CompTIA Network+® Lab Series
Network Concepts

Lab 2: Types of Networks

Objective 1.5: Identify common TCP and UDP default ports
Objective 1.6: Explain the function of common networking protocols

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 identify common functions of peer-to-peer and client/server networks. Students will create and access file and print shares in various ways, as well as access web and FTP resources.

This lab includes the following tasks:

1. Create a Shared File
2. Testing the Share and Re-assigning Permissions
3. Map a Drive to a Server
4. Sharing a Printer
5. Installing the Shared Printer
6. Accessing a Web and FTP Server

Objective: Identifying Common Network Types and Functions

Networks provide many useful functions. Some of these functions include sharing resources such as files and printers. In a peer-to-peer network, the sharing of resources is controlled by each individual user and computer. While they are easy to set up and are convenient for home users, they do not scale well. Client/server networks are more complex, but provide better security and scale better for enterprise networks. Networks can also provide access to resources over the Internet, such as web and FTP sites.

Key terms for this lab:

Peer-to-peer network – a network type where two or more computers share resources (such as files or printers) and each computer in the network is responsible for their own access and security. These networks are simpler and cheaper than client/server networks but are less efficient when many users exist or large amounts of resources need to be shared

Client/server network – a network where one centralized computer (called a server) controls access and security to shared resources. Other computers (called clients) connect to this central server to access shared resources

Simple file sharing – a wizard-based file sharing method that enables non-technical users the ability to easily share files over the network

Advanced file sharing – a file sharing method used by administrators to provide more granular control of shared files over the network

Universal Naming Convention (UNC) – a standard for identifying shared resources over the network. The UNC path uses double backslashes to precede the computer name then single backslashes to separate the shared path to the resource. UNC names do not use drive letters to identify resources

Permissions – the rights granted to a user or group to access a resource

New Technology File System (NTFS) – the primary Windows file system. NTFS includes its own set of file/folder permissions.

Line Print Terminal (LPT) – the logical named assigned to the parallel port on a PC. Parallel ports were typically used to attach local printers although they have become obsolete and replaced with USB

Universal Serial Bus (USB) – a type of serial interface that is used to connect peripheral devices to a PC

HyperText Markup Language (HTML) – the language used for documents on the World Wide Web

HyperText Transfer Protocol (HTTP) – the protocol used to transfer web files over the Internet. HTTP uses TCP port 80 for initiating requests

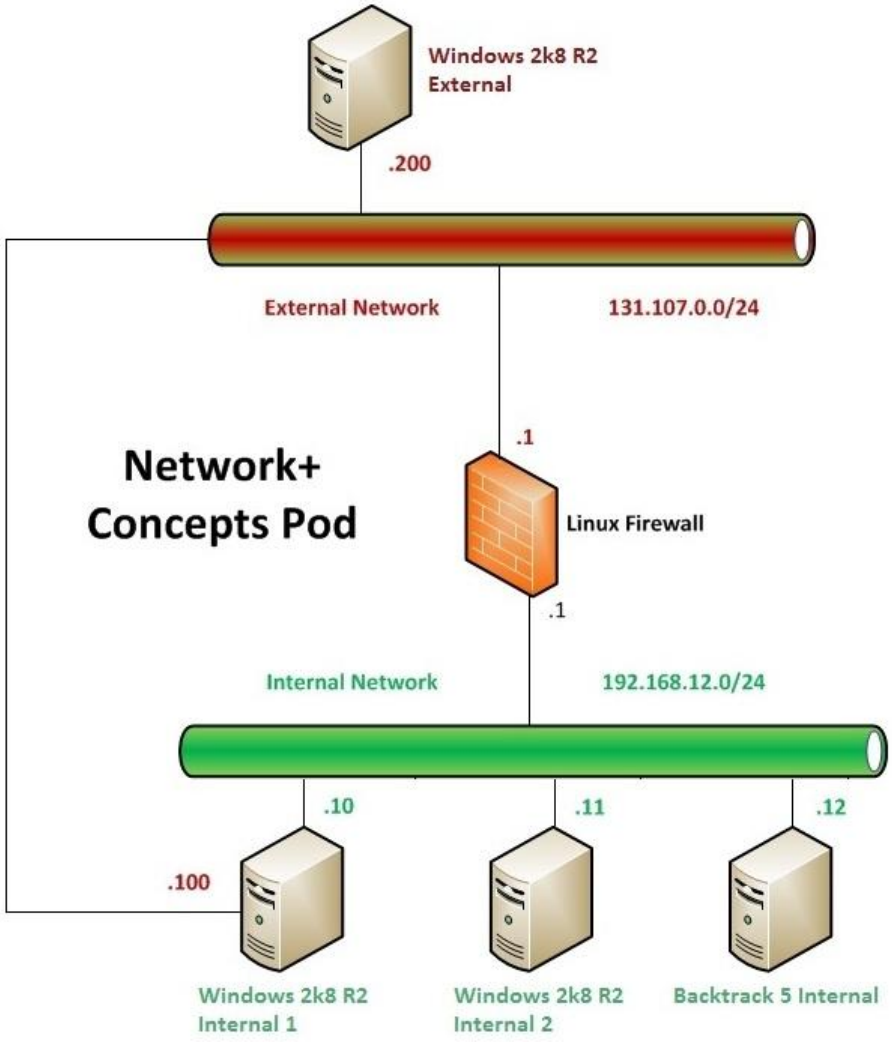
Universal Resource Locator (URL) – the named address of a resource on the Internet

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

File Transfer Protocol (FTP) – the protocol used to send and receive files from another computer on the Internet. FTP uses TCP port 21 to set up the exchange process and TCP port 20 to exchange the actual data

Internet Information Services (IIS) – Microsoft's web server

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.

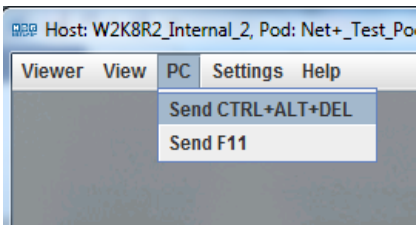
Required Virtual Machines and Applications

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

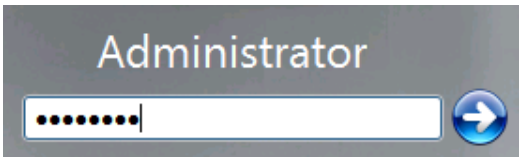
Windows 2k8 R2 Internal 1	192.168.12.10
Windows 2k8 R2 Internal 1 password	P@ssw0rd
Windows 2k8 R2 Internal 2	192.168.12.11
Windows 2k8 R2 Internal 2 password	P@ssw0rd

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 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.



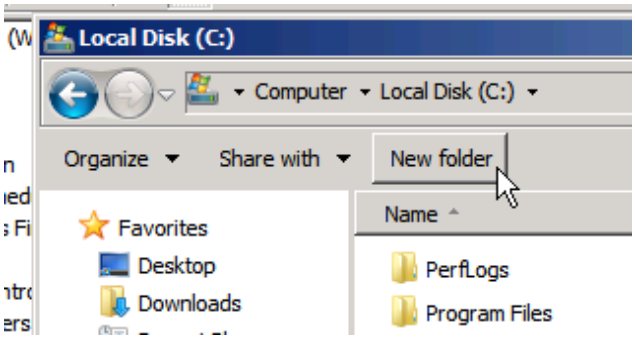
4. If the Initial Configuration Tasks and/or Server Manager windows appear, close them by clicking on the "**X**" in the top-right corner of the window

1 Sharing Files

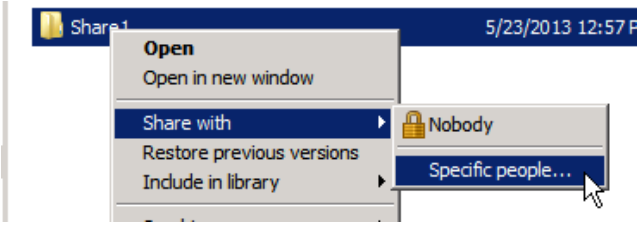
Networks provide many useful functions, including sharing resources such as files and printers. Sharing files over the network makes it easier for users to access and collaborate on files. It also prevents users from becoming confused when multiple copies of a file exist on many different machines.

1.1 Create a Shared File

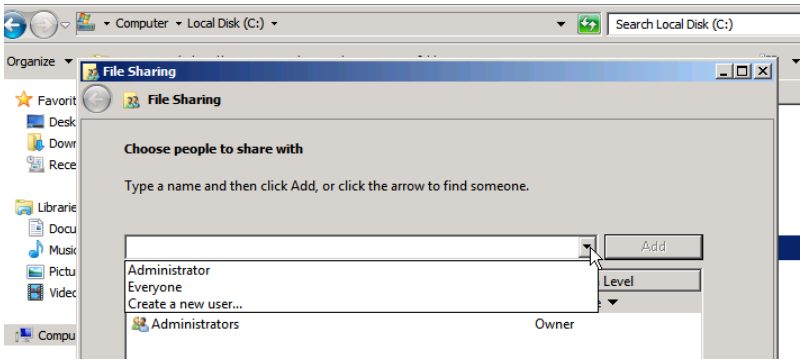
1. Use the instructions provided in the Lab Settings section to log into the Windows 2k8 R2 Internal 2 machine, if you are not logged in already.
2. Click on **Start -> Computer**. Double-click on **Local Disk (C:)** to view the contents of the hard drive.
3. Create a new folder by clicking the **New Folder** button. Name the folder **Share1.**



4. Share the folder by first right-clicking on it. In the context menu, select **Share with -> Specific People**. This is considered simple file sharing. Many home users prefer this interface because it requires little technical knowledge and provides a wizard interface for the user to follow and complete the share.



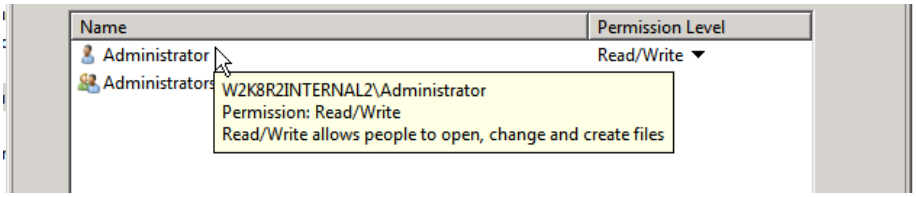
5. When the File Sharing wizard appears, click the down arrow to the left of the **Add** button. This is where you can select additional users to share the folder with. Remember that when you are sharing folders between computers that are not part of a domain, users must have an account on each computer they wish to access. If you do not see the user account you need, this wizard provides you with the option to **Create a new user…** Deselect this drop-down menu by clicking on another part of the File Sharing window.



6. Hover your mouse over the **Administrator** account name but do not click on it. A dialog box will appear showing you the full username, the current permission level and a brief description of what those permissions allow. Notice that the **Administrator** user currently has **Read/Write** permissions. These permissions allow this user to open, change and create files. Under the **Permission Level** heading, click the down arrow next to **Read/Write**. Change the permission level to **Read**. Hover your mouse once again over the **Administrator** account name.

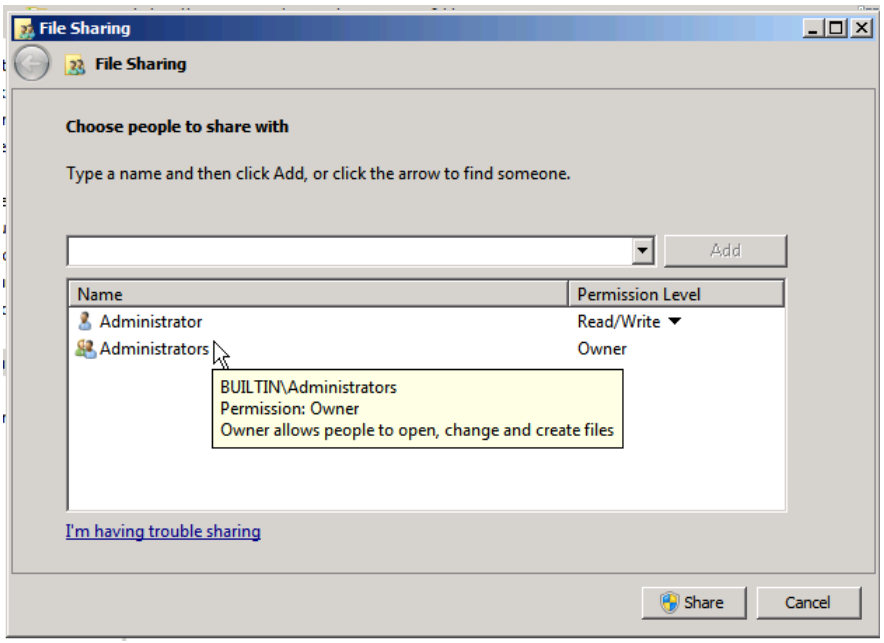
    1 *What does the **Read** permission allow a user to do?*

    Change the permissions back to the default of **Read/Write**.

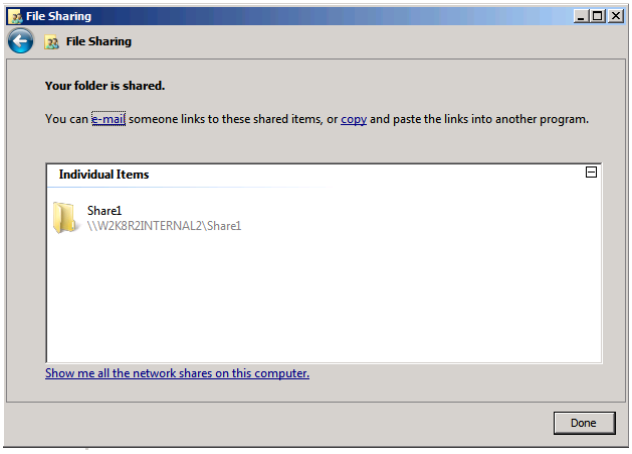


7. Notice the permission for the **Administrators** group is **Owner**. The owner always has full access to a file or folder even if all permissions have been removed for all users. This prevents a file or folder from becoming "widowed" (existing without anyone having permission to access it or its settings). Hover your mouse over the **Administrators** group name to display the dialog box. Notice the owner has the same access as the **Administrator** user with **Read/Write** permissions. Also notice that there is no drop down arrow next to **Owner,** so you cannot change the **Owner** permission in this wizard. It is recommended that only an administrator with a firm understanding of the consequences change the owner

of a file or folder. Ensure that all settings are in their default state then click the **Share** button at the bottom of the screen.



8. Once the folder is shared, you have the option to email someone the links to these shared items or copy and paste the links into another program. Notice the path listed next to the folder icon - **\\W2K8R2INTERNAL2\Share1**. This is known as the Universal Naming Convention (UNC) path. The double backslashes indicate the shared resource is located on the network. The next part is the computer name (W2K8R2INTERNAL2). The second backslash is followed by the shared folder name (Share1). Typing this path into the **Run** dialog box on another machine will cause that machine to attempt to connect to the **Share1** folder.
9. Click **Done** to complete the wizard. You have successfully shared the **Share1** folder. Leave this machine logged on, as you will need it for the next task.



1.2 Conclusion

Sharing files over the network makes it easier for users to access data and collaborate. Simple file sharing is useful for users with little technical knowledge as the wizard interface makes the process easy for users.

1.3 Review Questions

1. *Using the File Sharing wizard is known as what type of file sharing?*

2. *The creator of a file always has full access to the file regardless of other permissions. This account is also known as the_____ of the file.*

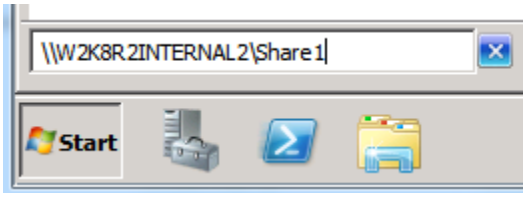
3. *The path \\W2K8R2INTERNAL2\Share1 is also known as the _____ path.*

2 Share Permissions

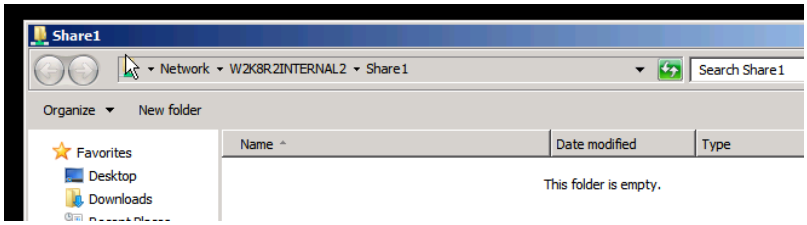
Sharing files over the network makes it easier for users to access data and collaborate. Permissions are used to control access to files. Users can be granted permission to read (view) a file and/or write (change) a file. Unauthorized users are not allowed to access the files at all.

2.1 Testing the Share and Re-assigning Permissions

1. Using the instructions in the Lab Settings section, log onto the Windows 2k8 R2 Internal 1 machine, if you are not logged in already.
2. Test the share you created in the first task. Click **Start** and in the **Search programs and files** text box, type the UNC path of the shared folder - **\\W2K8R2INTERNAL2\Share1** - and press **Enter**.

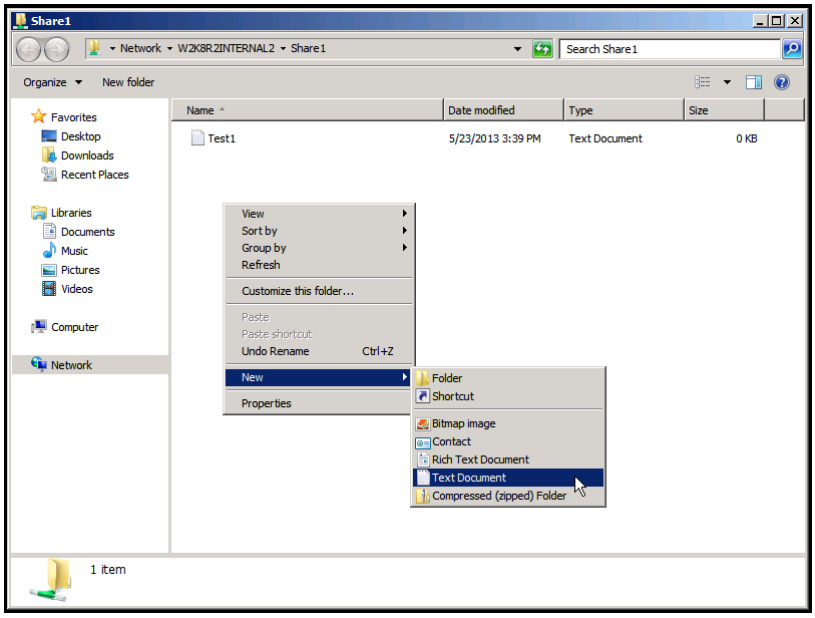


3. A Windows Explorer window appears, displaying the empty shared folder. Notice that you were not prompted for a username/password to access the folder. The reason for this is because the credentials you entered when you logged onto the Windows 2k8 R2 Internal 1 machine are the exact same as the credentials needed to access the Share1 folder on the Windows 2k8 R2 Internal 2 machine.

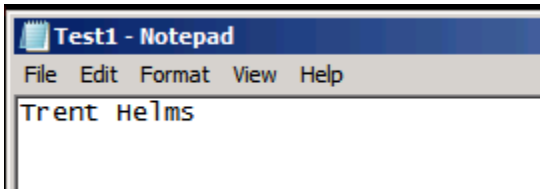


4. Create a file in the Share1 folder. Right-click in the right pane of the Explorer window. In the context menu that appears, select **New -> Text Document**. Name the file **Test1**.

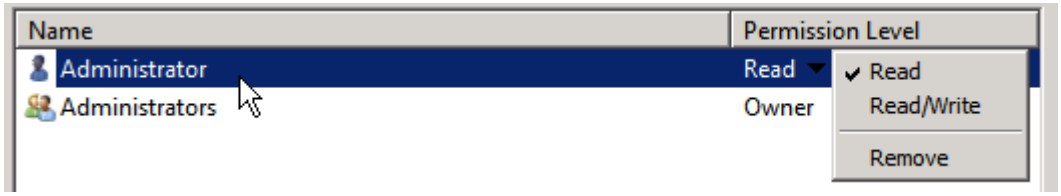
    1. *Why were you able to create the file?*



5. Open the Test1.txt file by double-clicking on it. Type your name into the file and save it by clicking **File -> Save**. You are permitted to do so based on the permissions set for the Administrator account.



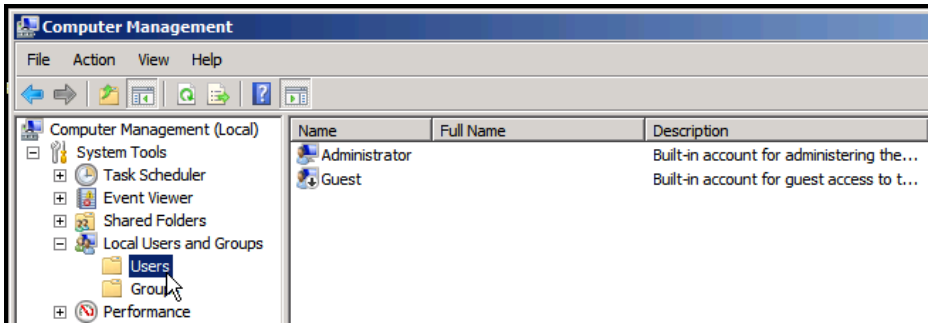
6. On the Windows 2k8 R2 Internal 2 machine, right-click on the **Share1** folder and select **Share with -> Specific people…**
7. When the **File Sharing** wizard appears, click the down arrow next to the **Administrator** account and change the permissions to **Read**. Click **Share** and **Done** to complete the changes.



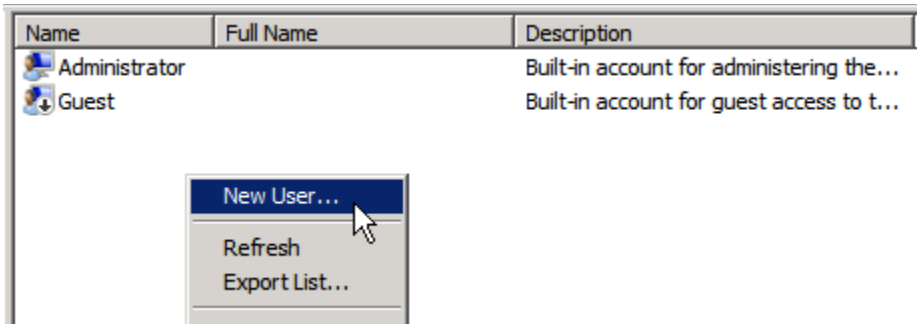
8. Back on the Windows 2k8 R2 Internal 1 machine, open the **Test1.txt** file, edit it and save it once again.

    2. *Why are you able to save your changes even though you only allowed the "read" permission?*

9. Close the **Test1.txt** file.
10. Create a new account on both machines called **ShareTest**.
    a. To do this, click on the **Start** menu, point to **Administrative Tools** and select **Computer Management**.
    b. Click the **+** sign next to **Local Users and Groups** in the left column to expand it.
    c. Click on the **Users** folder to display the current user accounts in the middle column.

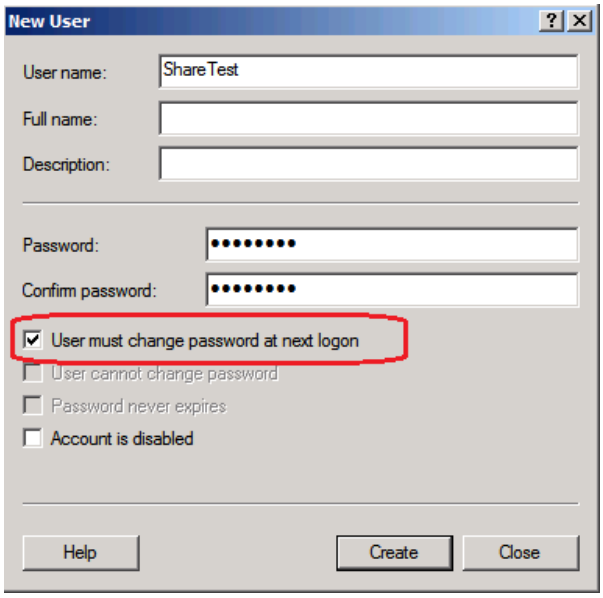


    d. Right-click within the white space in the middle column and in the context menu select **New User…**



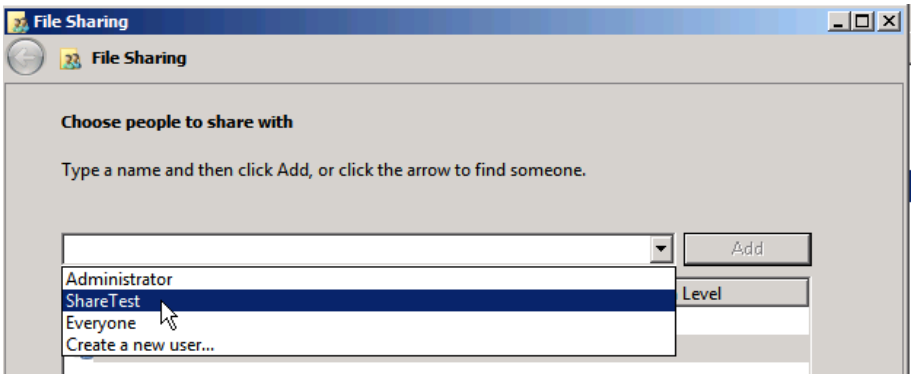
e. When the **New User** dialog box appears, type **ShareTest** for the User name. Type **P@ssw0rd** in the **Password** and **Confirm Password** dialog boxes. Clear the check next to **User must change password at next logon**. Once you have verified your settings, click **Create** to add the user account.

The account will not immediately appear once the button is clicked. You must click **Close** to exit the **New User** dialog before the account will appear.



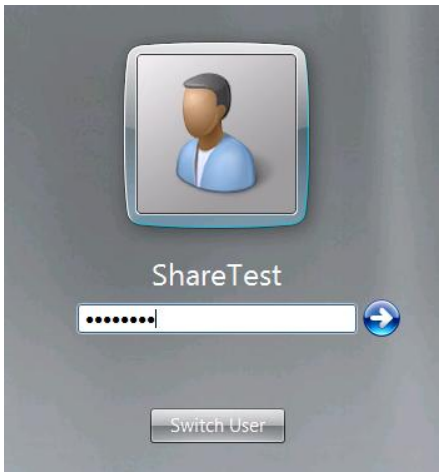
f. Complete the same steps on the other Windows 2k8 R2 Internal machine. Be sure that you use the exact same credentials when creating the second account. Once the accounts have been created, close the **Computer Management** dialog boxes.

11. On the Windows 2k8 R2 Internal 2 machine, right-click on the **Share1** folder and select **Share with -> Specific people…** Add the new **ShareTest** user to the share by clicking the drop-down arrow to the left of the **Add** button and selecting the **ShareTest** user from the list. Click the **Add** button to add the user to the list.

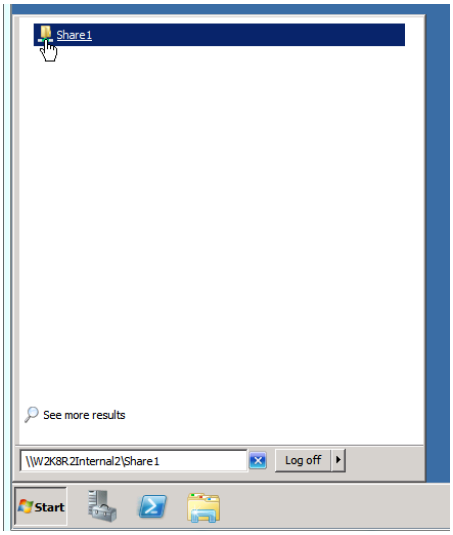


Notice that the default permission for this account is **Read**. Leave this as default and click **Share** and **Done** to add this user to the share.

5. Back on the Windows 2k8 R2 Internal 1 machine, log out of the **Administrator** account by clicking **Start -> Log off**.
6. 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).
12. Log in as **ShareTest** by clicking on the username, typing the password of **P@ssw0rd** and pressing **Enter** to log in.



13. Access the **Share1** folder by clicking **Start** and typing the UNC path **\\W2K8R2Internal2\Share1** in the **Search programs and files** text box.



14. Open the **Test1.txt** file and add some text to change it. Attempt to save the edited file as the same name.

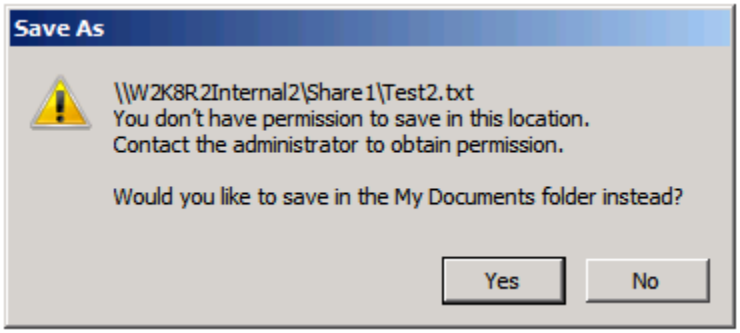
    3. *What error do you receive?*

15. Attempt to save the file as **Test2.txt**.

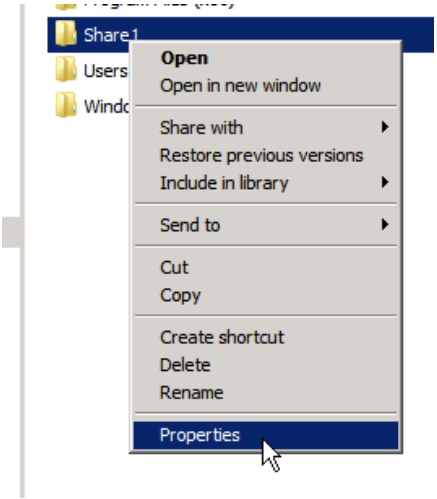
    4. *What error do you receive this time?*

    5. *Why do you receive these errors?*

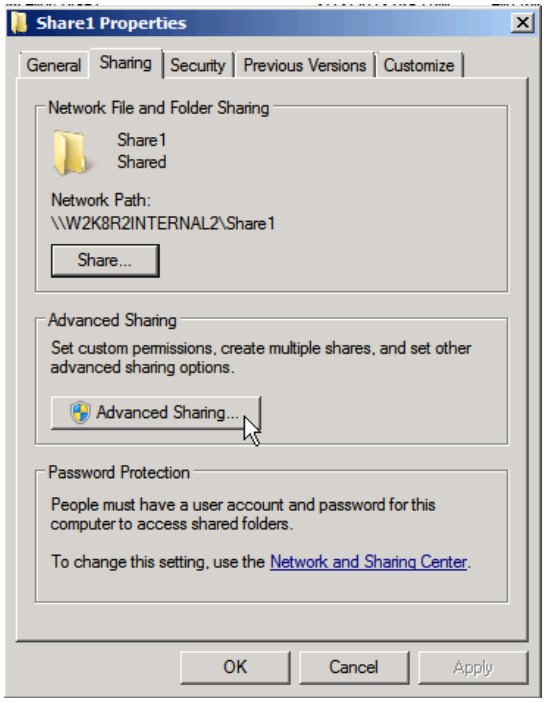
16. Click **No** to cancel the save then close all windows EXCEPT the **Share1** folder.



17. The Simple File Sharing method you have been using only allows you to set **Read** or **Read/Write** share permissions. The Advanced File Sharing method will also allow you to set a special permission known as **Full Control**. This permission will allow a user to not only access and change all files' contents, but also to change attributes such as the owner of a file or folder.
    a. To access the Advanced File Sharing return to the Windows 2k8 R2 Internal 2 machine, right-click on the **Share1** folder and select **Properties**.

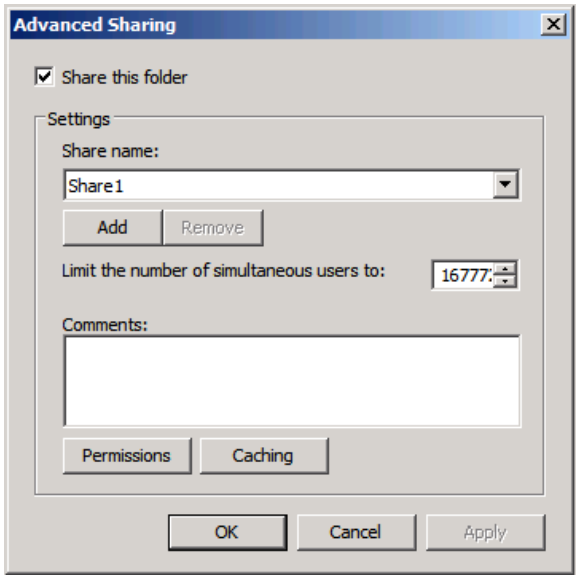


b. When the **Share1 Properties** dialog box appears, click on the **Sharing** tab at the top. Click the **Advanced Sharing** button in the middle of the dialog box.

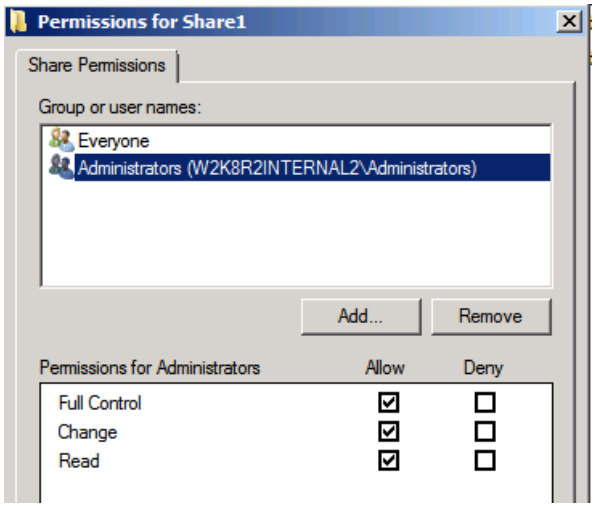


c. When the **Advanced Sharing** dialog box appears, notice the check in the box next to **Share this folder** and the Share name **Share1 under the Settings heading.**. These are filled in as a result of the Simple File Sharing wizard earlier.

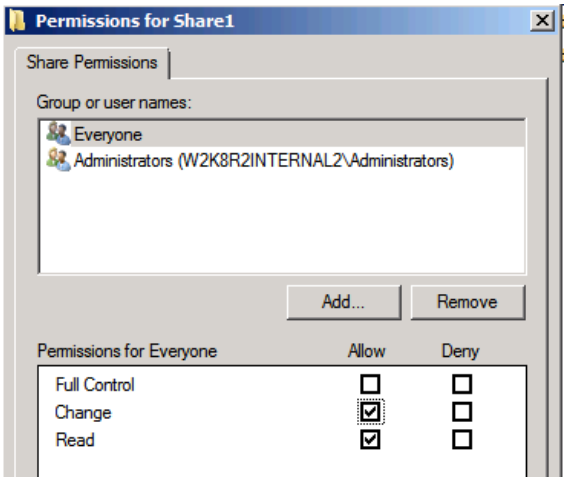
d. To access the permissions for this share, click the **Permissions** button.



e. In the **Permissions for Share1** dialog box, you can view/edit permissions for current users or add/remove users from the share. Click on the **Administrators** group. Notice the current permissions are set to **Full Control** as all of the boxes next to the permissions are checked. This is because this group was listed as the "Owner" for this share.

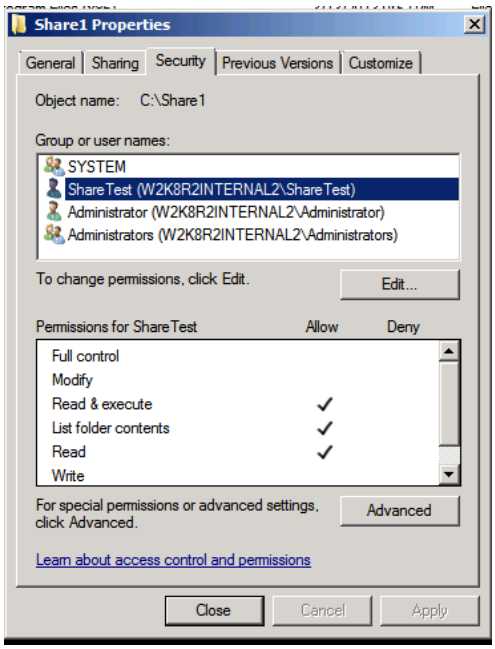


f. Click on the **Everyone** special identify. This identity is a "group" built into Windows that automatically includes all users and groups. Configure the **Everyone** special identity with the **Change** permission by checking the Deny check box for Full Control and putting a check under the **Allow** column for Change. Notice this also adds a check to the Read permission check box. This is the equivalent to the **Read/Write** permission in the Simple File Sharing wizard.

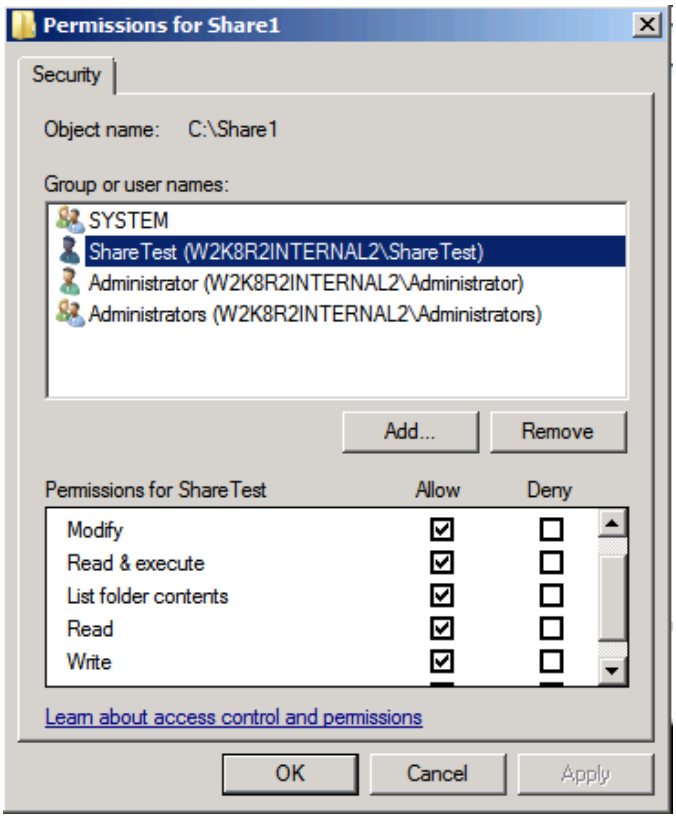


g. Click **OK** on all open dialog boxes to save your changes to the share permissions. Leave the **Share1 Properties** dialog box open.

18. On the Windows 2k8 R2 Internal 1 machine, access the share once again and attempt to create a new file or folder. After giving the **Everyone** special identity **Change** permissions one would expect to be able to Read/Write to the folder, but access to a folder on a file server can be determined through two sets of permission types: the share permissions set on a folder and the NTFS permissions set on the folder. In this case the shared folder resides on an NTFS volume, which affects local access and remote access. The NTFS permissions on that volume also apply to the share folder. When both sets of permissions are applied (share and NTFS), the most restrictive permissions will be enforced. Given that we know the share permissions are set to **Change** but we are still not able to create new files/folders, the NTFS permissions must be preventing us from being able to do so.
19. Check the NTFS permissions on the Windows 2k8 R2 Internal 2 machine by clicking on the **Security** tab in the **Share1 Properties** dialog box. Click on the **ShareTest** account to display the current NTFS permissions. Notice that you have more options for permissions with NTFS. This granularity is why many administrators prefer to set permissions using NTFS instead of just using share permissions. In this example, notice that the **ShareTest** user only has **Read**, **List folder contents** and **Read & Execute** permissions. While this set of permissions will allow you to access the **Share1** folder and its contents, it will not allow you to make any changes.



20. Click the **Edit** button. Select the **ShareTest** user and put a check in the box next to the **Modify** permission under the **Allow** column. Notice that checking this box also checks the **Write** permission. The difference between these permissions is that the **Write** permission allows you to change the contents of a file while **Modify** also allows you to change the attributes of the file. Click **OK** to save the changes made to the permissions for the **ShareTest** user.



21. Back on the Windows 2k8 R2 Internal 1 machine, attempt to create a new file or folder. This time, you are successful because all of the permissions (both share and NTFS) permit you to do so.
22. Close all open windows on both Windows 2k8 R2 Internal machines.

2.2 Conclusion

Sharing files over the network makes it easier for users to access data and collaborate. Permissions are used to control access to files. Users can be granted permission to read (view) a file and/or write (change) a file. Unauthorized users are not allowed to access the files at all.

2.3 Review Questions

1. *What share permission level only allows a user to view files and folders in a share?*

2. *What share permission level allows a user to view and change files and folders in a share?*

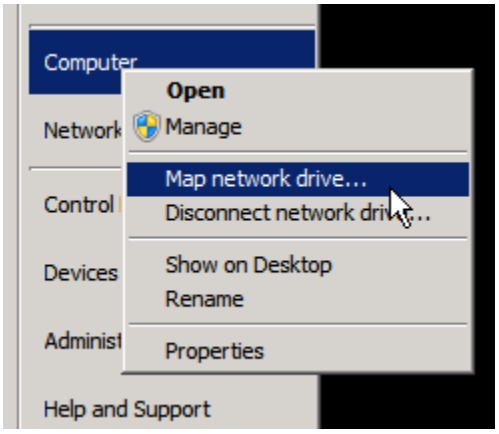
3. *If a share resides on an NTFS volume, which set of permissions take effect?*

3 Mapping a Drive

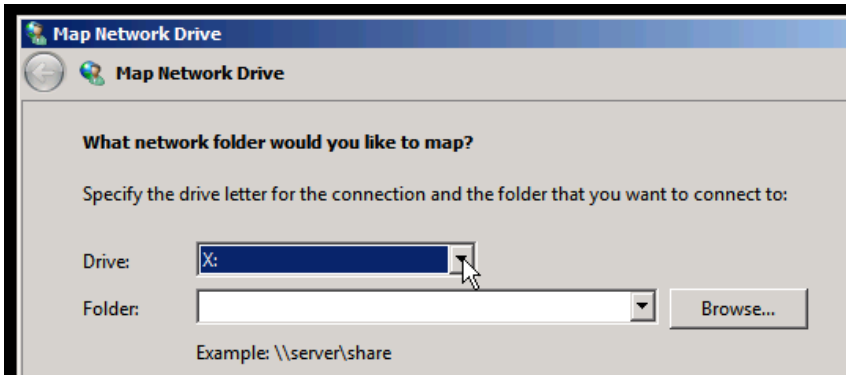
Another way to access shares is by mapping a drive. This is typical in client/server environments so clients don't constantly have to type in the share path to the folder. Mapped drives can also be deployed through group policy so the process is seamless to the end-user. When shares are mapped, they are associated with a drive letter in **Computer** (see section below) and accessed just like any other local drive on the computer.

3.1 Map a Drive to a Server

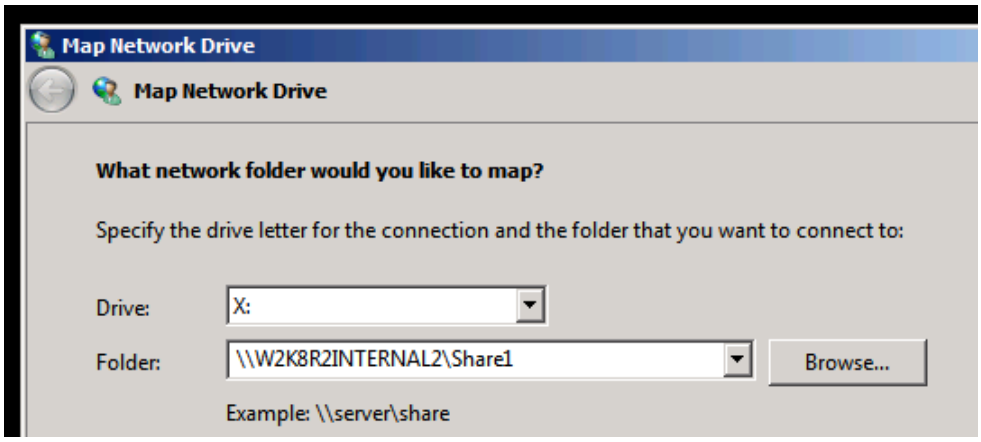
1. On the Windows 2k8 R2 Internal 1 machine, click **Start** and right-click **Computer**. In the context menu that appears, select **Map network drive…**



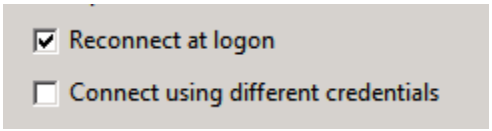
2. In the Map Network Drive dialog box, the **Drive:** dropdown menu allows you to select the letter you want to associate with the mapped share. You can choose any available letter from A-Z. Notice that the letters already assigned to a resource are not in the list. Also, drive letters are only locally significant meaning that the letter one user chooses to map to a share does not have to be the same letter someone else chooses to map to the same share. From the dropdown list, select **X:**



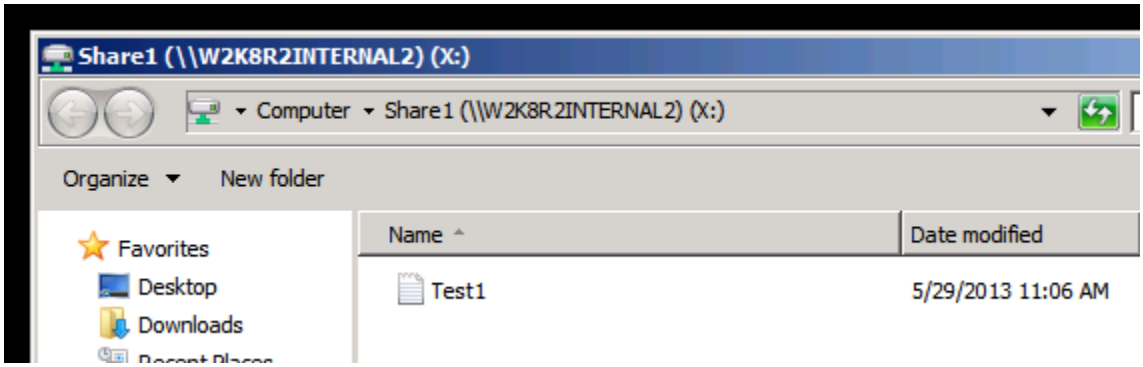
3. The **Folder** textbox is where you type the share path. Enter the following in the textbox: **\\W2K8R2INTERNAL2\Share1**



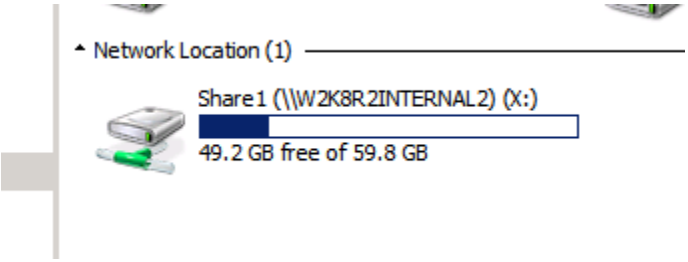
4. The **Reconnect at logon** checkbox will automatically map the share every time the user logs in. If you will need to constantly access the share, this is a good option. If you are only using the share once or very infrequently, you may want to uncheck the box. For this example, leave this option checked. If you check the box for **Connect using different credentials**, you can specify what username/password combination you want to authenticate with. This would be useful if you were attempting to access a share on a computer where you did not have an account. In a typical client/server environment, clients will typically have a domain account that would allow them to log in on any computer. Therefore, this option could be used to access a share your account doesn't have permission to access. Since the user we are currently logged in as has permission to access the share, we will leave this box unchecked.



5. Click **Finish** to map the drive. An explorer window will open displaying the contents of the drive. Notice the letter at the top of the window.



6. Click **Computer** on the left column. Notice the mapped drive shows up just like a local drive. However, we know it is shared because 1) it shows up under the **Network Location** heading, 2) the icon showing a network connection and 3) the share path shows up next to the drive letter.



7. Close all open windows on the Windows 2k8 R2 Internal 1 machine.

3.2 Conclusion

Another way to access shares is by mapping a drive. This is typical in client/server environments so clients don't constantly have to type in the share path to the folder. Mapped drives can also be deployed through group policy so the process is seamless to the end-user. When shares are mapped, they are associated with a drive letter in on the computer and accessed just like any other local drive on the computer.

3.3 Review Questions

1. *When mapping a drive, what option will cause the drive to automatically reappear the next time you log in?*

2. *How can you map a drive if the user you are currently logged in as does not have access to the shared folder?*

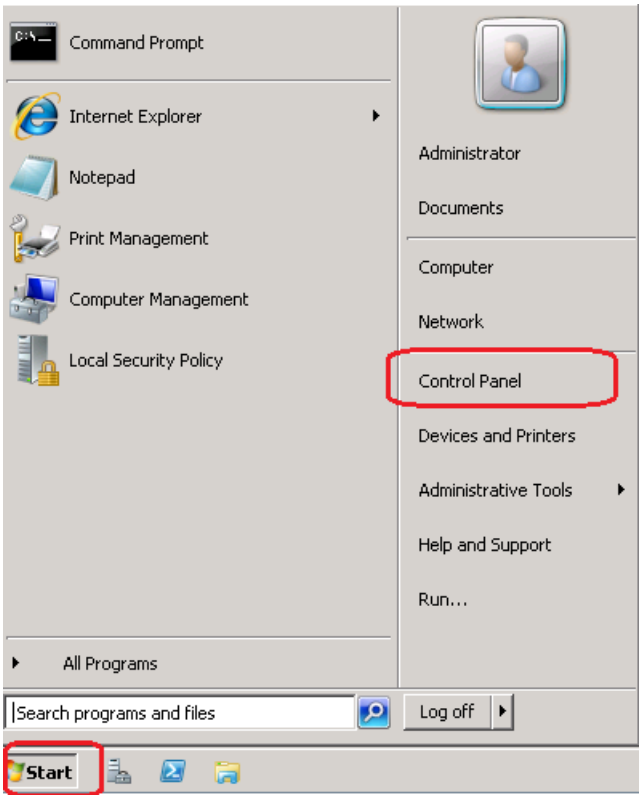
3. *True or false? Mapped drives must have the same drive letter on all machines accessing the shared folder.*

4 Sharing Printers

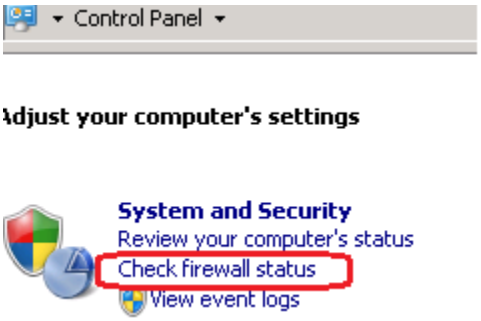
Another use for networks is sharing printers. In a peer-to-peer network, this consists of installing the printer on one peer, sharing it on the network and installing it on the other peer. On a client/server network, the process is nearly the same, but permissions to the printer are centrally controlled on the server.

4.1 Sharing a Printer

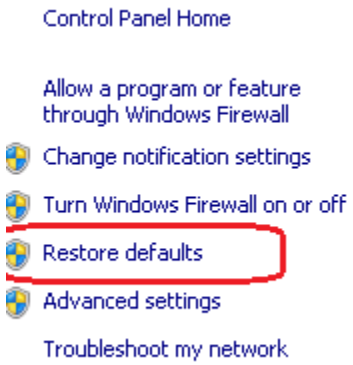
1. On the Windows 2k8 R2 Internal 2 machine, click **Start** and select **Control Panel.**



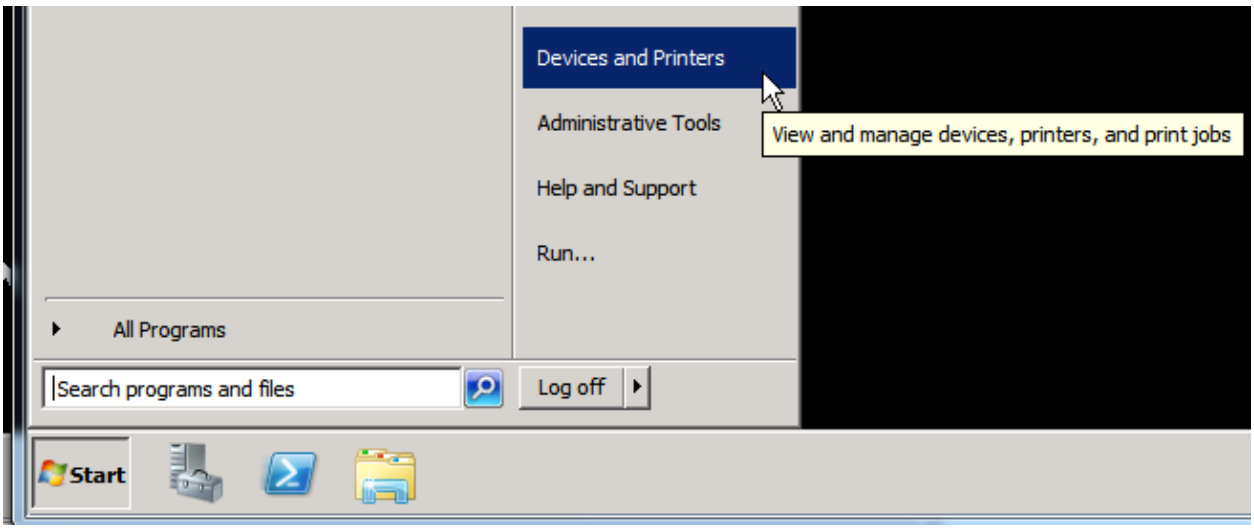
2. In the Control Panel window, click on the **Check Firewall Status** link under the **System and Security** heading.



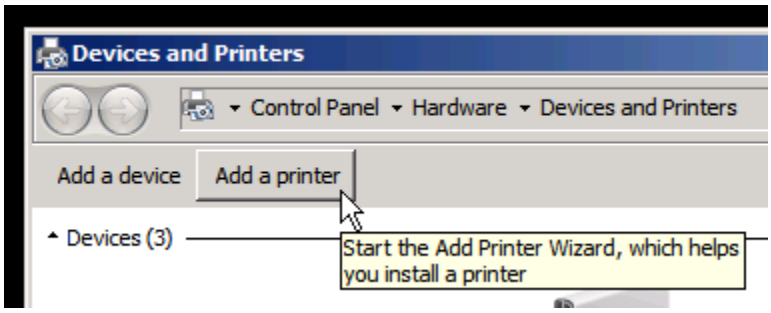
3. On the left side of the page, click on **Restore Defaults.**



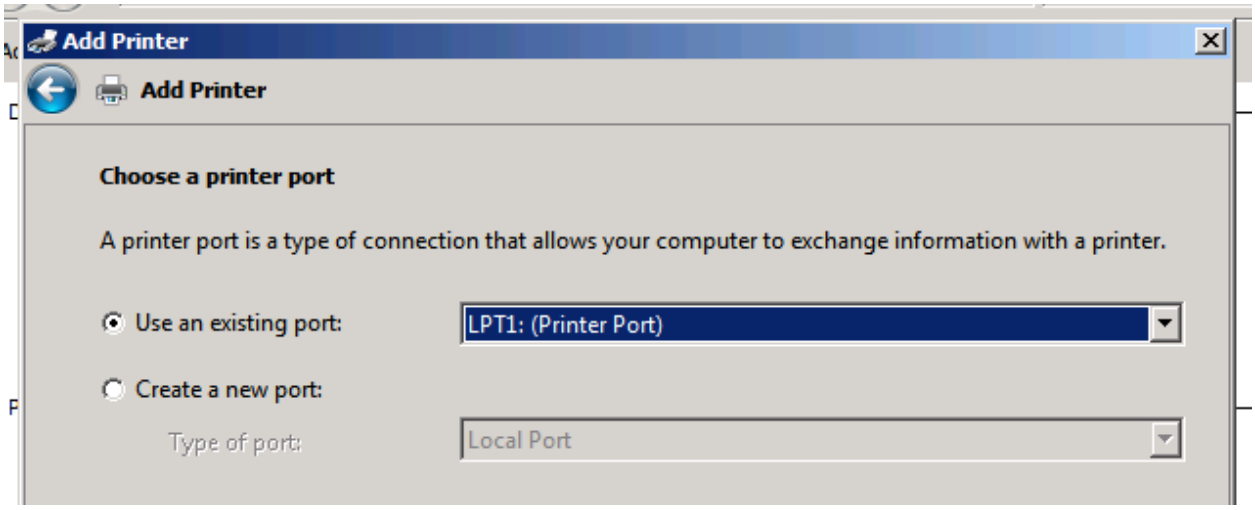
4. You will need to click on **Use recommended settings** and then on the Restore Defaults Settings page click on the **Restore Defaults** button. Click on **Yes** when asked to confirm your choice.
5. An error may occur if you have stopped or disabled the Windows Firewall Service. To share printers in Windows 7 or in Windows Server 2008 R2, you must have the Windows Firewall Service enabled, which is why the previous steps are necessary before you can begin sharing the printer.
6. On the Windows 2k8 R2 Internal 2 machine, click **Start** and select **Devices and Printers**.



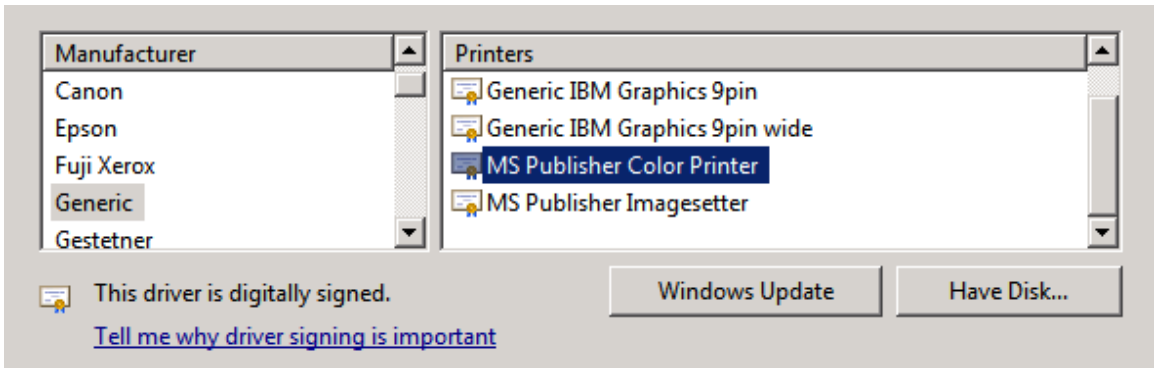
7. In the **Devices and Printers** dialog box, click **Add a printer**.



8. In the **Add Printer** wizard, choose the option **Add a local printer**. On a peer-to-peer network, the printer will typically be connected to a local port such as LPT or USB. The printer could also have its own IP address. In this example, we will use the local LPT port so leave the default and click **Next**.

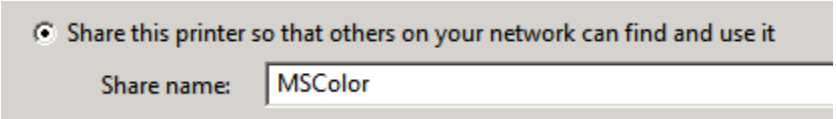


9. In the **Manufacturer** list, choose the option for **Generic**. Then under the list of Printers, choose the option for **MS Publisher Color Printer**. If you had a disk from the manufacturer, you could select the option **Have Disk**. With the options selected, click **Next**.



10. When asked which version of the driver to use, leave the default driver that is currently installed. Click **Next**.
11. Leave the default name and click **Next**.

12. Once the printer driver installs, you will be asked if you want to share the printer. Sharing the printer allows others to see the printer on the network and install it as if it were a local printer. Select the **Share this printer so that others on your network can find and use it**, change the default share name to **MSColor** and click **Next**.



13. Click **Finish** to close the wizard. If you click on the printer in the **Devices and Printers** dialog window, you will notice the state is shared.

14. Close all open windows on the Windows 2k8 R2 Internal 2 machine.

4.2 Conclusion

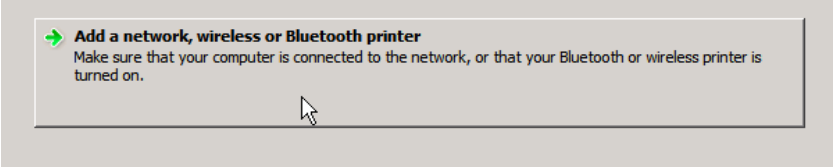
Another use for networks is sharing printers. In a peer-to-peer network, this consists of installing the printer on one peer, sharing it on the network and installing it on the other peer. On a client/server network, the process is nearly the same, but permissions to the printer are centrally controlled on the server.

5 Installing the Shared Printer

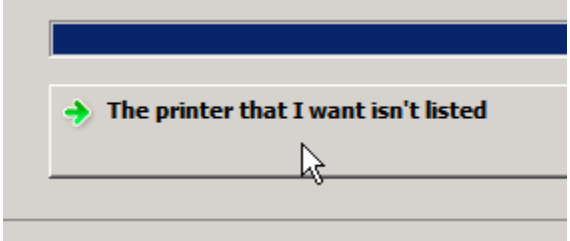
Now we will install the shared printer on another machine. Installing the shared printer will allow the other machine to use the printer like it was a locally attached device and have the ability to control its own access and settings.

5.1 Installing the Shared Printer on a Remote Computer

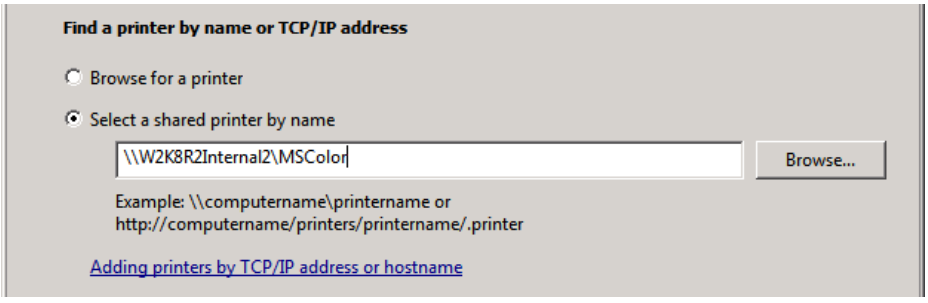
1. On the Windows 2k8 R2 Internal 1 machine, click **Start** and select **Devices and Printers**. In the **Devices and Printers** dialog box, click **Add a Printer**.
2. In the **Add Printer** wizard, choose the option **Add a network, wireless or Bluetooth printer**.



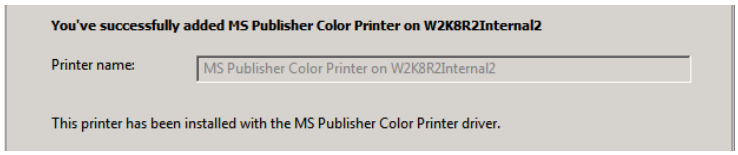
3. The wizard will attempt to locate the printer on the network but will be unsuccessful. To manually specify the printer information, click the link **The printer that I want isn't listed**.



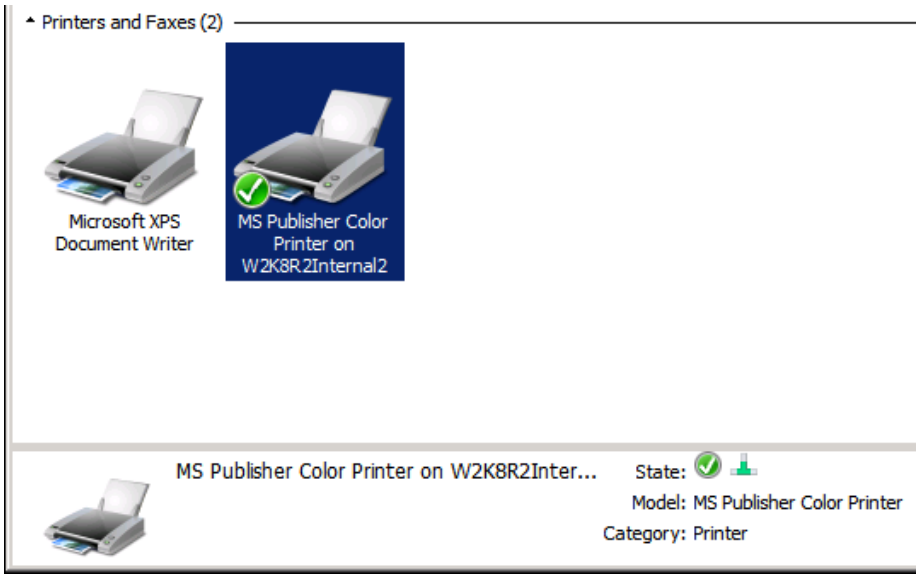
4. Select the option **Select a shared printer by name**. In the text box, type the UNC path to the shared printer, **\\W2K8R2Internal2\MSColor**, and click **Next**.



5. After a brief moment, the printer will install and you will see a message that you have successfully added the printer. Click **Next** and **Finish** to exit the wizard.



6. In the **Devices and Printer** dialog box, click on the printer to highlight it. You will notice the name of the printer gives you the network location from where you installed it. You will also notice the icon next to **State** that shows a network connection.



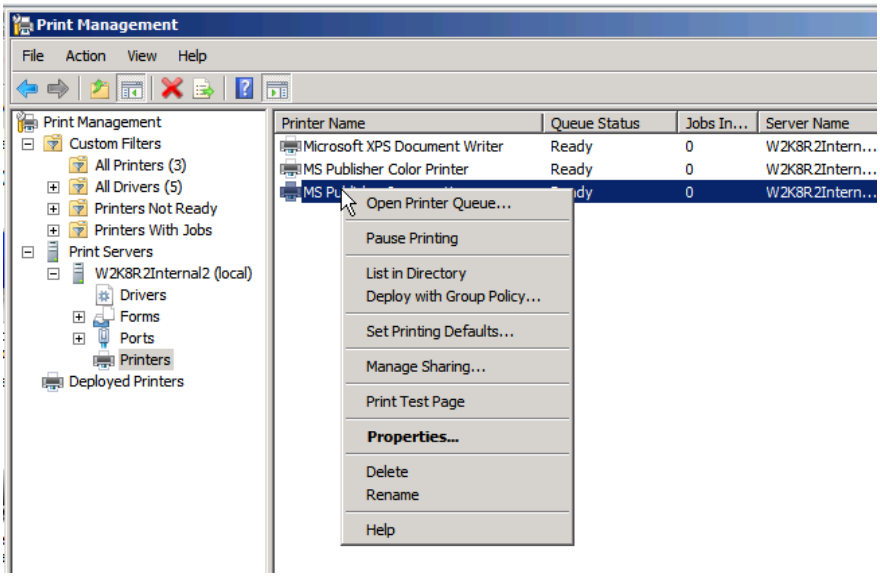
7. Close all open windows on the Windows 2k8 R2 Internal 1 machine.

5.2 Conclusion

Installing a shared printer will allow other machines to use the printer as if it is a locally attached device with the ability to control access and settings.

Installing a printer from a print server is a similar process. A major difference is that if you are in a domain, administrators control access to the printer from the central server. They have the option to list the printer in the directory, which allows users to browse the list of printers in Active Directory and install the ones they want. Or, they have the option to deploy the printer with Group Policy. This forces the printer (and all settings) to be installed on computers that the policy applies to. Administrators have two choices when installing printers in this manner. They are Per User and Per Computer. Per User means the policy is applied to the user account and is available to user regardless of the system they log on to as long as they use their user credentials.

Per Computer means the printer will be installed to all computers the policy applies and any user with access to the system and log on and have permissions to use the printer. Administrators can choose one or both options. The choices can be made through the Print Management console.



5.3 Review Questions

1. *If the Add Printer wizard is unable to automatically find your printer on the network, what do you need to do to install it?*

2. *True or false? Shared printers installed in a peer-to-peer network can control their own access and settings for that printer.*

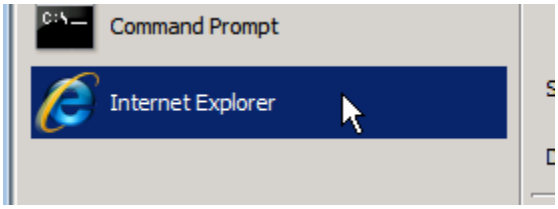
3. *How can network administrators force a printer to be installed for a user regardless of the computer they log into?*

6 Accessing a Web and FTP Server

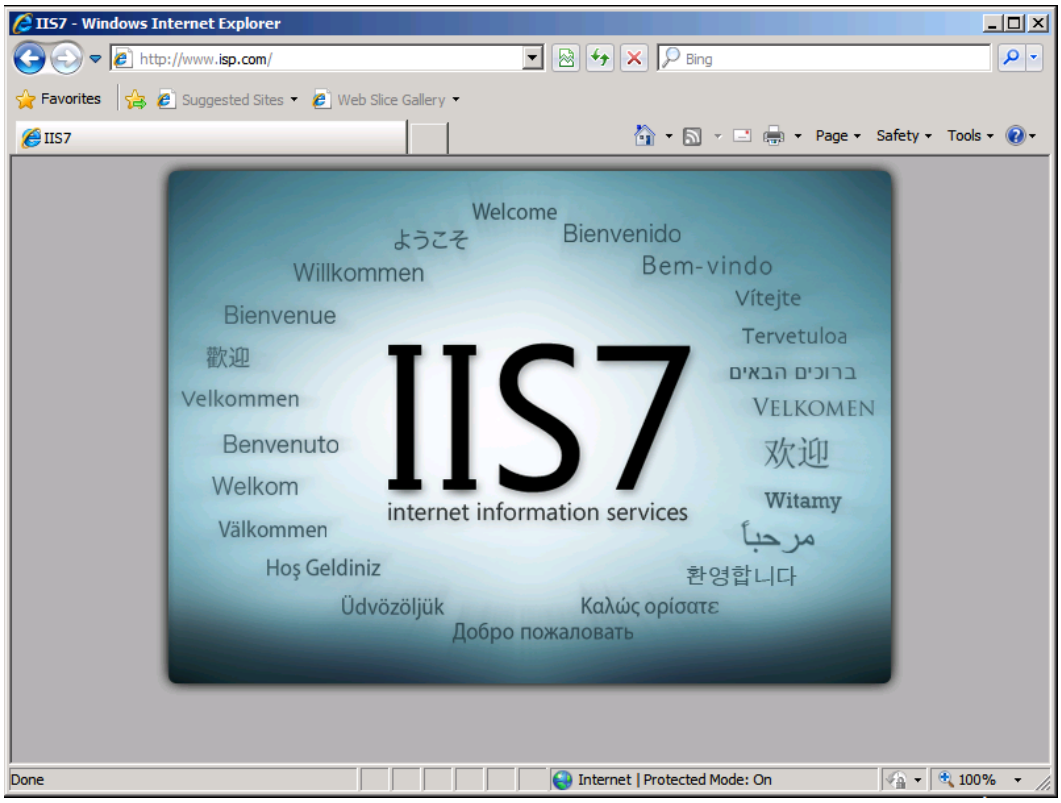
In addition to sharing resources, servers are also useful for hosting resources that many users need to access. Two very common resources that are hosted on servers are web (www) and FTP services. These services can be configured to only allow Intranet access (access only within an organization) or Internet access (access to the public). To access a web site, you need a web browser. Some examples of web browsers include Microsoft Internet Explorer, Mozilla Firefox and Google Chrome. Web browsers translate the HTML code that makes up the webpage and displays the page in a human-friendly format. Web browsers use the default HTTP TCP port 80 to initiate requests. Web browsers also support a secure form of HTTP (called HTTPS) which uses TCP port 443 to access web pages. URLs are used in web browsers to identify resources. URLs are registered domain names that are linked to the public IP address associated with the resource. DNS servers across the Internet exchange these name-to-IP address mappings so users need only remember the name of the resource and not the IP addresses. DNS uses UDP port 53 to exchange information. Web browsers can also be used to access FTP resources. FTP sites are like having a shared folder accessible from the Internet. By default, FTP uses TCP port 21 to exchange control information and TCP port 20 to exchange data.

6.1 Accessing a Web Server

1. Access the web browser on the Windows 2k8 R2 Internal 1 machine by clicking **Start** and selecting **Internet Explorer**.



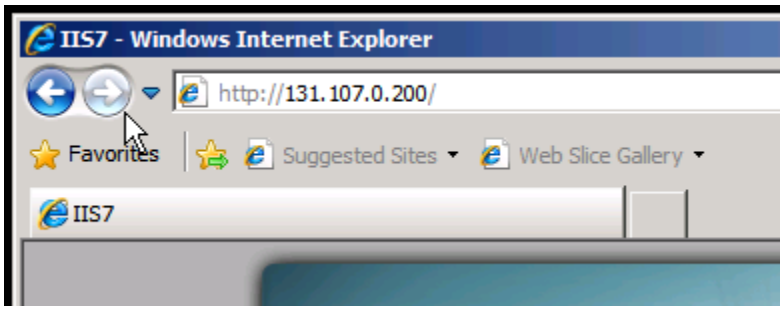
2. In the address bar, type the URL **http://www.isp.com** and press **Enter**. The IIS7 page that appears is being hosted on the Windows 2k8 R2 External machine acting as the web server.



3. If you know the IP address of the server hosting your resource, you can type this into the address bar as well. Type the IP address of the server, **131.107.0.200** into the address bar and press **Enter**. You will notice the same IIS 7 page appears.

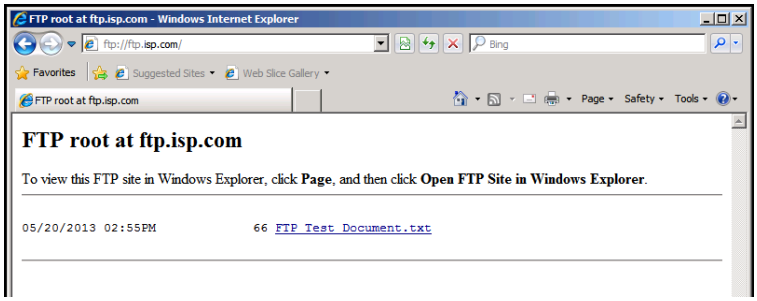
    1. *What change happened in the address bar?*

    Notice that the browser automatically added the http:// in front of the IP address. This is because the browser automatically assumed you wanted to use the HTTP protocol to access the resource.



6.2 Accessing an FTP Server

1. HTTP resources aren't the only resource that can be accessed via a web browser. FTP resources can also be accessed through the browser's interface. Like web sites, FTP sites can be accessed by their URL or IP address. In the Internet Explorer window, type the URL **ftp.isp.com** and press **Enter**. Notice the browser has specified the FTP protocol for you by adding ftp:// in front of the URL. It is a common practice for companies to name their FTP sites in this convention, so the browser assumes you want to access the site using this protocol. You will also notice that you now get a directory listing of the files on the root of the FTP server. These sites make it easy for companies to share files across the Internet. Click on the **FTP Test Document**. The contents of the text file are displayed.



2. **Open a command prompt on your local computer. On the command line, type your first and last names. Take a screenshot that contains your full name and the output window you get at Step 1 above.**

3. It does not matter which URL you use to access the resource as long as they are all mapped to the same IP address. Try the following URLs in the Internet Explorer window and see which site comes up. Pay close attention to how you are typing the URL so you can understand why you get the appropriate site:
   http://www.isp.com – The IIS7 page (http site)
   ftp://www.isp.com – The FTP root
   http://ftp.isp.com – The IIS7 page (http site)
   ftp://ftp.isp.com – The FTP root
   Each of these URLs point to the same server, so by specifying the protocol you can control what resources you access from the server.

4. Close all open windows on the Windows 2k8 Internal 1 machine.

6.3 Conclusion

Servers are useful for hosting resources that many users need to access. Two very common resources that are hosted on servers are web (www) and FTP services. These services can be configured to only allow Intranet access (access only within a corporation) or Internet access (access to the public). To access a web site, you need a web browser. Some examples of web browsers include Microsoft Internet Explorer, Mozilla Firefox and Google Chrome. Web browsers translate the HTML code that makes up the webpage and displays the page in a human-friendly format. Web browsers use the default HTTP TCP port 80 to initiate requests. Web browsers also support a secure form of HTTP (called HTTPS) which uses TCP port 443 to access web pages. URLs are used in web browsers to identify resources. URLs are registered domain names that are linked to the public IP address associated with the resource. DNS servers across the Internet exchange these name-to-IP address mappings so users need only remember the name of the resource and not the IP addresses. DNS uses UDP port 53 to exchange information. Web browsers can also be used to access FTP resources. FTP sites are similar to having a shared folder accessible from the Internet. By default, FTP uses TCP port 21 to exchange control information and TCP port 20 to exchange data.

6.4 Review Questions

1. *What* protocol is used to access web pages on a server?

2. *What protocol is used to access files shared over the Internet?*

3. *What is the default port for the following protocols:*
    a. *HTTP:*
    b. *HTTPS*:
    c. *FTP:*
    d. *DNS:*