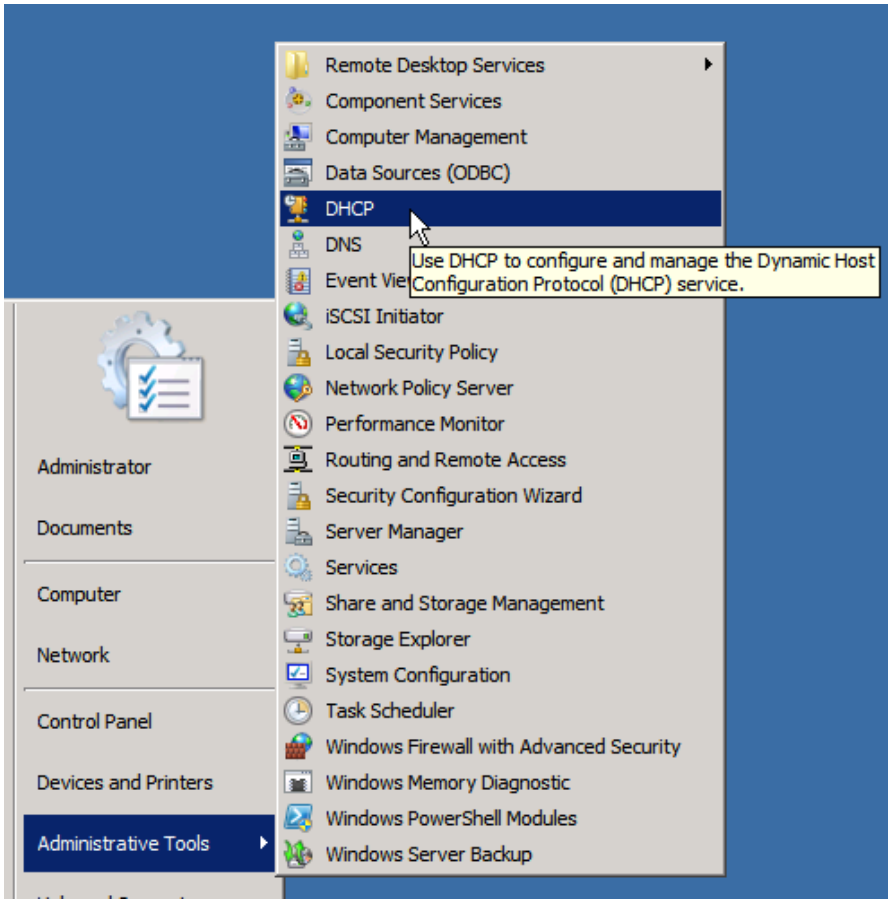


1 Create and Test a DHCP Scope

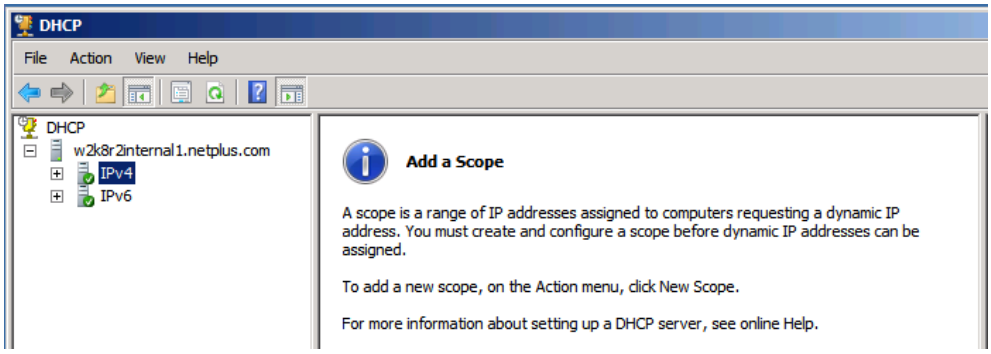
Dynamic Host Configuration Protocol (DHCP) is a protocol in the TCP/IP suite that allows a server to automatically assign TCP/IP settings to a client computer. This simplifies the administrative overhead since an administrator only needs to create the pools and assign options in one location. Once properly configured, very few changes ever need to be made to the DHCP server.

1.1 Create a DHCP Scope

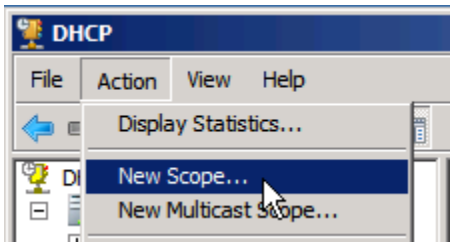
1. Use the instructions provided in the Lab Settings section to log into the Windows 2k8 R2 Internal 1 machine, if you are not logged in already.
2. The DHCP role has already been added to this server. Now, it must be configured. To access the DHCP configuration console, click **Start**, point to **Administrative Tools**, and select **DHCP**.



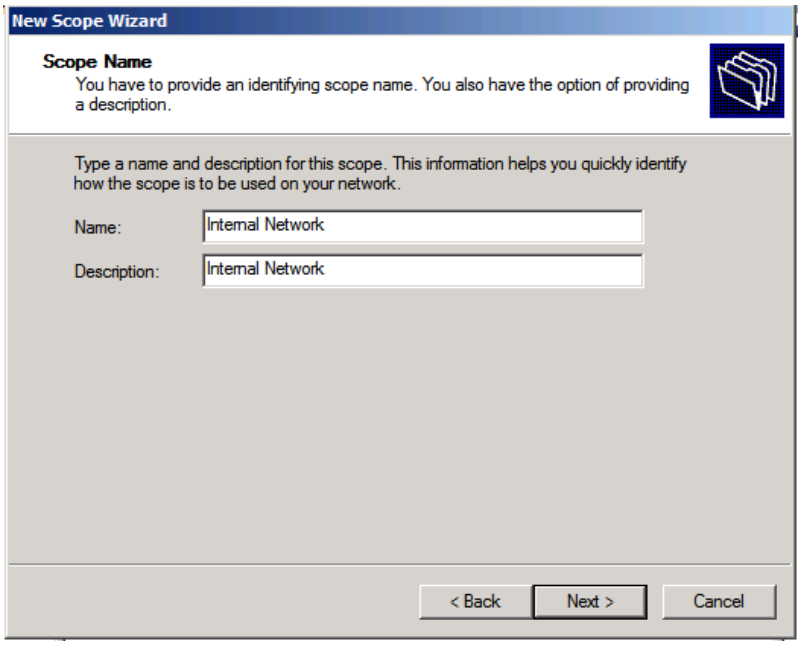
3. Click the "**+**" next to the server name to expand the tree. Notice that DHCP can be used for both IPv4 and IPv6 addressing. Click on **IPv4** in the tree. Notice the information page in the center pane with instructions on how to create a new scope.



4. Following the instructions on the screen, click the **Action** menu and click **New Scope**.



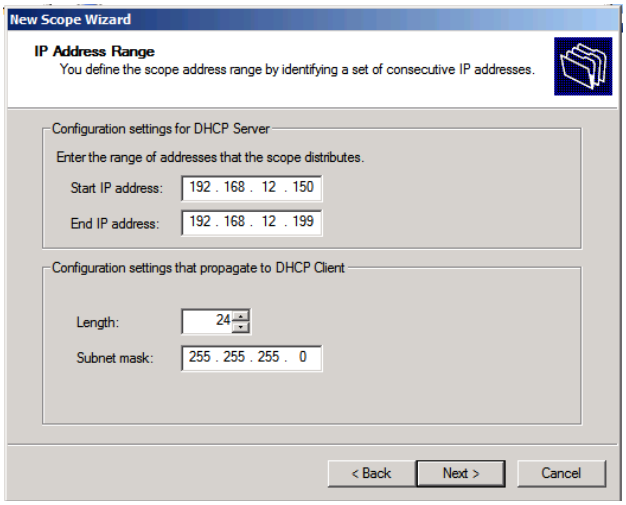
5. When the **New Scope Wizard** appears, click **Next** on the Welcome screen to continue.
6. On the **Scope Name** page, type **Internal Network** in the **Name** and **Description** fields. Click **Next.**



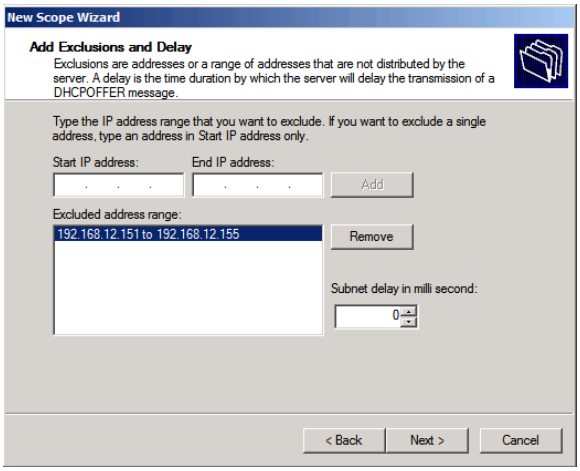
This page configures the range of addresses handed to clients as well as the subnet mask that needs to be associated with the address. The DHCP server compares the information from a DHCP request to its available pools to see if it can service the request.

7. To complete the **IP Address Range** page use the following information:
   - Start IP address: 192.168.12.150
   - End IP address: 192.168.12.199
   - Length: 24
   - Subnet Mask: 255.255.255.0

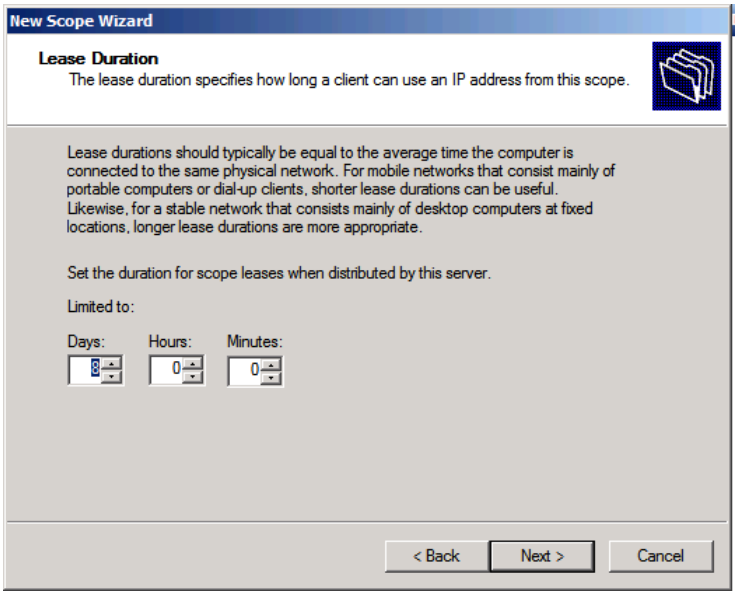
   Click **Next**.



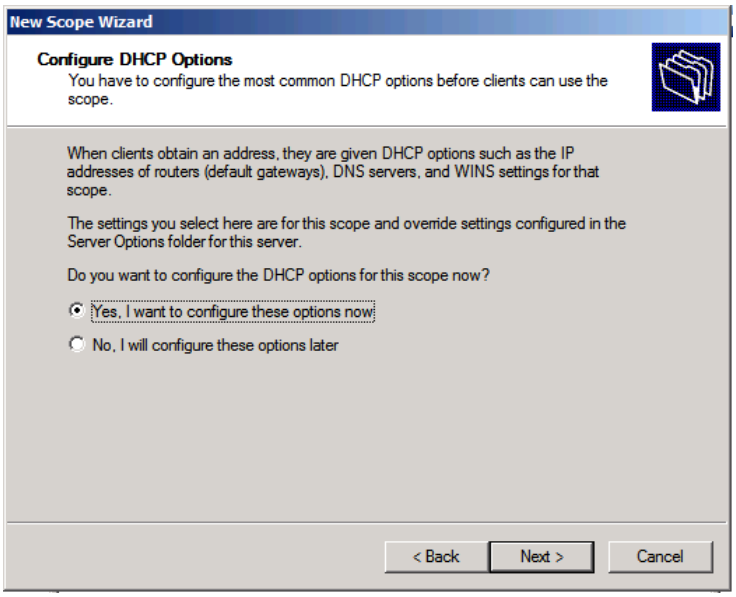
8. Read the description provided on the **Add Exclusions and Delay** page. An example of addresses that could be excluded in a range could be those used for network printers. In this example, exclude the IP address range **192.168.12.151** through **192.168.12.155**. Once the IP addresses have been entered, click the **Add** button to add them to the list. Multiple ranges or even single IP addresses can be excluded within the same scope. Click **Next**.



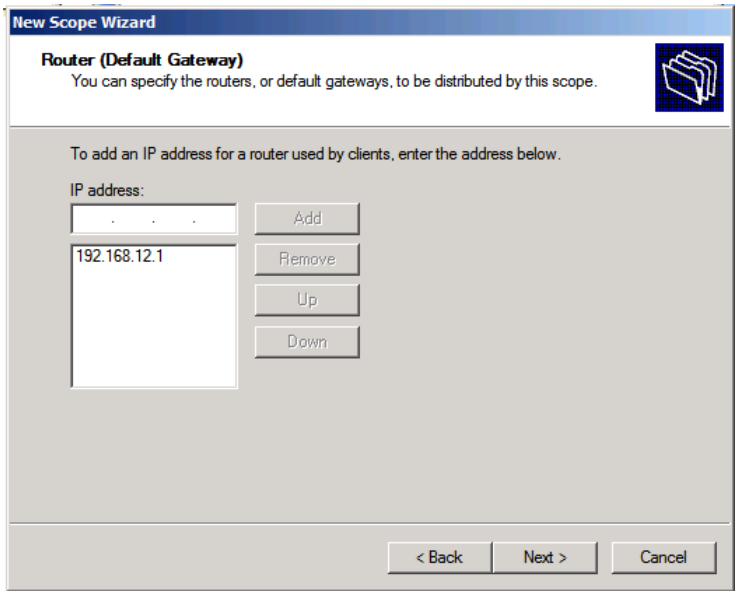
9. Leave the **Subnet delay** as default and click **Next** to continue.
10. The default **Lease Duration** for a Windows-based DHCP server is 8 days. For networks that change infrequently (such as most wired networks) or networks not at risk of running out of addresses, longer DHCP leases reduce the amount of DHCP traffic propagating throughout the network. For networks that change very frequently (such as a guest wireless network), shorter DHCP leases return IP addresses back to the available pool more quickly so they can be assigned to new clients. For this example, leave the default setting and click **Next** to continue.



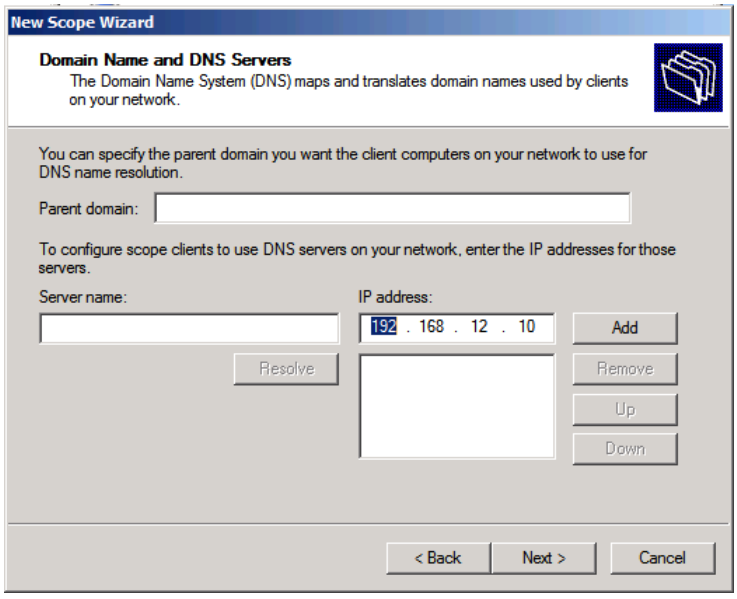
11. Read the description on the **Configure DHCP Options** page. There are two types of DHCP options in Windows – scope options and server options. As their name describes, scope options apply only to the particular scope they are configured with while server options apply to all DHCP scopes. If an option is set in both places, scope options take precedence over server options. For example, the **Router** option (referring to the default gateway) is typically set as a scope option since that default gateway is only valid for that network while the **DNS server** option is typically set as a server option since all computers on all networks typically use the same DNS server. To configure scope options now, leave the default **Yes, I want to configure these options now** and click **Next** to continue.



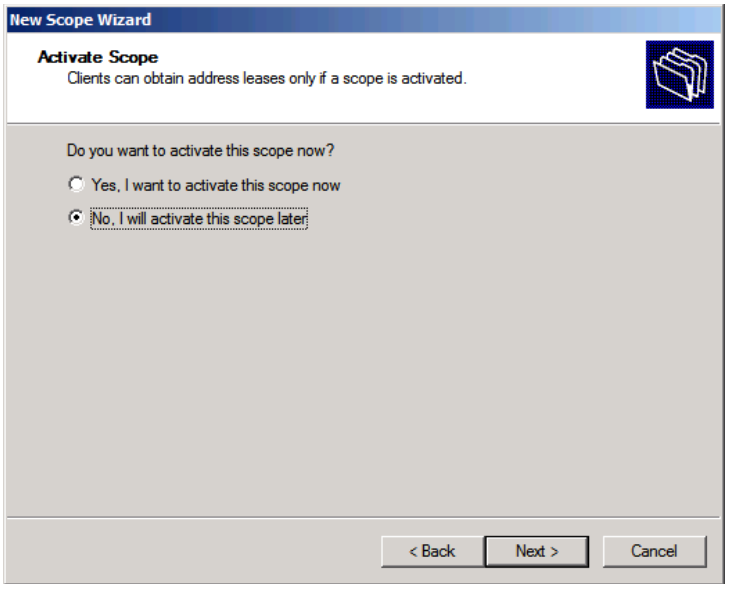
12. On the **Router (Default Gateway)** page, type the IP address **192.168.12.1** and click the **Add** button. Once the address has been added, click **Next** to continue.



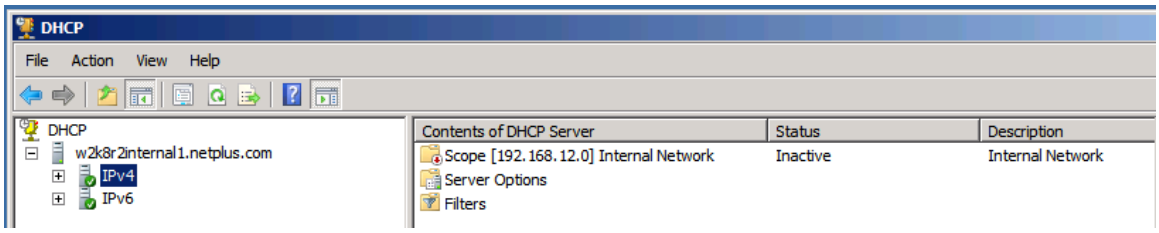
13. On the **Domain Name and DNS Servers** page, click the address listed under the **IP address** heading and click **Remove**. While it is not incorrect to configure these options now, for the purpose of this lab these settings will be configure as server options later. Click **Next** to continue.



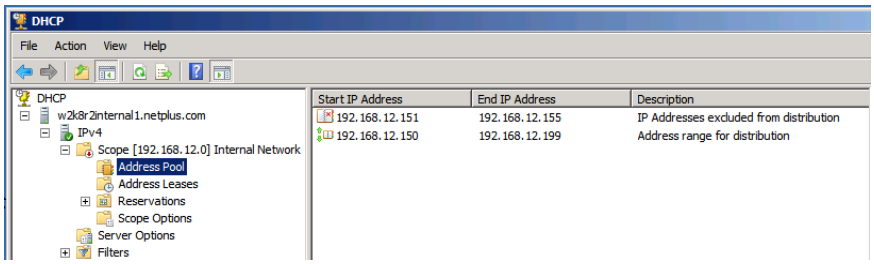
14. Click **Next** to continue past the **WINS Servers** page.
15. On the **Activate Scope** page, select the option **No, I will activate this scope later**. Once a scope is active, it will service DHCP requests from clients. However, since more settings need to be configured first, this DHCP server is not ready to service requests. Allowing the server to service requests before all settings have been properly configured may result in IP configuration errors that do not allow the client to properly communicate on the network. Once the selection is made, click **Next** to continue.



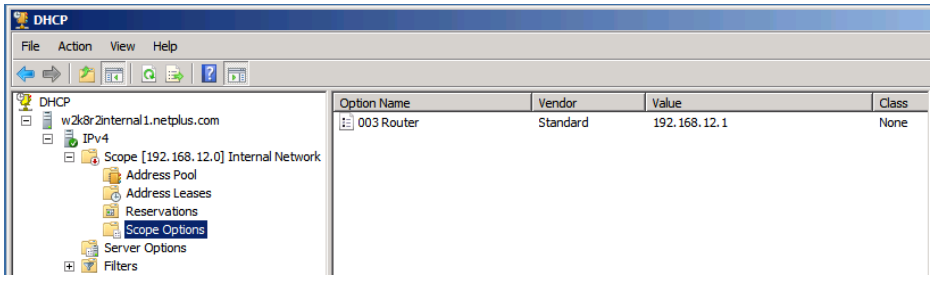
16. Click **Finish** to complete the **New Scope Wizard**. The new scope will appear in the center pane with a red down arrow indicating the scope is not active. The **Status** column also appears as **Inactive**.



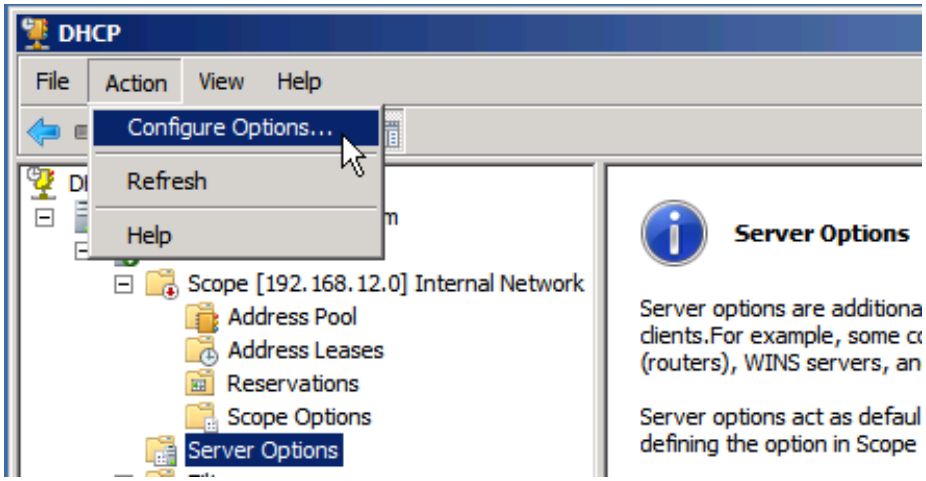
17. Clicking the "**+**" arrow next to **IPv4** and then **Scope** expands the scope to reveal its settings.



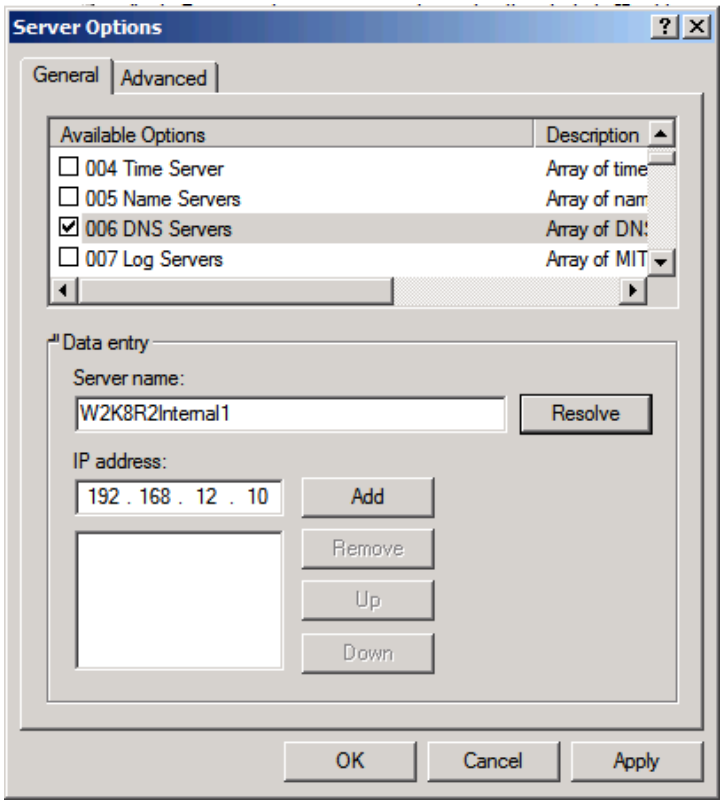
- The **Address Pool** shows which addresses are available for DHCP to distribute to a scope as well as any configured exclusions.
- The **Address Leases** shows all addresses that have been assigned by the DHCP server to clients. At this time, there will be no items to show in this view, as the scope has not been activated.
- The **Reservations** shows any addresses that an administrator has manually configured for a DHCP server to assign to a client. Creating a DHCP reservation ensures that the DHCP client always receives the same IP address even though it has been configured to automatically obtain its IP address via DHCP. Note that no reservations exist at this time, but information is displayed on how to create one.
- The **Scope Options** shows all DHCP options that have been configured for just this scope. Windows DHCP server will also list any server options that have been configured in this list as well, but will not allow an administrator to modify them from this screen. Since the **Router** option was configured via the wizard, it appears in this list.



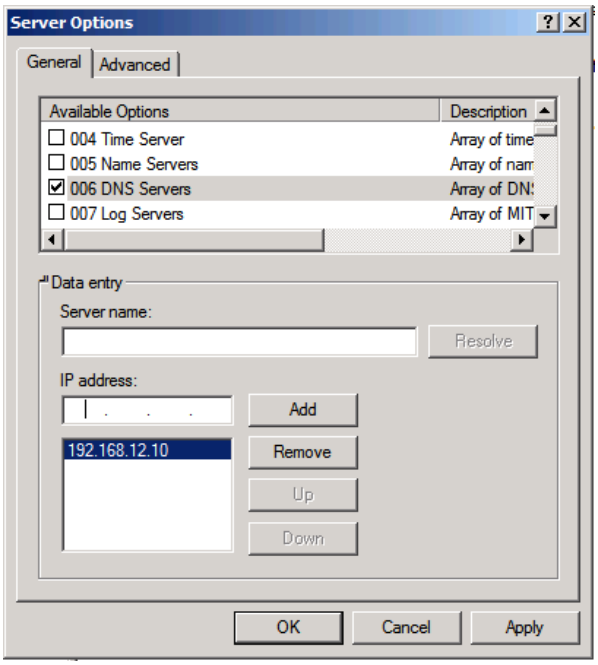
18. To add or modify **Server Options**, click on the link in the left column. No options are currently configured for this server. For this example, the DNS options will be configured here. Read the information in the center pane, then click on the **Action** menu and select **Configure Options**.



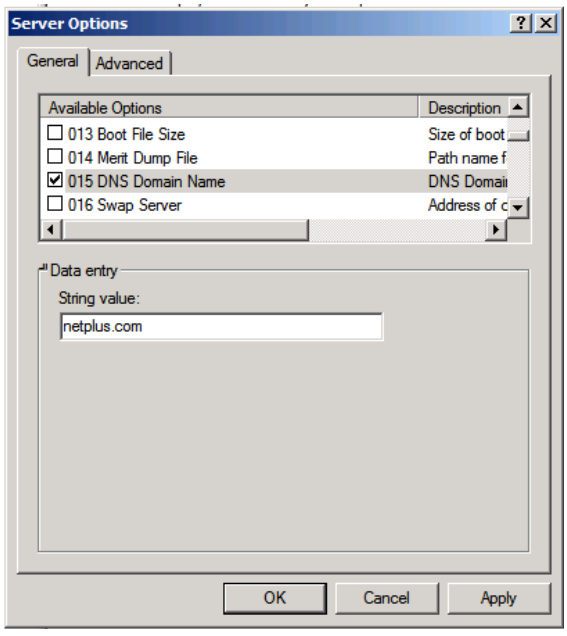
19. The **Server Options** dialog box allows multiple options to be added at one time. Scroll down the list of available options, put a check next to the **006 DNS Servers** option and be sure the selection is highlighted. Since the server you are currently working with is also providing DNS service, type the name of the server, **W2K8R2Internal1**, into the **Server Name** dialog box and click **Resolve**.



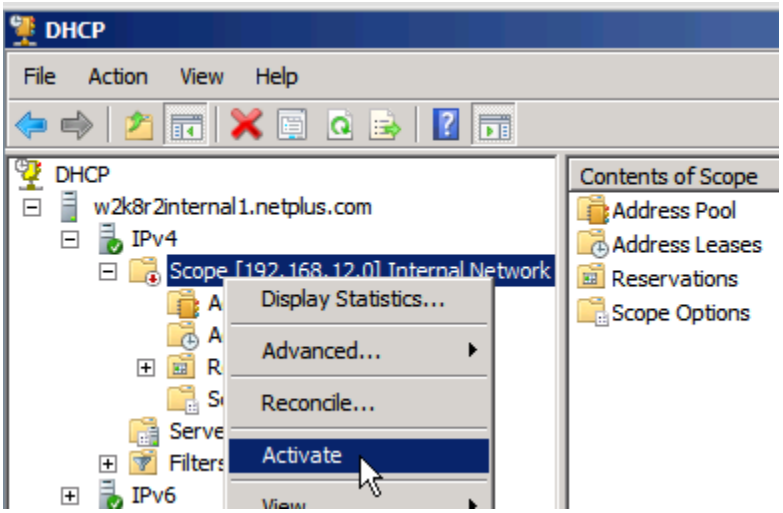
20. Notice the IP address of the machine appears in the dialog box below. Alternatively, the IP address could have been typed directly into this dialog box. Click the **Add** button to add this server to the list. Once the server has validated that the machine in question is actually providing DNS service, the IP address will be added to the list.



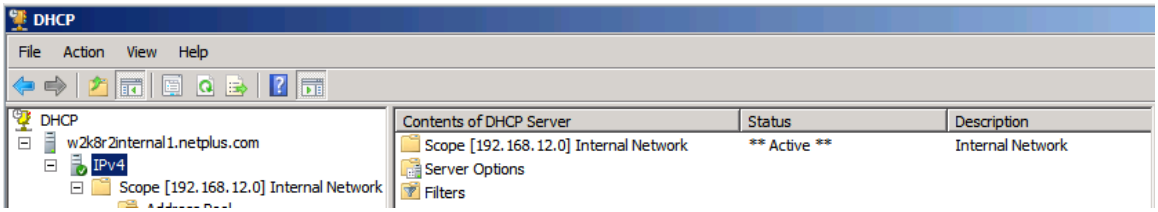
21. Continue scrolling down the list and put a check next to the **015 DNS Domain Name** option. In the **String value:** textbox, type **netplus.com**. Continue scrolling through the list of available options to see what is available. Click **OK** to save the changes to the two options.



22. The two configured options now appear in the center pane. Clicking on the **Scope Options** reveals the newly configured options as well. Pay close attention to the icons associated with each option. Keep in mind that while server options do appear with the scope options, they cannot be modified from this section.
23. Now that the scope is configured, it needs to be activated. In the left pane, right-click on **Scope [192.168.12.0] Internal Network** then select **Activate** from the context menu.



24. Notice that the red down arrow disappears from the scope. Clicking on **IPv4** also reveals the status for the scope has changed to ****Active****.

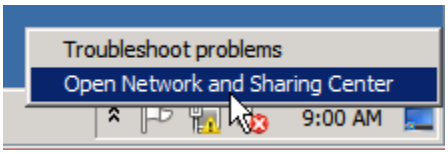


25. Keep all windows open to continue with the next task section.

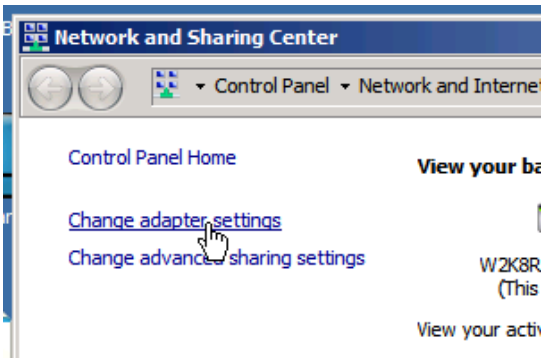
1.2 Test the DHCP scope

1. Use the instructions provided in the Lab Settings section to log into the Windows 2k8 R2 Internal 2 machine, if you are not logged in already.
2. Currently, the IP address on this machine is set statically. A quick look at the output of the command **ipconfig /all** from the command line confirms this.

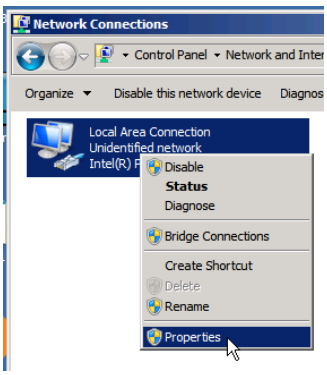
3. Change the settings for this machine to be able to obtain an IP address automatically. Open the Network and Sharing Center by right-clicking the network icon in the system tray and clicking **Open Network and Sharing Center**.



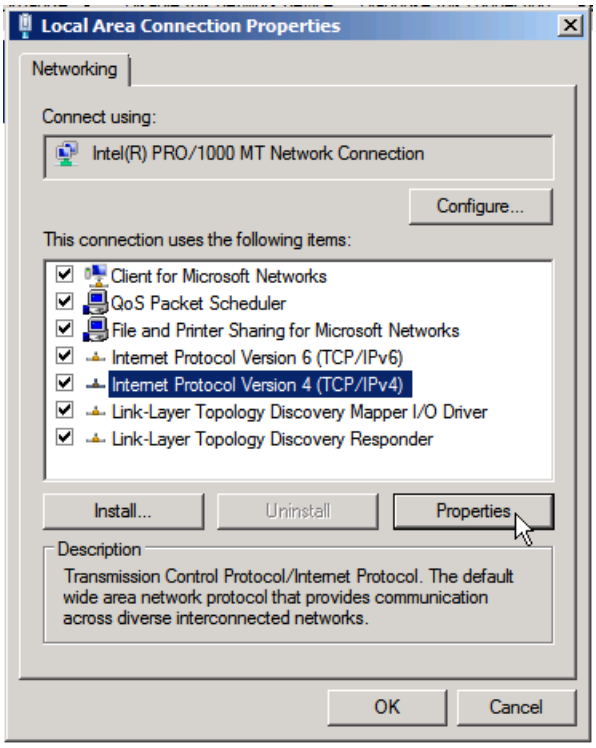
4. When the Network and Sharing Center window appears, click the link **Change Adapter Settings** in the left column.



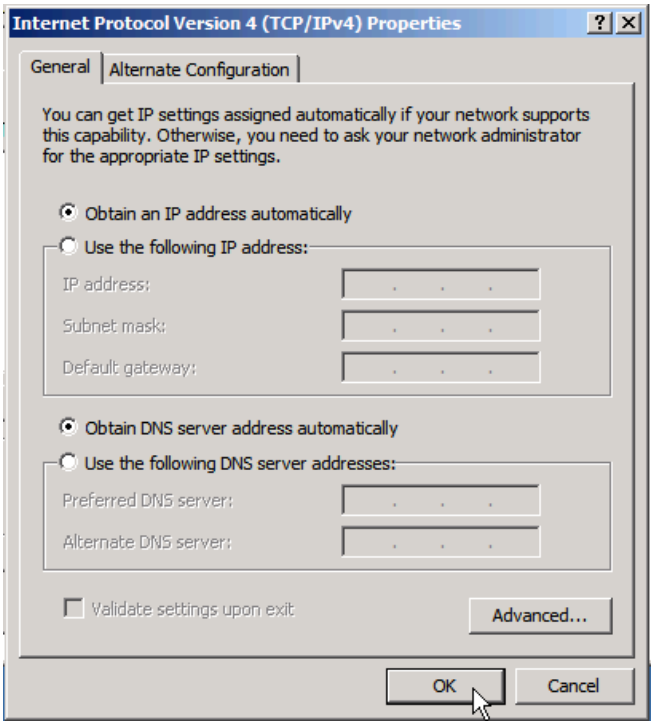
5. Right-click the Local Area Connection and select **Properties** from the context menu.



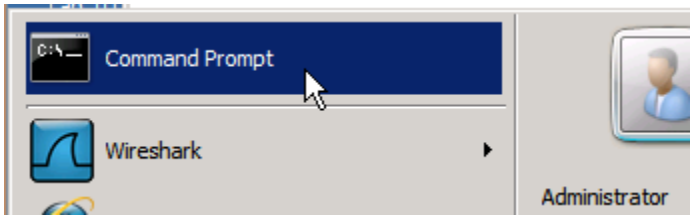
6. Select the option **Internet Protocol Version 4** from the list and click **Properties**.



7. In the IPv4 Properties window, select the radio buttons next to **Obtain an IP address automatically** and **Obtain DNS server address automatically**. Click **OK** and **Close** to save these changes.



8. Open a command prompt window by clicking **Start** and clicking the **Command Prompt** icon.



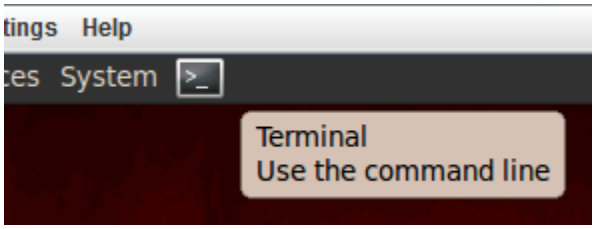
9. To initiate the DHCP process, type the command **ipconfig /renew** into the command prompt window and press **Enter**. After a brief moment, the newly obtained IP address should appear under the **Ethernet adapter Local Area Connection** heading. Notice that this address is the first available IP address from the DHCP pool. Also, notice the DNS suffix and default gateway are also set as those were options set in the DHCP configuration.

```
C:\Users\Administrator>ipconfig /renew

Windows IP Configuration

An error occurred while releasing interface Loopback Pseudo-Interfac
stem 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. . . . . . . . . . . : 192.168.12.150
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.12.1
```

10. Now issue the command **ipconfig /all**. Notice the **DHCP Enabled** is now **Yes**. The DNS server address, which was also an option set in the DHCP configuration, is also set.

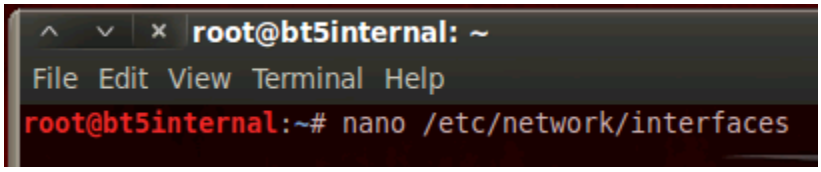
```
C:\Users\Administrator>ipconfig /all

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. . . . . . . . . . . : 192.168.12.150(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Thursday, August 08, 2013 2:19:11 PM
   Lease Expires . . . . . . . . . . : Friday, August 16, 2013 2:23:33 PM
   Default Gateway . . . . . . . . . : 192.168.12.1
   DHCP Server . . . . . . . . . . . : 192.168.12.10
   DHCPv6 IAID . . . . . . . . . . . : 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
```

11. Now, use the instructions in the Lab Settings section to log into the BackTrack 5 machine.
12. Click the icon to the right of the **System** menu to gain access to the terminal window.

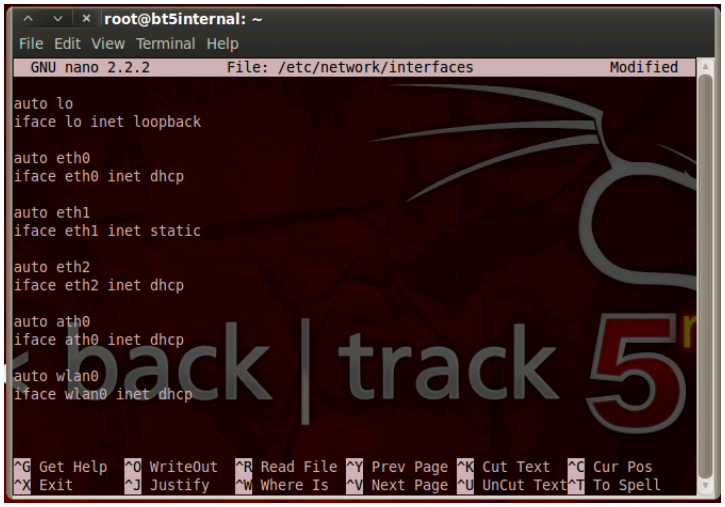


Keep in mind that **Linux commands are case sensitive**. The Linux commands below must be entered exactly as shown.

13. In Linux, configuration files are used to configure many aspects of the operating system including the network interface settings. To edit the interface settings, type the command **nano /etc/network/interfaces** in the terminal window and press **Enter**.

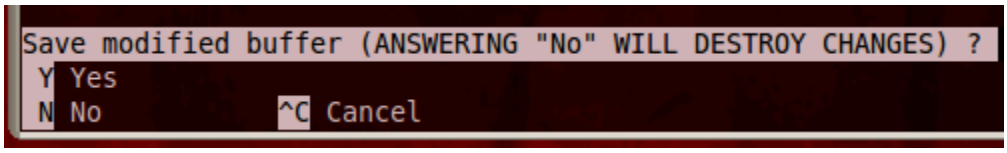


14. Using the arrow keys, position the cursor to the front of the line **address 192.168.12.12** two lines under the **auto eth0** heading. Carefully use the delete key to remove this and the next two lines, **netmask 255.255.255.0** and **gateway 192.168.12.1**. Next, use the arrow keys to position the cursor in front of the word **static** on the line immediately under the **auto eth0** heading. Use the delete key to remove the word **static** and replace it with **dhcp**. When completed, the screen should look exactly like the figure below.

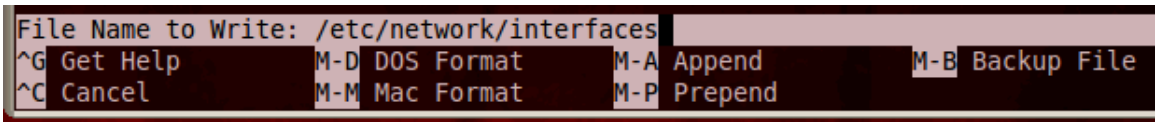


WARNING: Be extremely careful not to change any settings other than those listed in this step for the **eth0** interface as this could cause undesirable results.

15. Once the configuration file has been correctly modified, press **Ctrl**+**X**. When prompted to **Save modified buffer**, press **Y**

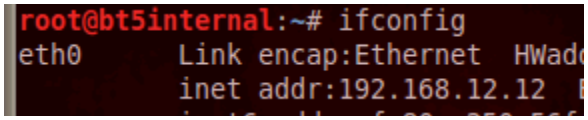


16. When prompted for **File Name to Write**, press **Enter** to accept the default name. This will overwrite the old configuration file with the new one.

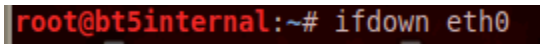


The editor will close and revert to the terminal prompt.

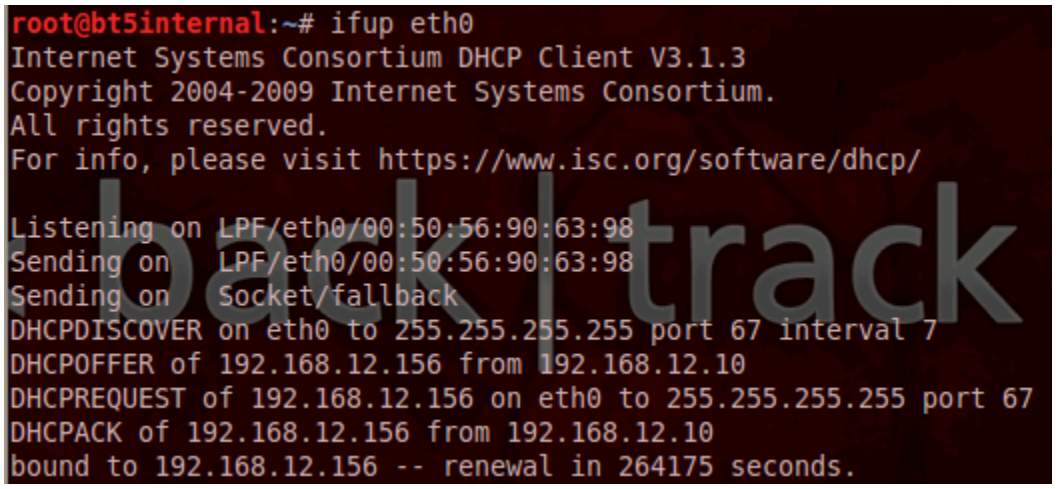
17. Changes made to a Linux configuration file do not take effect immediately. Instead, the service or interface associated with the configuration file needs to be restarted. For the network interface, this can be verified by typing the command **ifconfig** into the terminal window and pressing **Enter**. Notice the line **inet addr:** is still set to static IP address in the old configuration file.



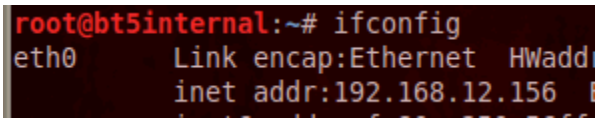
18. To restart the network interface, first type the command **ifdown eth0** into the terminal window and press **Enter**. This shuts down the interface.



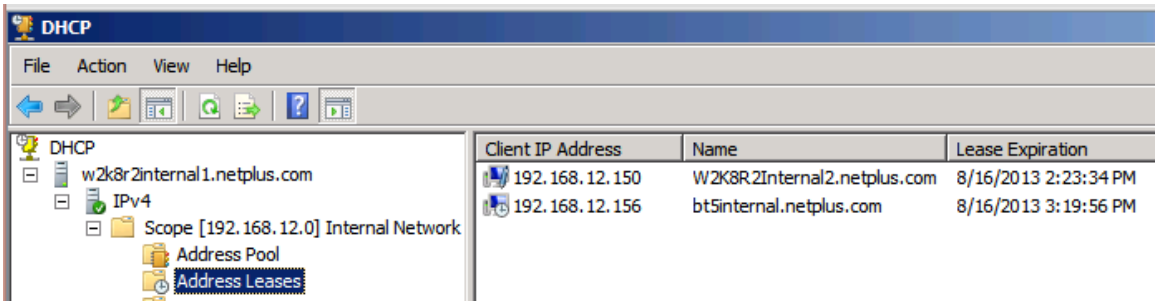
19. To bring the interface back online, type the command **ifup eth0** into the terminal window and press **Enter**.



Notice the last four lines of the command output. The entire DHCP DORA (Discover-Offer-Request-Acknowledge) process is displayed. During the Discover process, the BackTrack 5 machine sent a broadcast to port 67 (all DHCP servers) wanting an IP address. The DHCP server offered the BackTrack 5 machine the IP address of 192.168.12.156 during the Offer process. The BackTrack 5 machine broadcasted its request to use the address 192.168.12.156 during the Request phase. Finally, the DHCP server acknowledges the BackTrack 5 machine will use the IP add 192.168.12.156 and creates a binding. Issuing the **ifconfig** command once again verifies the new IP address.



20. Go back to the Windows 2k8 R2 Internal 1 machine and the DHCP console. Click on the **Address Leases** in the left pane. Notice both machines appear in the center pane. If no leases are displayed in the center pane, click the **Action** menu and select **Refresh**.



26. Keep all windows open to continue on with the next task section.

1.3 Conclusion

Dynamic Host Configuration Protocol (DHCP) is a protocol in the TCP/IP suite that allows a server to automatically assign TCP/IP settings to a client computer. This simplifies the administrative overhead since an administrator only needs to create the pools and assign options in one location. Once properly configured, very few changes ever need to be made to the DHCP server.

1.4 Review Questions

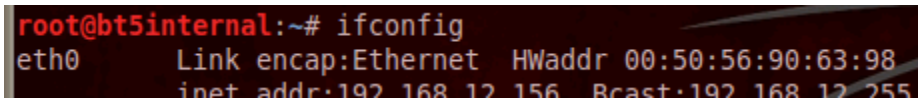
1. *What command, in Windows, restarts the DHCP lease process?*
2. *What commands will reset a network interface in Linux?*
3. *Name the four steps, in order, in a successful DHCP process.*

2 DHCP Reservations

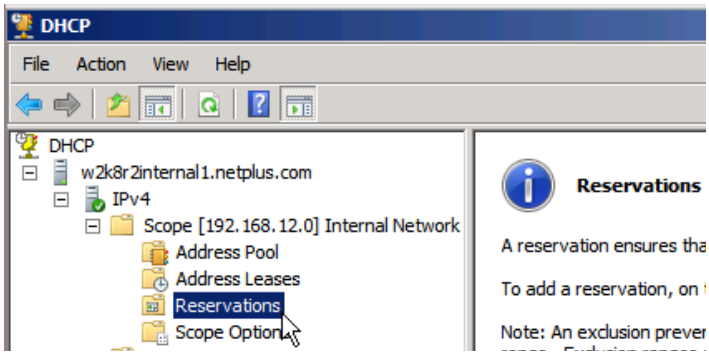
Administrators sometimes need a specific IP address to always be assigned to the same client. Two options exist in these scenarios – statically assign the address or create a DHCP reservation. Reservations allow a DHCP administrator to control which client gets a particular IP address. Reservations are optional, but convenient when an administrator wants to control the IP settings for a device such as a network printer.

2.1 Create and Test a DHCP Reservation

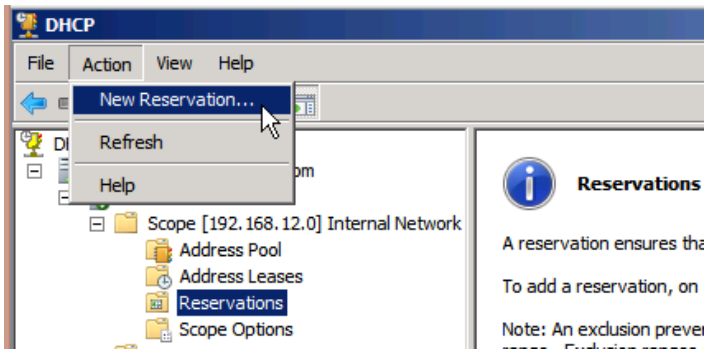
1. Before a reservation can be created, an administrator must know the MAC address associated with the machine the reservation will be made for. In this example, the **BackTrack 5 Internal** machine will be used. In the terminal window, type the command ifconfig and press Enter. Look for the section labeled HWaddr on the first line. This is the MAC address for this machine. Write this address down as it will be used in the next section.



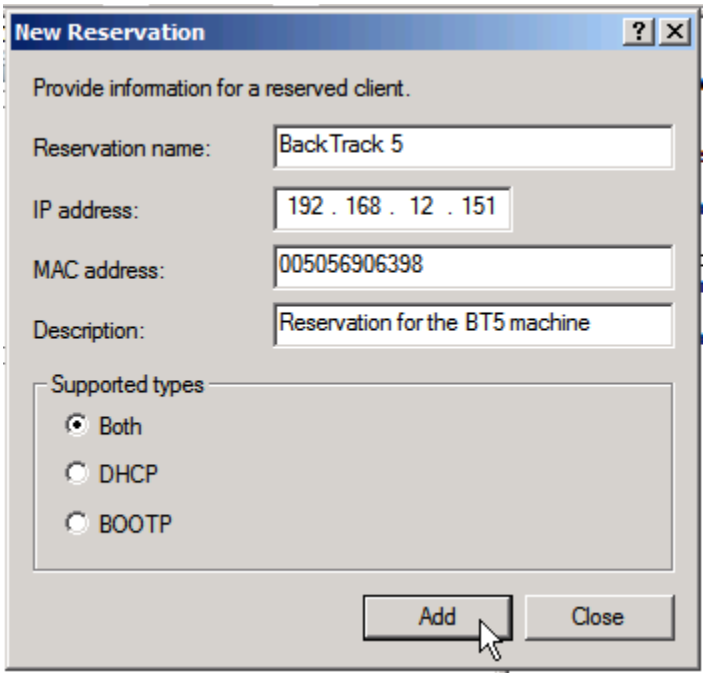
2. In the DHCP console on the Windows 2K8 R2 Internal 1 machine, click on Reservations in the left pane.



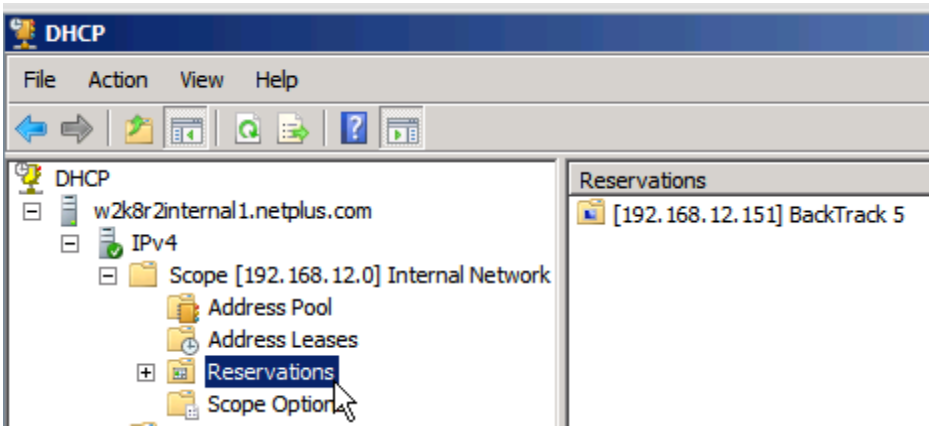
3. Click the **Action** menu and select **New Reservation…**



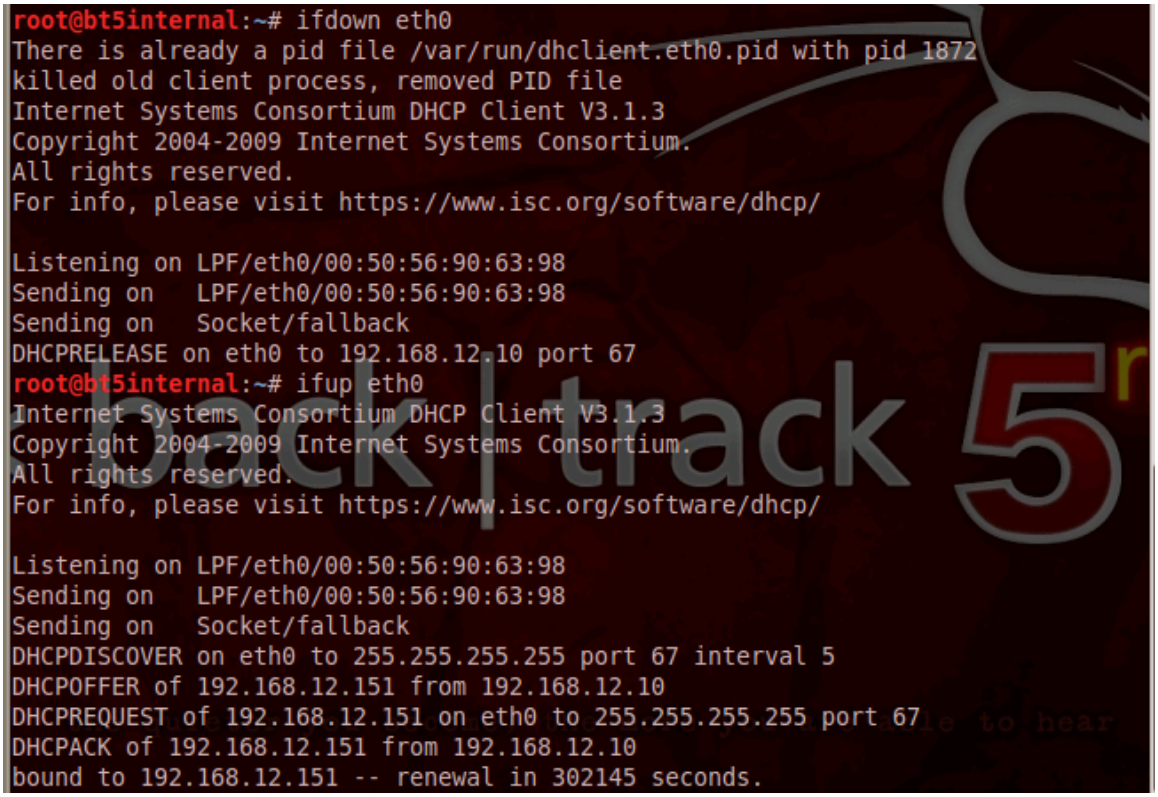
4. In the New Reservation window, type **BackTrack 5** for the **Reservation name**. The first three octets have already been filled in for the **IP address**, so simply type **151** in the fourth octet. For the **MAC address**, type the address from step 1 above without using colons. Type a brief description of the reservation in the **Description**. Once all fields have been completed, click **Add** to create the reservation.



5. Upon adding the reservation, the New Reservation dialog box will remain open in case other reservations need to be made. Click **Close** to close the dialog box. The reservation now appears in the center pane.



6. To test the reservation, reset the network interface on the BackTrack 5 Internal machine by typing **ifdown eth0** followed by **ifup eth0** in the terminal window. The **ifdown** command issues a DHCPRELEASE to the DHCP server allowing its address to be placed back into the pool of available addresses. The **ifup** command issues a DHCPRENEW command to ask the DHCP server for a new IP address. This time, the MAC address from the BackTrack 5 Internal machine matches a reservation created on the DHCP server, so the DHCP server issues the reserved address to the machine. Notice that this occurs even though the address used in the reservation is part of the excluded range created in the DHCP pool. DHCP reservation are another example of addresses that can be excluded from DHCP pools.



7. Keep all windows open to continue with the next task section.

2.2 Conclusion

Administrators sometimes need a specific IP address to always be assigned to the same client. Two options exist in these scenarios – statically assign the address or create a DHCP reservation. Reservations allow a DHCP administrator to control which client gets a particular IP address. Reservations are optional, but convenient when an administrator wants to control the IP settings for a device such as a network printer.

2.3 Review Questions

1. *What command displays the IP configuration on a Linux machine?*

2. *True or false? Colons are required when entering the MAC address into the Reservation window?*

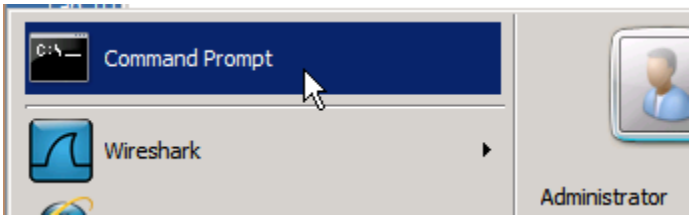
3. *True or false? Reservations are immediate and do not require the DHCP lease process to be restarted?*

3 DNS Records

Domain Name System (DNS) is the protocol in the TCP/IP suite that allows end users to have the capability to remember names for clients instead of their IP addresses (which can change). DNS servers provide the name-to-IP address translations necessary to allow communication across TCP/IP networks. If configured properly, they can also provide the reverse IP address-to-name translations.

3.1 Create and Test DNS Records

1. On the Windows 2K8 R2 Internal 1 machine, open a command prompt window by clicking **Start** and clicking the **Command Prompt** icon.



2. Ping the BackTrack 5 Internal machine using the fully qualified domain name by typing the command: **ping bt5internal.netplus.com**

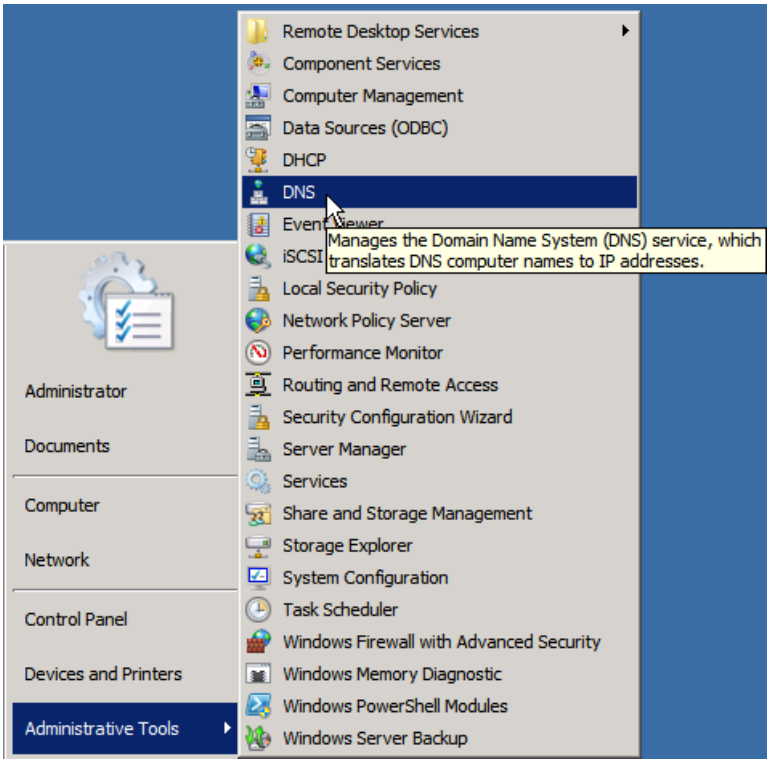
```
C:\Users\Administrator>ping bt5internal.netplus.com

Pinging bt5internal.netplus.com [192.168.12.12] with 32 bytes of data:
Reply from 192.168.12.10: Destination host unreachable.
Reply from 192.168.12.10: Destination host unreachable.
Reply from 192.168.12.10: Destination host unreachable.
Reply from 192.168.12.10: Destination host unreachable.

Ping statistics for 192.168.12.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

Notice the error message returned states “Destination host unreachable”. This message sometimes indicates that the client in question does not exist on the network. This client, however, does exist. Look closely at the first line, specifically the IP address.

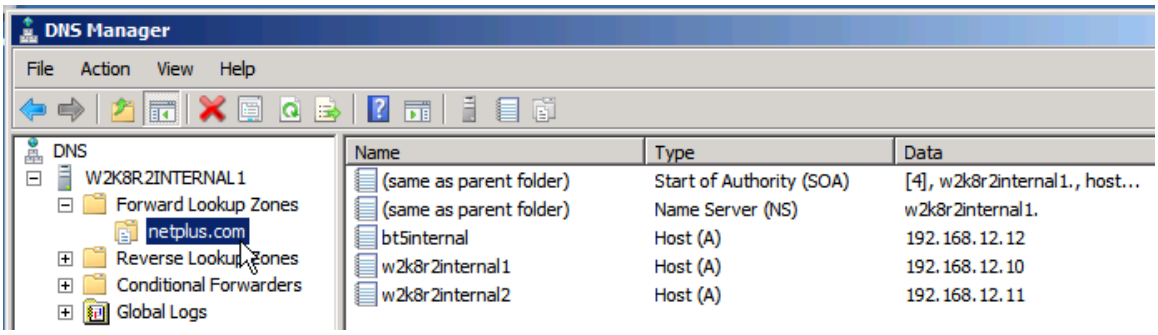
```
Pinging bt5internal.netplus.com [192.168.12.12]
```

In the previous task, a reservation was created for the BackTrack 5 Internal machine with an IP address of 192.168.12.151. However, when pinging the IP address by name, the DNS server resolves the name to an IP address, it comes up with its old address which is now invalid. To correct this error, changes must be made to the DNS records using the DNS console.

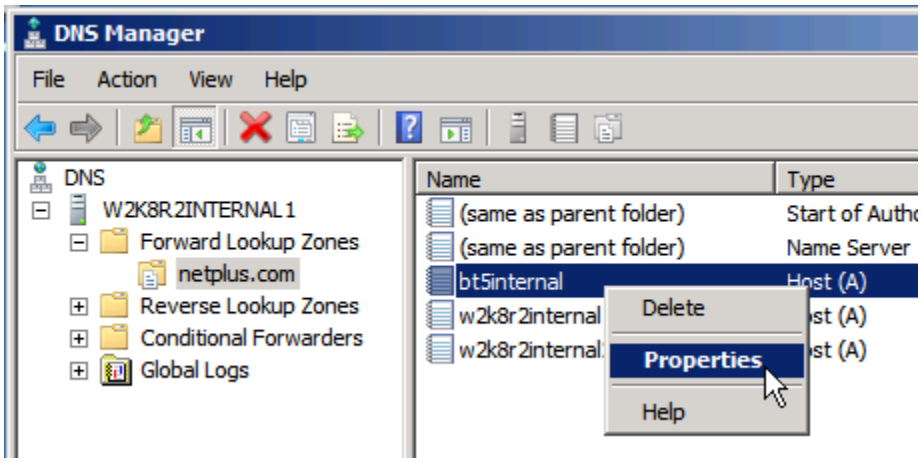
3. To open the DNS console on the Windows 2K8 R2 Internal 1 machine, click **Start**, point to **Administrative Tools** and click **DNS**.



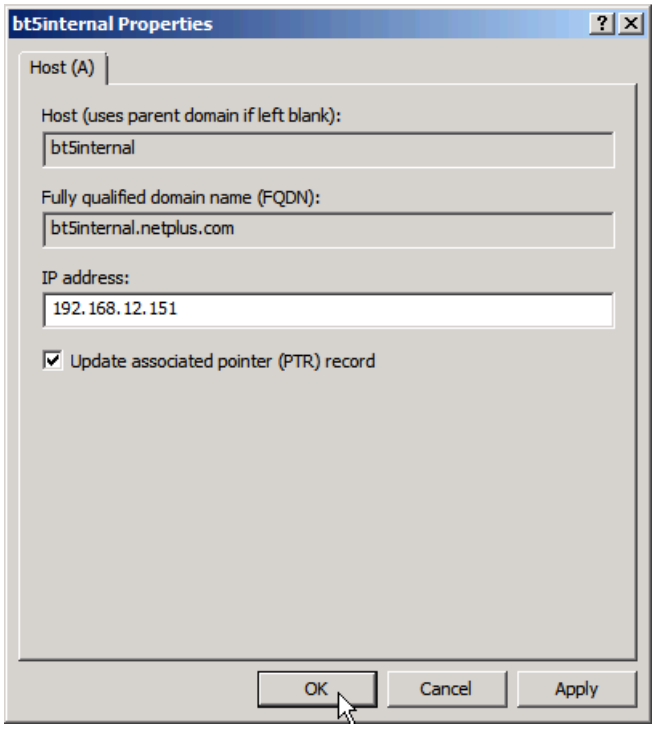
4. When the DNS Manager console appears, click the "**+**" next to **Forward Lookup Zones** in the left pane then click **netplus.com**. The records available for this zone are displayed in the right pane.



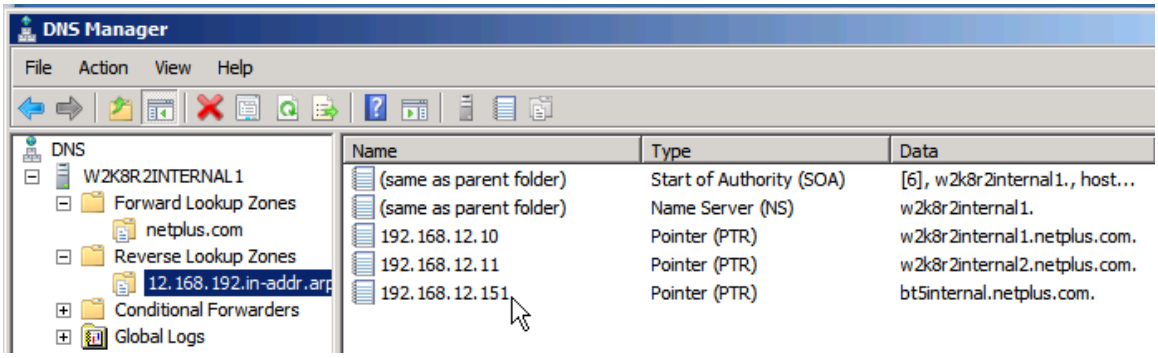
5. Notice the Host (A) record for the **bt5internal** machine. Had this record been automatically created by DHCP, it would have been updated when the DHCP server handed out its address. Since this record was manually created by an administrator, this record was not updated. To edit the record manually, right-click on the record and select **Properties**.



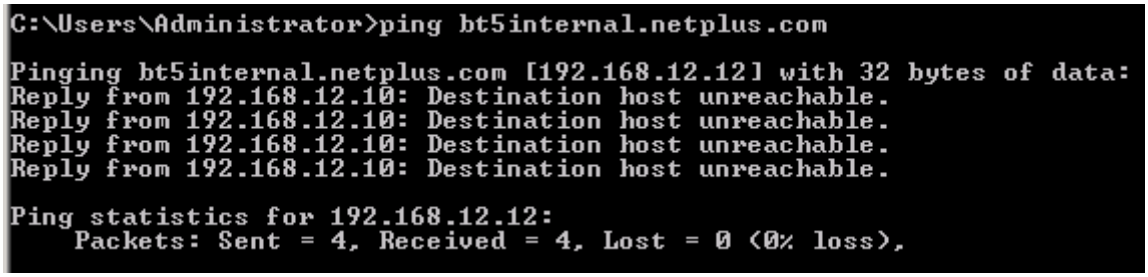
6. In the Properties window, change the IP address to match the IP address in the reservation, **192.168.12.151**. The machine's pointer (PTR) record (if it exists) can also be updated from this properties window. The PTR record exists in the reverse lookup zone and allows the machine's IP address to be used to resolve the name of the machine, hence why it is called a "reverse lookup". Put a check in the box to **Update associated pointer (PTR) record**. Once the information is correct, click **OK** to save it.



7. Notice the record is updated in the center pane. To verify the PTR record was also updated, click the "**+**" next to **Reverse Lookup Zones** in the left pane then select **12.168.192.in-addr.arpa**. If the record has not updated, click the **Action** menu and select **Refresh**. The record should be updated in the center pane.

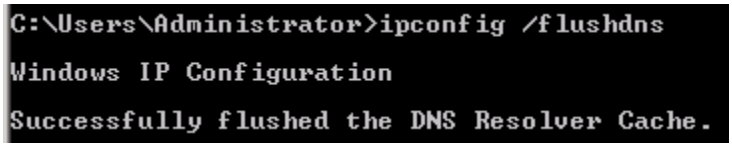


8. Test the updated DNS configuration by going back to the command prompt and pinging the BackTrack 5 machine by name once again. The ping fails once again with the same error and IP address.



The reason the ping fails this time is because of the DNS cache. When a domain name is resolved by DNS, your machine caches the information locally for a period of time to avoid having to ask the DNS server for the information again. This reduces the amount of load on the DNS server as well as traffic on the network. However, when changes are made to DNS records just like above, it can cause disruptions in network communications until the cache is cleared or times out.

9. To manually clear this cache, type the command **ipconfig /flushdns** in the command prompt window and press **Enter**. A message should appear stating the DNS resolver cache was successfully flushed.

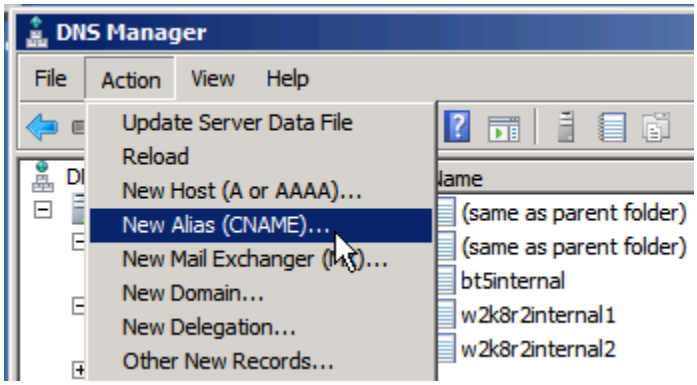


10. Try to ping the BackTrack 5 Internal machine once again. This time, the ping should be successful and resolve to the correct IP address.

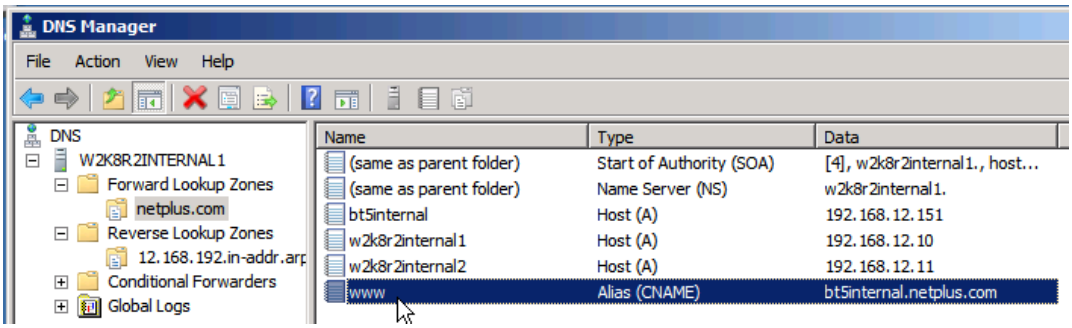
```
C:\Users\Administrator>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Users\Administrator>ping bt5internal.netplus.com

Pinging bt5internal.netplus.com [192.168.12.151] with 32 bytes of data:
Reply from 192.168.12.151: bytes=32 time<1ms TTL=64
Reply from 192.168.12.151: bytes=32 time<1ms TTL=64
Reply from 192.168.12.151: bytes=32 time<1ms TTL=64
Reply from 192.168.12.151: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.12.151:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

11. Administrators sometimes create Alias (CNAME) records for machines that allow them to respond to DNS names other than their primary hostname. This is common when a server may host a service such as web or ftp, for example. An administrator may create an alias to allow the machine to respond to the name "www" or "ftp" instead of its configured hostname. For this example, assume the administrator is going to make the BackTrack 5 Internal machine a web server. Therefore, an alias needs to be created to allow it to respond the name "www".

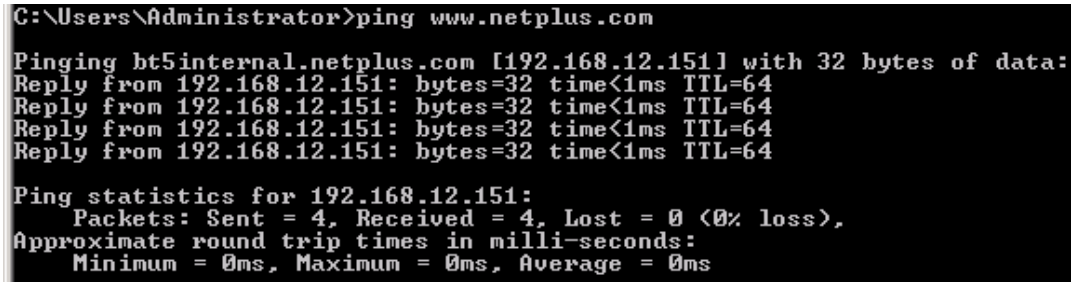
    In the DNS Manager console, click **netplus.com** under **Forward Lookup Zones**. With the **netplus.com** zone selected, click the **Action** menu and select **New Alias (CNAME)…**



12. For the **Alias name** type **www**. Notice this alias is appended to the domain name, netplus.com, to create the FQDN of www.netplus.com. Type the FQDN of the BackTrack 5 Internal machine, **bt5internal.netplus.com**, into the dialog box labeled **Fully qualified domain name (FQDN) for target host**. Alternatively, the **Browse** button could have been used to select the appropriate record from the list. Once the information on the screen is correct, click **OK** to create the record. The record now appears in the right pane.

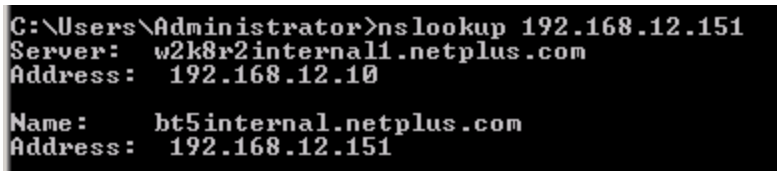


13. Test the new record by going back to the command prompt and pinging the new FQDN, www.netplus.com.



Notice the name of the machine is resolved along with the correct IP address. Here's why… the DNS server first looks up the name www.netplus.com. When the DNS server finds a record for this name, it realizes it is an Alias (CNAME) record with the FQDN of the machine it represents. The server must then find the Host (A) record associated with that FQDN. Once a record is found, the IP address along with the FQDN of the actual host is returned and the ping is attempted.

14. To test the Pointer (PTR) record in the reverse lookup zone, the **nslookup** command must be used. This command is useful for finding DNS information or additional aliases associated with a machine. At the command prompt window, type the command **nslookup 192.168.12.151** and press **Enter**. Notice the IP address successfully resolves to the BackTrack 5 Internal machine.



15. Close all open windows.

3.2 Conclusion

Domain Name System (DNS) is the protocol in the TCP/IP suite that allows end users to have the capability to remember names for clients instead of their IP addresses (which can change). DNS servers provide the name-to-IP address translations necessary to allow communication across TCP/IP networks. If configured properly, they can also provide the reverse IP address-to-name translations.

3.3 Review Questions

1. *What number is associated with the DNS server option?*
2. *What number is associated with the domain name?*
3. *What command clears the DNS cache on a Windows machine?*
4. *What is another name for an A record?*
5. *What is another name for a CNAME record?*