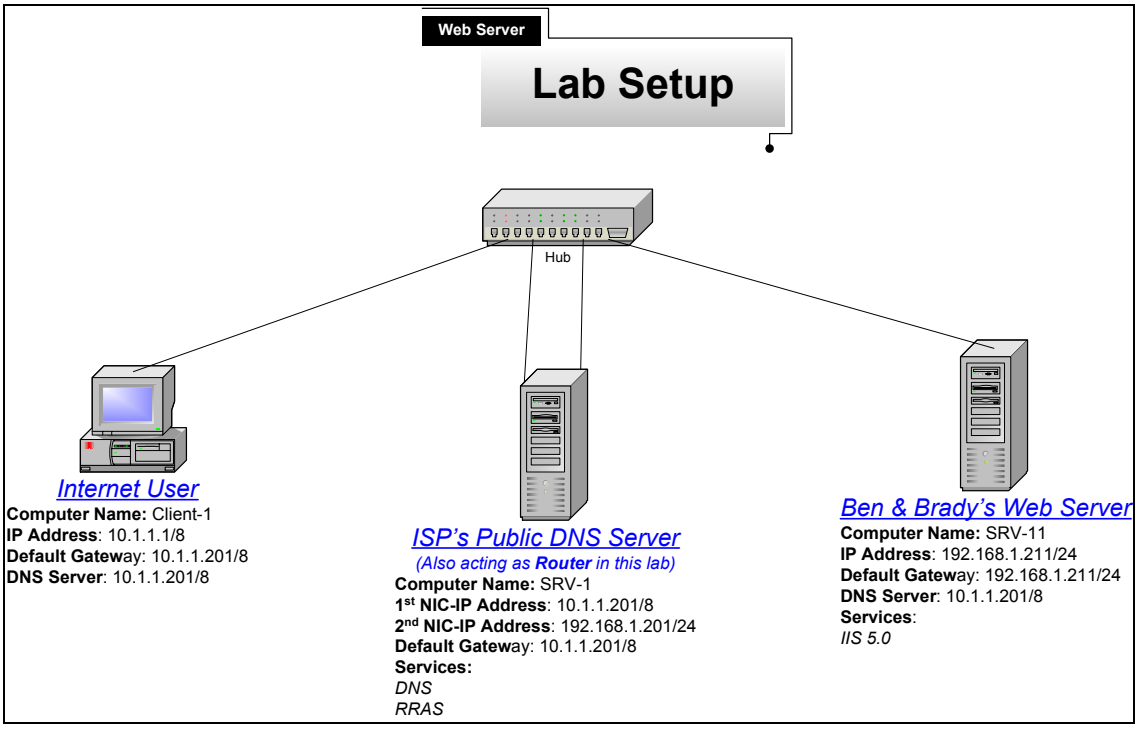
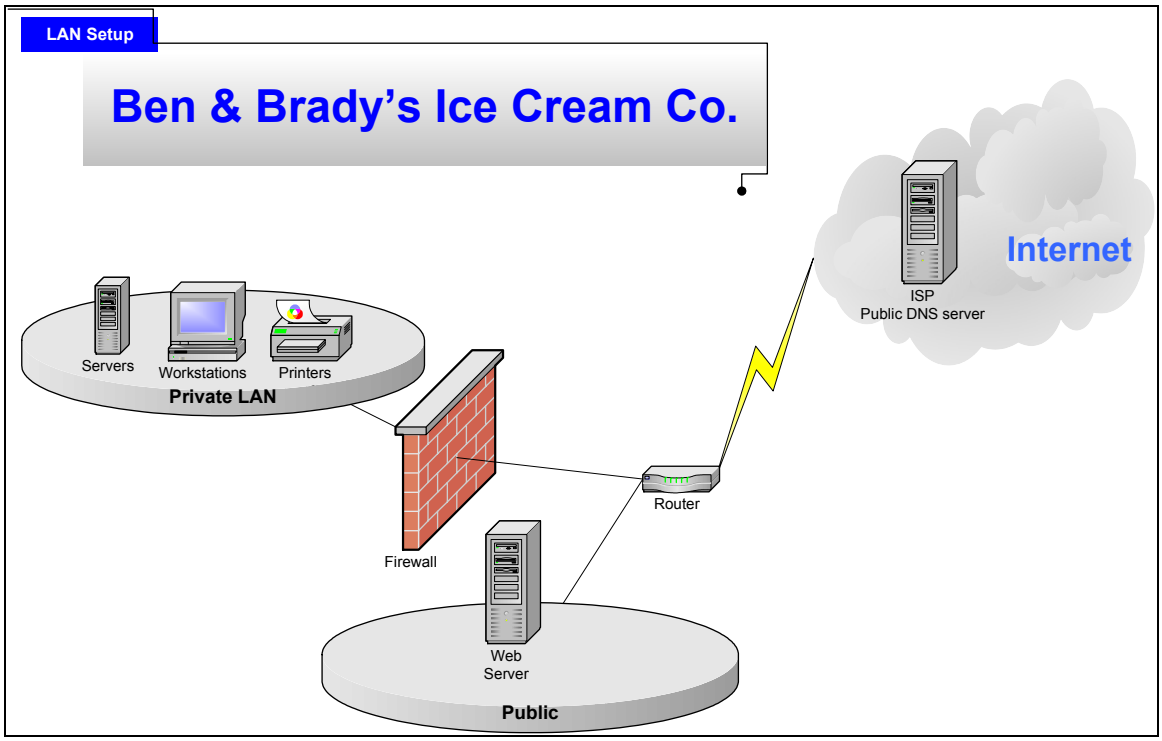
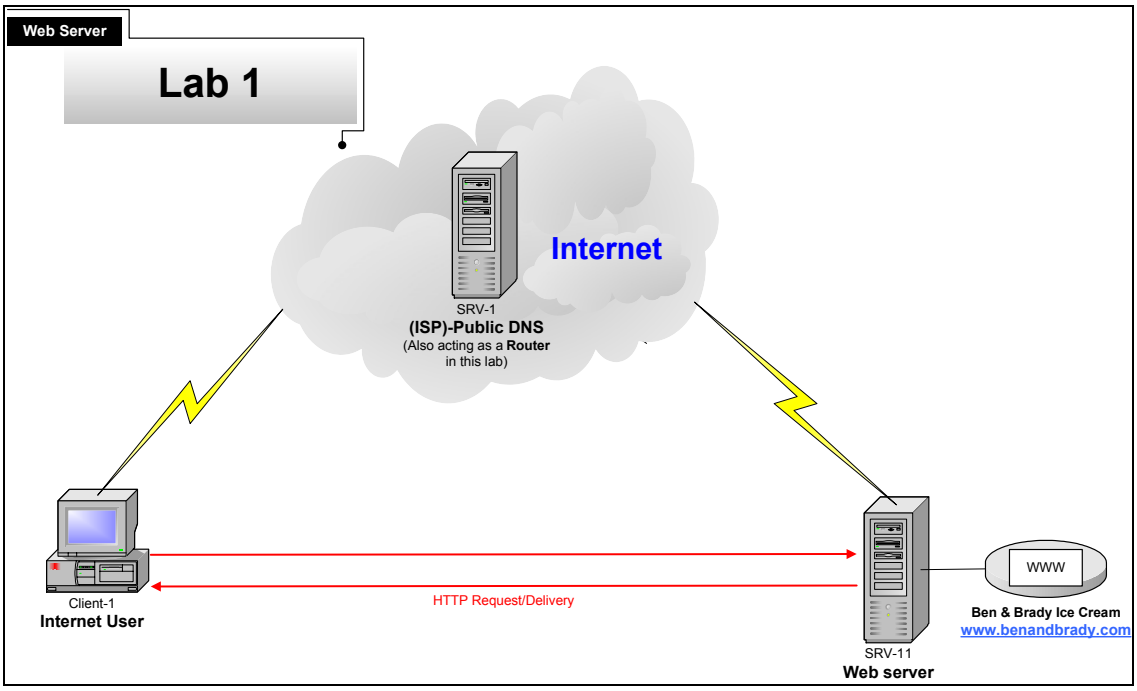
Building a Web Server for
Ben & Brady's Ice Cream, Corp.

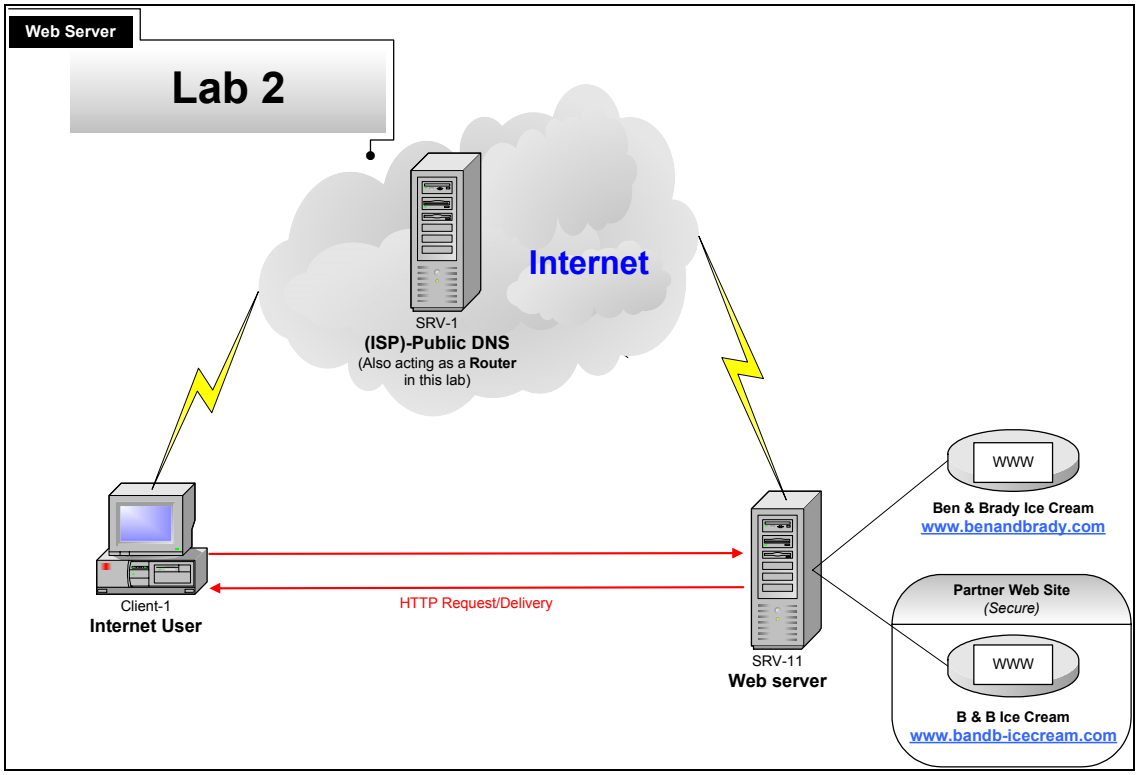
Mega Lab 3

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









Building a Web Server for Ben & Brady's Ice Cream, Corp.

Mega Lab 3

Part 3 of 3 in the Building a Windows 2000 Server Series

About the Authors

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

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

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

Copyright and other Intellectual Property Information

Disclaimer and Limitation of Liability

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

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

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

Choice of Law:

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

TABLE OF CONTENTS

Introduction

Welcome to Train Signal!

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

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

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

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

Thank you for choosing Train Signal!

Lab Setup

Setting up the Lab

1. Computer Equipment Needed

Item	Minimum	Recommended
Computers	(3) Pentium I 133 MHz	(3) Pentium II 300MHz or greater
Memory	128 MB	256 MB
Hard Drive	2 GB	4 GB or larger
NIC	1/machine & 1 computer (SRV-1) should have 2 NICs	1/machine & 1 computer should have 2 NICs
Hubs	1	1
Network Cable	(4) Category 5 cables	(4) Category 5 cables

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

2. Computer Configuration Overview

Computer Number	1	2	3
Computer Name	SRV-1	SRV-11	Client-1
IP Address	192.168.1.201/24 & 10.1.1.101/8	192.168.1.211/24	10.1.1.1/8
OS	W2K Server	W2K Server	W2K Pro
Additional Configurations	SP2 DNS Router (needs 2 NICs)	SP2	SP2

*****Note*****
Windows 2000 (Pro or Server) should be installed on each of these systems with only the **default settings**. If you modify settings or add unnecessary Windows components, parts of this lab might not work correctly!

3. Detailed Lab Configuration

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

Computer 1

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

SRV-1 will be acting as the ISP's DNS Server and will not be a member of any domain. You should leave SRV-1 in it's default workgroup (named workgroup). It will have a static IP address of 192.168.1.201* with a 255.255.255.0 subnet mask on one NIC and static IP address of 10.1.1.101* with a 255.0.0.0 subnet mask on the second NIC. You can leave the default gateway field blank for both NICs and the preferred DNS server setting should be set to point to SRV-1's own IP address (192.168.1.201) for both NICs. The alternate DNS Server fields can be left blank. This system will also need to route information between the other two computers in the lab, so routing must be enabled.**

To enable routing go to:
Start → Programs → Administrative Tools → Routing and Remote Access.

In the left pane of the console right click on SRV-1 and select **Configure and Enable Routing and Remote Access**. On the RRAS wizard select **Network Router** as the configuration, select **TCP/IP** as the protocol and select **No** for Demand Dial connections. When the installation is finished you should have a green arrow next to SRV-1 indicating that the server has routing enabled. Routing is beyond the scope of this lab, but will be covered in another Mega Lab. See figure 1, next page.

Computer 2

Computer 2 will be named SRV-11 and Windows 2000 (either version once again) will be installed on this computer with Service Pack 2. SRV-11 will act as the web server for Ben & Brady's Ice Cream Corp. and should **not** be a member of any domain. Like SRV-1, SRV-11 should be left in the default workgroup named "workgroup." SRV-11 will have a static IP address of 192.168.1.211* with a 255.255.255.0 subnet mask. You should configure the default gateway field and the preferred DNS server setting to point to SRV-1, 192.168.1.201* and leave the alternate DNS setting blank. See figure 1, next page.

Computer 3

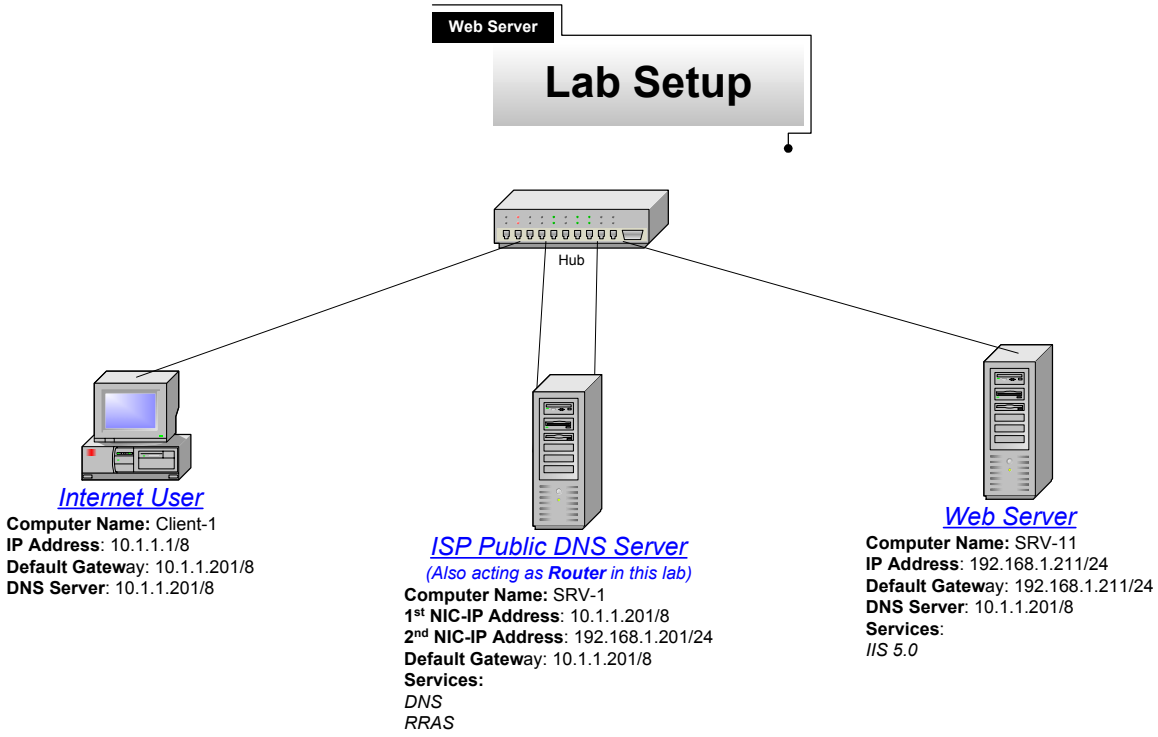
Computer 3 will be named Client-1 and have Windows 2000 Professional installed as the operating system. Client-1 will not be a member of any domain and will be part of the default workgroup named "workgroup." Client-1 will be acting as a public Internet user to test access to the web sites. It should be configured with a static IP address of 10.1.1.1* with a 255.0.0.0 subnet mask. You should configure the default gateway field and the preferred

DNS server setting to point to SRV-1, 10.1.1.101. You can leave the alternate DNS setting blank. See figure 1, next page.

* It's not recommended that you use public IP addresses on your network if you have computers that can connect to the Internet. In order to be safe, we are using private class IP addresses for the web server in this lab. In the real world, public IP addresses would have to be used in some capacity on all three of these machines.

** Routing is enabled on SRV-1 in this lab, to allow it to pass traffic between two different networks. Routing is not required or necessary for DNS to function or to host your web site.

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



(figure 1)

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

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

Lab 1

Creating a Web Server for Ben & Brady's Ice Cream, Corp.

You will learn how to:

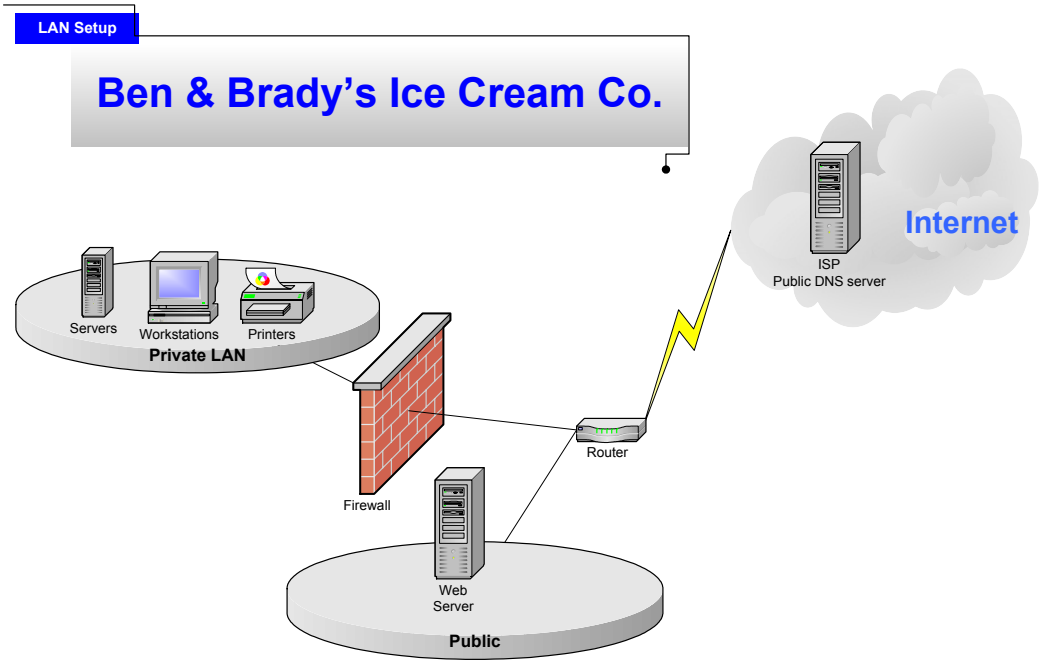
- Install IIS 5.0 on Windows 2000
- Create an HTML file
- Create a new public website
- Configure DNS for the website
- Test and view the website from the client

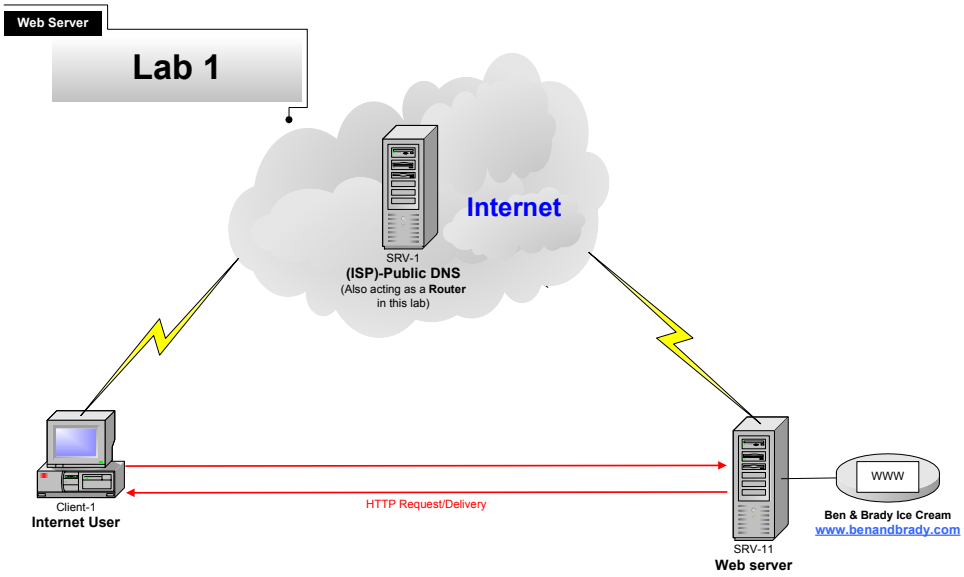
Scenario

Ben & Brady's Ice Cream Co., is a manufacturer of gourmet ice cream products that are sold internationally. Their main headquarters is located in San Francisco and they also have a manufacturing facility in Charlotte, North Carolina. The San Francisco office currently has 5 servers, all running Windows 2000 Server, and 125 workstations, all running Windows 2000 Professional. They are connected to the Internet with a full T1 (1.544 Mbps), and Microsoft's ISA Server (firewall) protects the internal network. The facility in Charlotte is used to manufacture ice cream and to ship to Ben & Brady's east coast distributors. This location currently has 5 servers, all running Windows 2000 Server, and 30 workstations, also all running Windows 2000 Professional. Charlotte is connected to the Internet with a Fractional T1 (768 Kbps) and they also use ISA Server to protect their internal network. The two locations are connected together through a VPN formed between the two ISA Servers over the Internet. Currently, Ben & Brady's does not host any public servers (i.e. DNS, Web, Email) but rumors have been circulating that this will change…

Jill, the IT manager, has decided to give you the project of hosting the company web site on a Windows 2000 server locally. The company previously outsourced web hosting but they have had too many problems with the hosting company. They have decided to give their networking experts a shot at hosting the web site locally. Jill makes you the team leader of the new project because you have proven to be reliable and efficient in previous projects. The project folder that Jill gave to you contains all of the specifications that you need in order to get the project started. Reading through the document you see that initially, you are required to create an HTML file to use temporarily when you test the site. Also, the company has obtained a range of public IP addresses from their ISP and you have been given one of these to use. In addition, the public DNS domain name of benandbrady.com will continue to be used, along with the host name of www (the web site will be found at www.benandbrady.com). But, DNS will still be hosted by your ISP (pretend the DNS server that you install and use in this lab belongs to the ISP!)

In this lab you will create your test site, set up your web server and then host the site from the web server. You will also set up a public DNS server so that the Internet client (Client-1) can connect to the web server using the URL www.benandbrady.com.

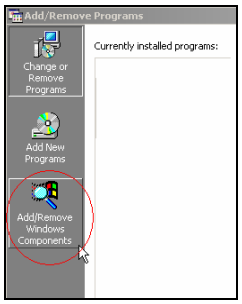




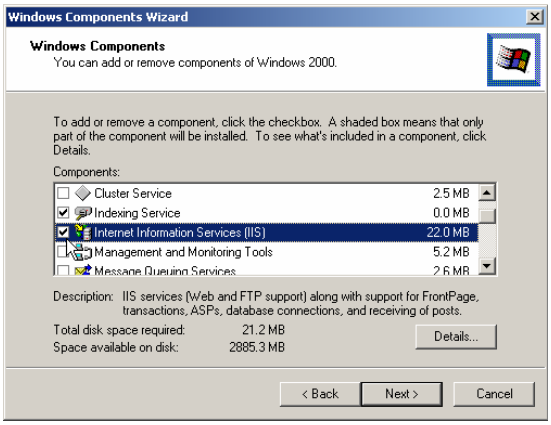
Installing IIS on Windows 2000 Server

Windows 2000 comes with Internet Information Services (IIS) version 5.0 included in the operating system. IIS is automatically installed during the initial installation of Windows 2000, unless you specifically choose for it not to be installed (it is located within Windows Components). Nonetheless, the first step is to check and see if IIS is already on the server - if not, then follow steps 1-3 to get it installed.

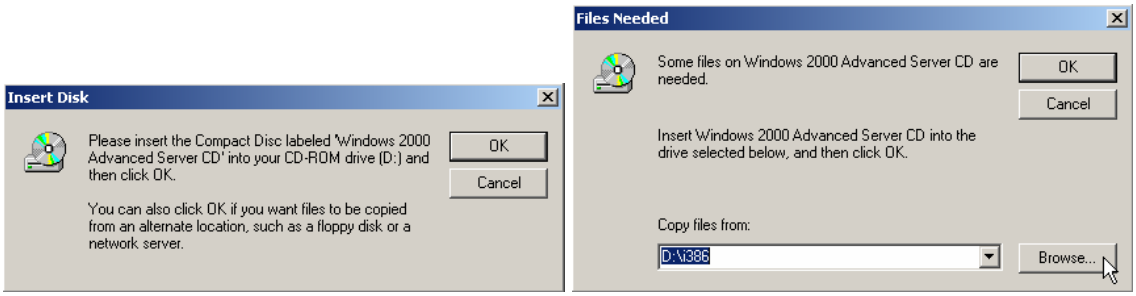
1. Log on to **SRV-11** with the administrator account and go to **Start→Settings→Control Panel**. Double click on **Add/Remove Programs.** Within Add/Remove Programs click on the **Add/Remove Windows Components** button on the bottom left of the screen.



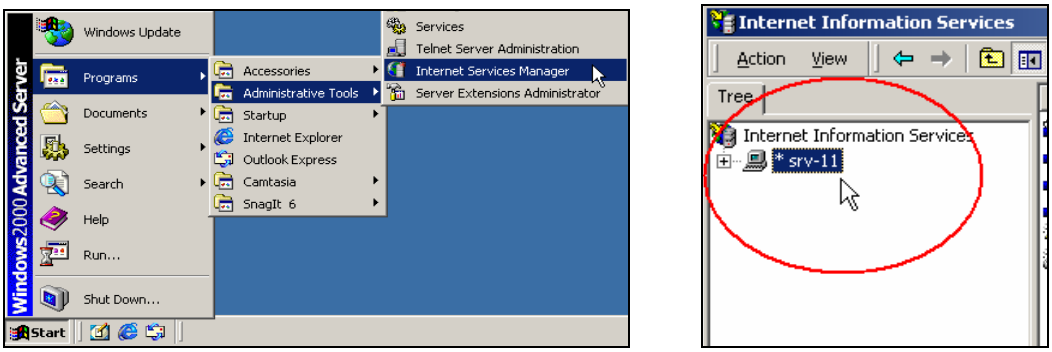
2. That will bring up a screen with a list of all available Windows components for the Windows 2000 operating system. Scroll down the list until you find the **Internet Information Services (IIS)** component. If the box to the left of it is not marked with a checkmark then IIS is not installed. If it is checked then it is installed and you can click **Cancel** to close the Add/Remove Programs screen and move on to the next section of this lab. If it is not installed then simply place a check mark in the box next to the **Internet Information Services (IIS)** component and click **Next** to start the installation.



3. During installation you will be prompted to insert the **Windows 2000 Server CD-Rom** or locate the **I386** folder in order for the installation to continue. Once the installation is complete, Click on **Finish**. Then close the **Add/Remove Programs** window and the **Control Panel**.



4. Make sure that the installation was successful by trying to open the **Internet Services Manager** from the Start menu.. Go to **Start→Programs→Administrative Tools→Internet Services Manager**. If you can open the console and see SRV-11 on the top of the tree in the left pane, then you have successfully installed IIS on this server.



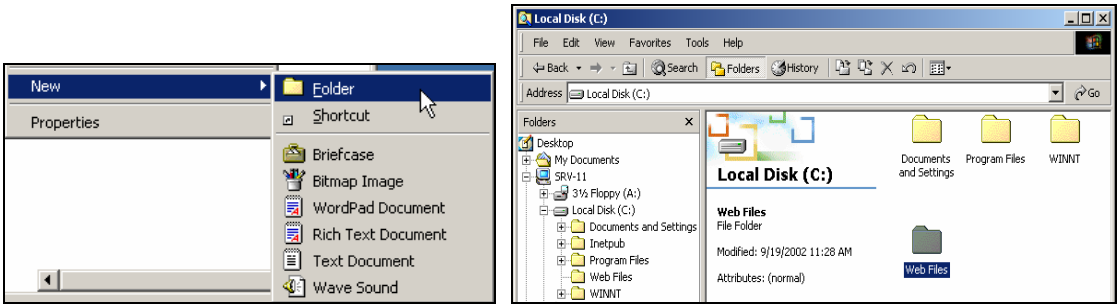
Creating an HTML file

Before you build your web server, you need to create a file that will be used to represent your website within IIS. You will be creating a Hyper Text Markup Language (HTML) file. HTML is one of the most common and simplest authoring languages used to create websites. HTML files can be created with Microsoft's Notepad, WordPad or Word as well as many other programs that are purely designed for creating web pages.

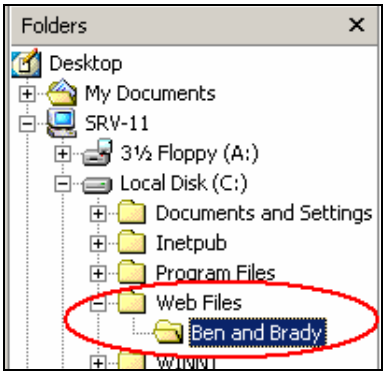
Although IIS automatically creates folders for Internet services when it is installed, you are better off creating your own folders for your web sites. Creating your own folder structure

allows you to organize your web site files and folders any way you like. It will also make your system more secure, since hackers will look for the built in root folders first if your web server is ever penetrated.

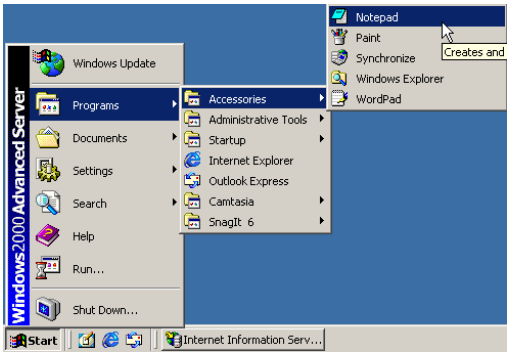
1. Close the **Internet Services Manager** console and open **Windows Explorer**. On the C: drive, create a new folder and name the folder **Web Files.** This can be done by right clicking on an empty space within the **C: drive** and selecting **New Folder** from the shortcut menu.



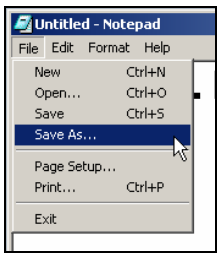
2. Now open the **Web Files** folder and create a new folder within it named **Ben and Brady**. You should now have a root folder named Web Files on the C: drive and a folder within it named Ben and Brady for the benandbrady.com web site. Close **Windows Explorer** when you are finished.



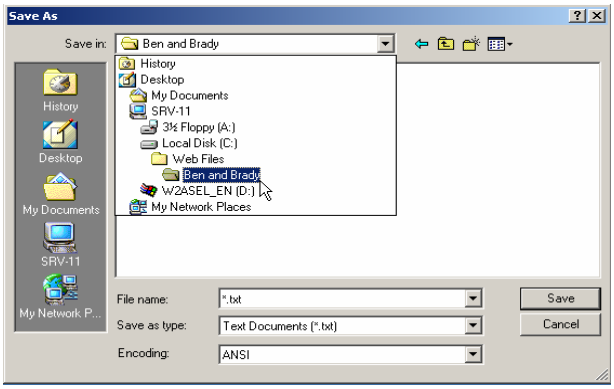
3. Next, use Notepad to create a simple HTML file that will be used to test the www.benandbrady.com website. Go to **Start→Programs→Accessories→Notepad.**



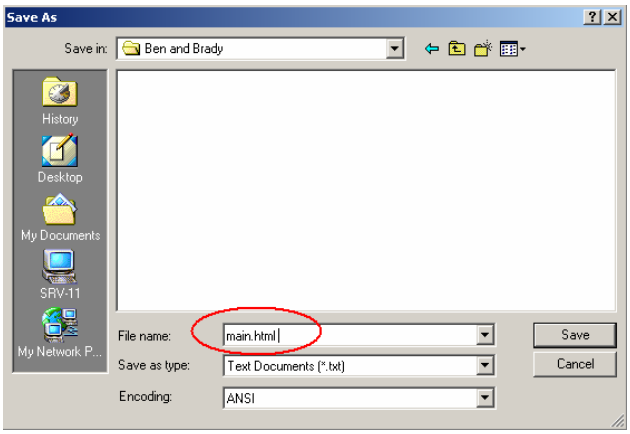
4. In notepad, type in **WWW.BENANDBRADY.COM**. Then from the File Menu select **Save As.**



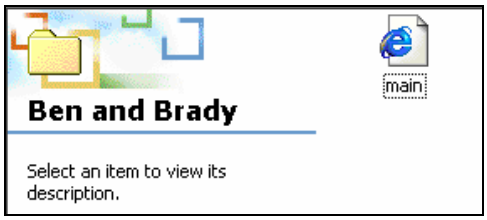
5. On the Save As screen, open the **Save in drop down menu** and select the **Ben and Brady** folder that you created earlier as the location to save this file in.



6. Once you have selected the Ben and Brady folder as the location to save the file, enter the filename **main.html**. Placing .html after the file name will automatically convert the file to HTML format. Click on the **Save** button and close **Notepad.**

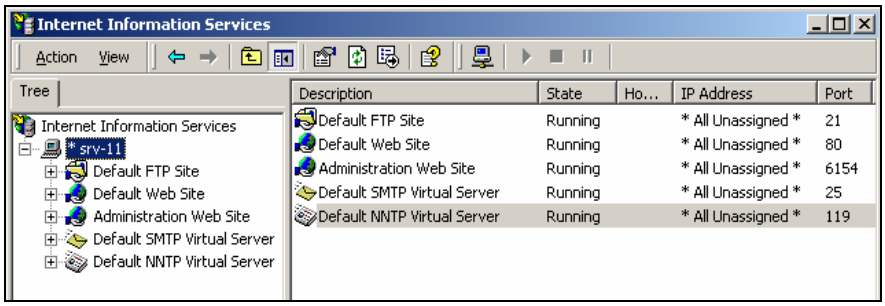


7. Next, open the **Ben and Brady** folder using Windows Explorer to make sure that the file was saved as HTML. If the file appears with an Internet Explorer icon then the file has been successfully saved as an HTML file. Close **Windows Explorer**.

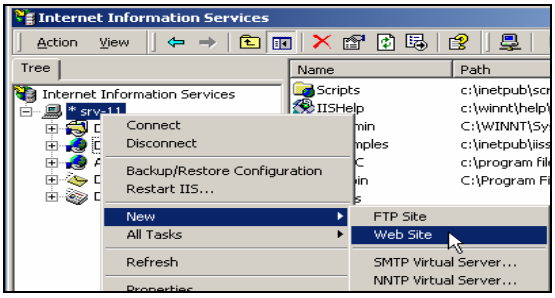


Hosting Ben & Brady's site

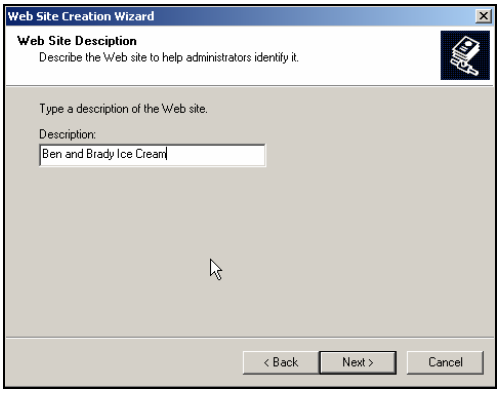
1. Open the **Internet Services Manager**. You'll see that there are already some services running on SRV-11. All of these services are created and started by default when IIS is installed.



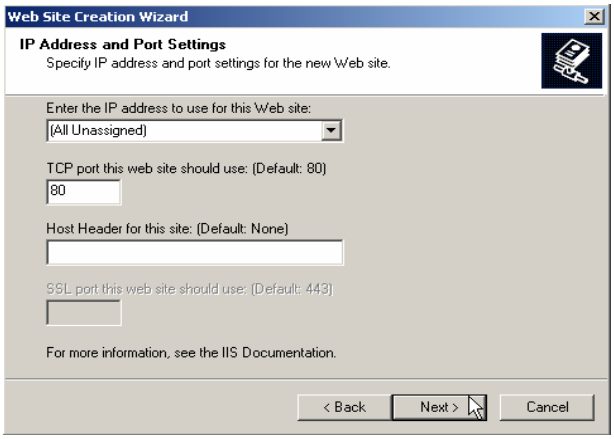
2. To create a new website right click on **SRV-11** and select **New→Web Site** from the shortcut menu. This will start a wizard that walks you through the basic steps for creating a web site. The first screen on the wizard is just a welcome screen, click on **Next**.



3. The next screen of the wizard will ask you to give the new web site a description. This is how the web site will appear within the Internet Services Manager tool. Type in: **Ben and Brady Ice Cream** and click **Next**.

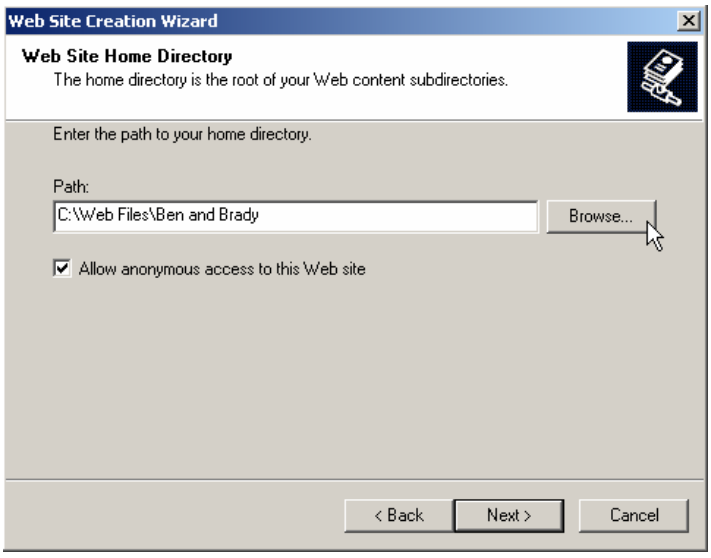


4. The next screen is used to specify the IP address and port number from which this web site should listen to web requests. If you have only one IP address configured on your system, then your web server will listen on this one IP address. If you have multiple IP addresses on your computer (either physical IPs assigned to multiple NICS or logical IPs assigned to one NIC) then you can choose which IP address you want this site to listen for requests on. Using multiple IP addresses allows IIS to host a different website on each different IP address. By default, All Unassigned will be selected. All Unassigned allows the web page to be viewed using any available IP address on the system. Change this setting and select the only IP address that is assigned to this computer: **192.168.1.211**.

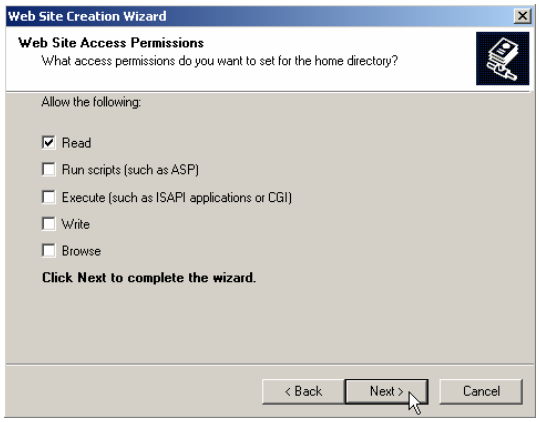


The next field is used to specify the TCP port number that this site will listen on. By default, the port number 80 will appear because this is the port number used for HTTP. HTTP is the protocol used on the Internet by Internet browsers trying to access web sites. Leave the default port number at 80 because changing it will make it much more difficult for anyone trying to connect to your web site. Browsers (i.e. Internet Explorer or Netscape Navigator) use port 80 by default when they attempt to connect to web sites. If you change your port number, Internet users will not be able to connect to your site unless they specify the correct port number after the web site address. For example if you enter a port number of 81 the user trying to reach your site will have to enter: www.benandbrady.com:81 into the web browser address box to reach the web site. The next field on this screen is used to specify a host header, which by default is blank. The host header will tell the server what the name of this web site is. We will cover this concept in more depth later in this course. For now, leave the host header blank and click **Next**.

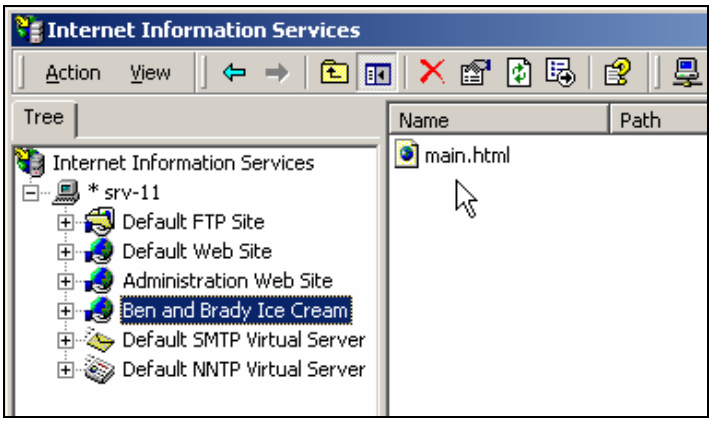
5. The next screen will ask you to specify the path to the home directory for the web content. In other words, where the HTML files for this web site are located. Click on **Browse** and select the **Ben and Brady** folder as the home directory for the web site. Under the path name there is a box **Allow anonymous access to this Web site** that is already checked. This is selected by default as Internet users must have permission to read these files to connect to the site. Therefore, selecting this option allows any user on the Internet to connect to the site without having to enter a user name and password. Leave the option checked and click **Next**.



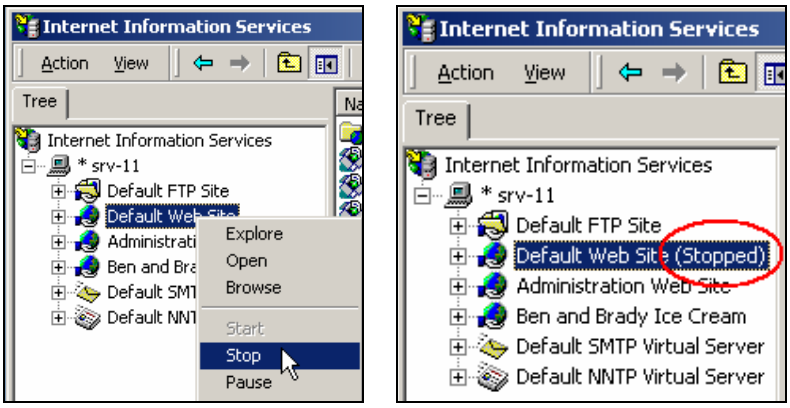
6. The next screen will ask you to specify the permissions that you want to set on the web site for Internet users. By default the Read and Run scripts permissions will be checked. The Read permission will allow users to navigate through the pages of the web site's home directory. The Run scripts permission allows users to execute Active Server Pages (ASP) scripts. The Execute permission allows users to execute any applications that use ISAPI or CGI. Typically, web based applications and other programs require one or both of these permissions (Run scripts or Execute). The Write permission allows users to upload files into the directory or to enter data into a file. This permission is typically not assigned to an anonymous Internet user. Finally, the Browse permission will allow users to browse the home directory of the web site as if they were using Windows Explorer. This web site is strictly for customers to read information about the company and its products. It will therefore only require the Read permission. Un-check the **Run scripts** permission and leave the Read permission as the only one selected. Click **Next**.



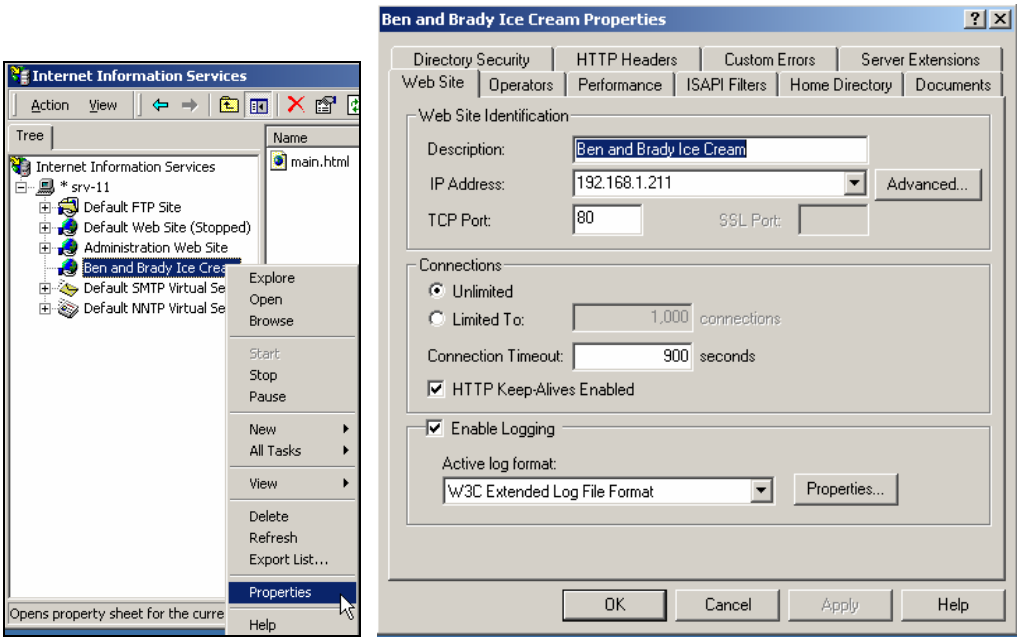
7. On the final screen of the wizard click **Finish** and you should now see the web site for Ben and Brady Ice Cream appear in the left pane of Internet Services Manager.



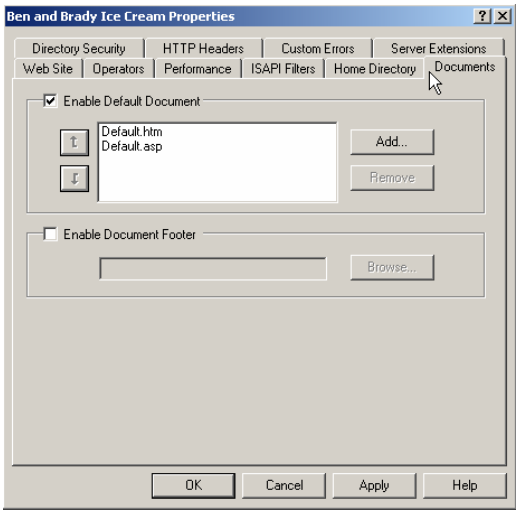
8. The next step is to disable the Default Web Site that was automatically created when you installed IIS. The default web site contains help files and general information about IIS and listens for web requests on Port 80. Stopping the web site or deleting it altogether will prevent it from conflicting with any site you may host on the web server yourself. Right click on **Default Web Site** and select **Stop**. You should then see the word Stopped in parenthesis next to the Default Web Site letting you know that the web site is no longer running.



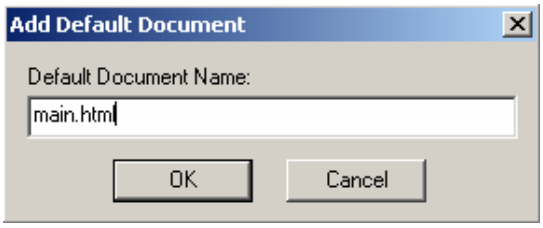
9. Now right click on **Ben and Brady Ice Cream** and select **Properties** from the shortcut menu. This will open the Properties page for the Ben and Brady Ice Cream web site. From here you can make changes and set many other site options.



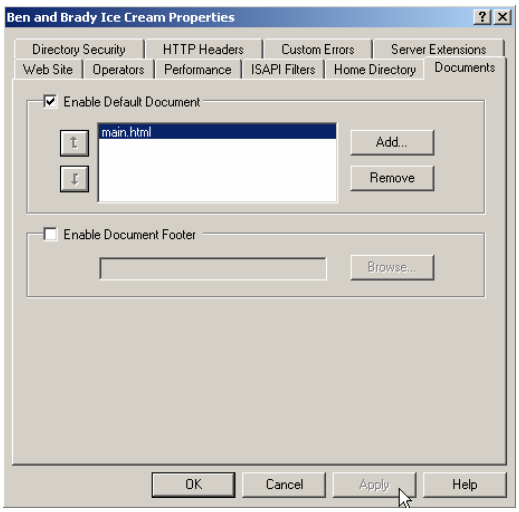
10. On the Properties page for the Ben and Brady Ice Cream web site, select the **Documents** tab. Here you are able to specify the name of the file that you want Internet users to see when they first arrive at your web site. By default IIS uses Default.htm as the default document that users will see, but if there is no file with that name in the site's home directory then users will get an error message. It is therefore very important that you address this issue anytime you set up a new site. You can either go to the home directory and change the name of the main.html file to **default.htm** or you can add the **main.html** file as a default document.



11. Instead of changing the name of the HTML file that you created just add the main.html file to the list of default documents. Click on the **Add** button. Enter **main.html** into the dialog box that appears and click **OK**.



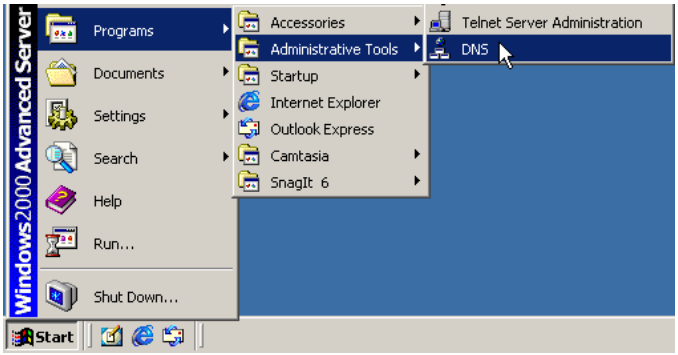
12. You should now have main.html appear in the documents list along with default.htm and default.asp. There is no reason to keep the other default documents on the list, so remove them by selecting each one and then clicking on **Remove** until **main.html** is the only document left on the list. Click **OK** and close the Internet Services Manager.



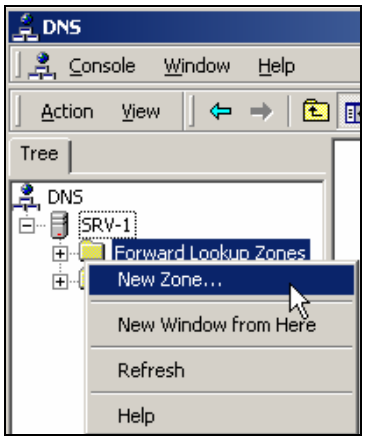
Configure DNS so Internet users can find your website

Now you must configure DNS to resolve any requests for www.benandbrady.com. This must be done on the public DNS server so that Internet users will be able to reach the web site. In this lab you will be making the zone and the host records point to Ben & Brady's web server, but in a production environment this will most likely be handled by an ISP.

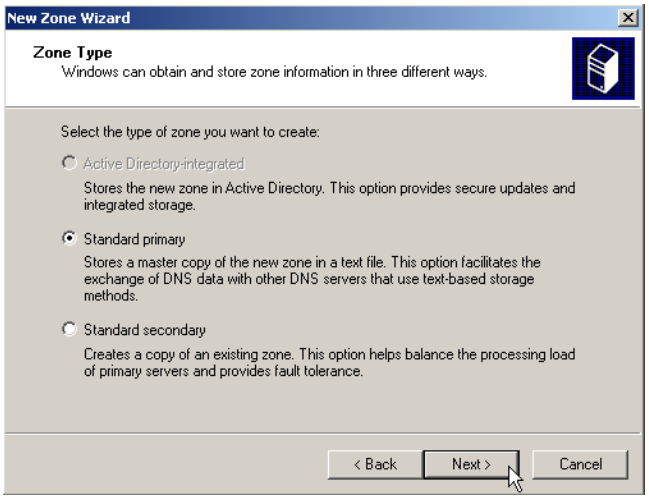
1. Log on to **SRV-1** with the administrator account and open the DNS management console. Go to **Start→Programs→Administrative Tools→DNS.**



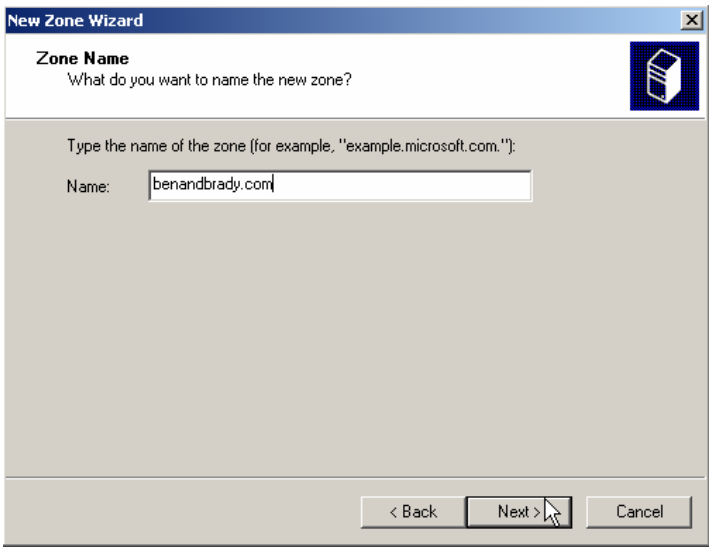
2. You need to create a forward lookup zone and records for benandbrady.com so that clients on the Internet will be able to resolve the DNS name to IP address. Right click on the **Forward Lookup Zone** folder under **SRV-1** and select **New Zone** from the shortcut menu. That will start the Forward Lookup Zone wizard that will walk you through the steps for creating a new zone. The first screen of the wizard is just a welcome screen, click on **Next**.



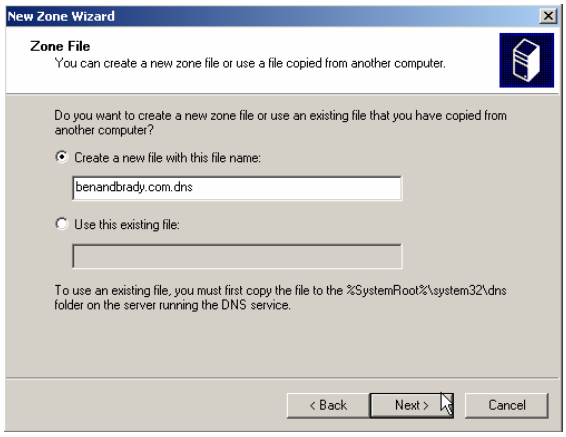
3. The next screen will ask you to specify the type of zone you would like to create. You will only have two options available, one is a **Standard Primary** zone and the second is a **Standard Secondary** zone. The standard secondary zone can only be chosen if there is a standard primary zone already available because it copies the DNS database over from an already existing standard primary zone. In this case we don't have a standard primary zone created for **benandbrady.com,** so you will have to create a new standard primary zone. Select **Standard primary** and click **Next**.



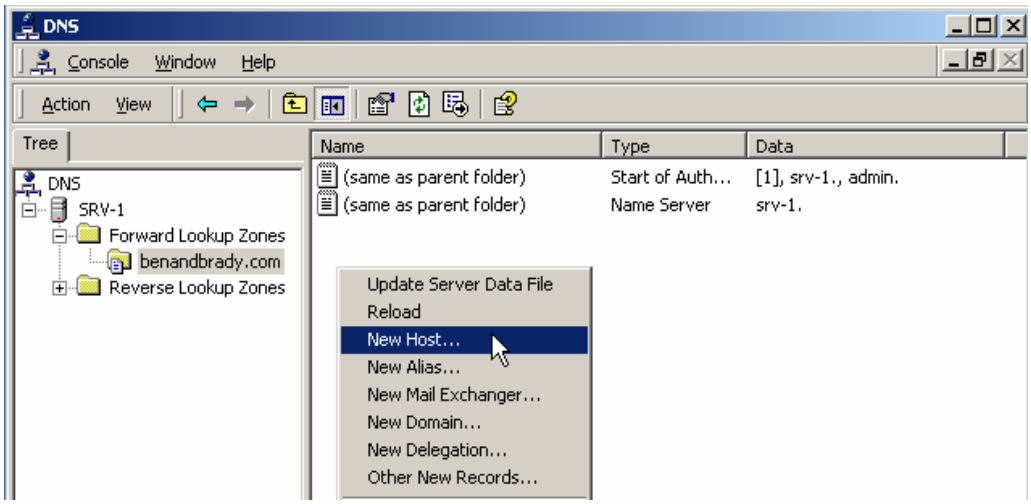
4. The next screen will ask you for the name of the new zone. Enter **benandbrady.com** as the zone name and click **Next**.



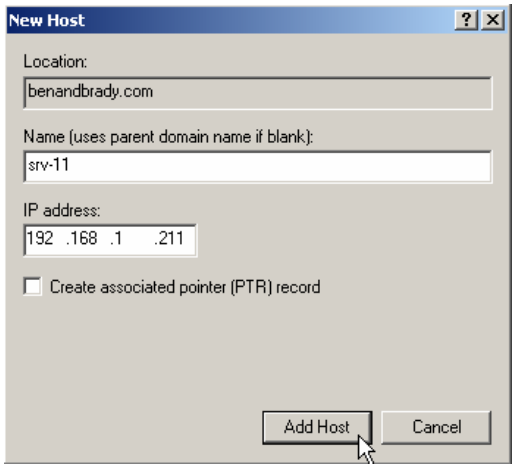
5. Then you will be asked to specify the name of the zone file. You can give the zone file any name you want, but there is no reason to change the default name of benandbrady.com.dns. Click **Next** and you will be taken to the final screen of the wizard, which is just a summary of all the information that you entered in the wizard. Make sure that everything is correct and click **Finish**.



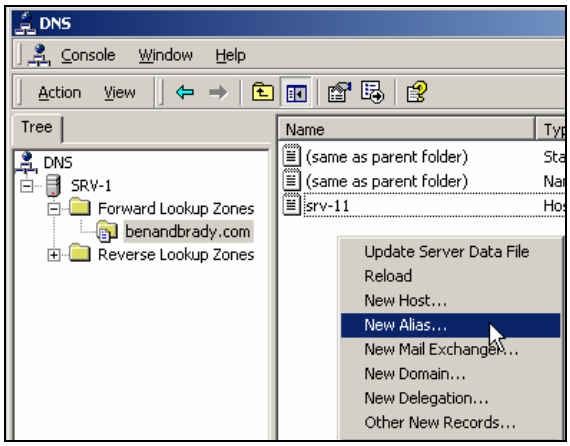
6. Next you need to create a host and an alias record in the benandbrady.com zone for the web server. Open the **benandbrady.com** forward Lookup zone. In the right pane right click on an empty space and select **New Host** from the shortcut menu.



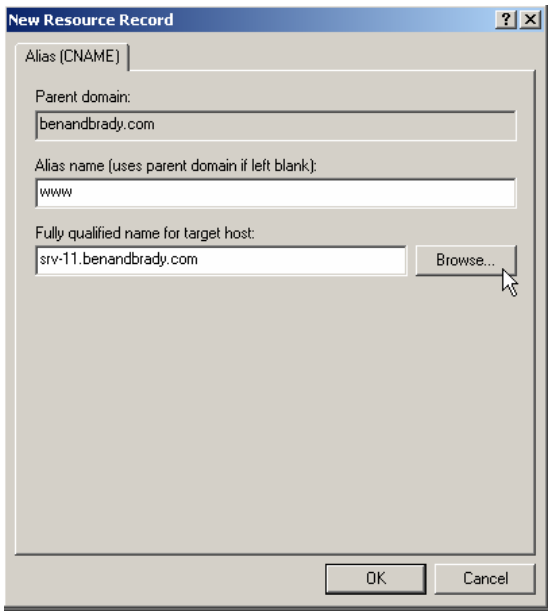
7. In the New Host form, enter **SRV-11** for the name and **192.168.1.211** for the IP address. Then click on the **Add Host** button to create the host record. You will get a dialog box informing you that the host record for srv-11.benandbrady.com has been created successfully. Click **OK** and then click **Done** to close the new host screen.



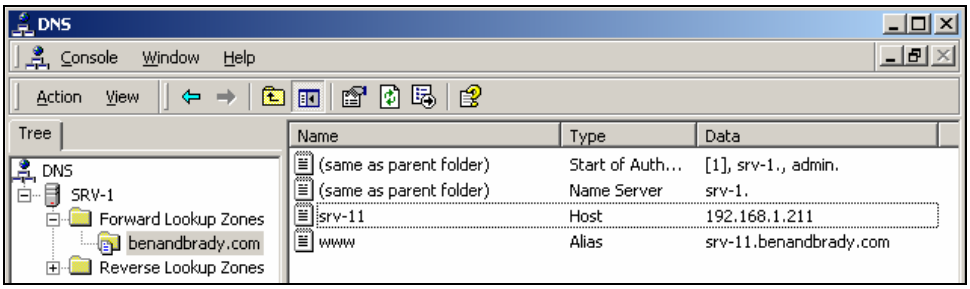
8. You now will need to create an alias record that will point to the web server. An alias record is simply an alternative name for an already existing host record. In this case you will create an alias for SRV-11 so that users can reach the web site by entering www.benandbrady.com into their internet browsers**.** In the right pane, right click on an empty space and select **New Alias** from the shortcut menu.



9. The New Resource Record screen will appear, asking for information to create a new alias. Enter **www** as the Alias name and **srv-11.benandbrady.com** for the fully qualified name. You can also browse for the host record of srv-11.benandbrady.com. Click **OK**.



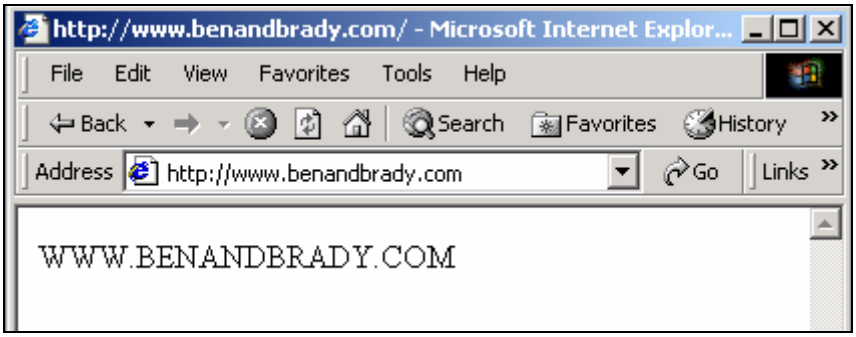
10. You should now see a host record for SRV-11 and an alias record for www appear in the right pane of the DNS console. This will resolve any DNS query made for www.benandbrady.com.



Testing the website from the client

1. Log on to **Client-1** with the administrator account (any user account would be fine) and open the **Internet Explorer** browser.

2. In the Internet Explorer address box enter **www.benandbrady.com** and click **Go**. That should take you to the test web site for the Ben and Brady Ice Cream Company.



Lab 2

Creating an additional secured web site for Ben & Brady's Partners

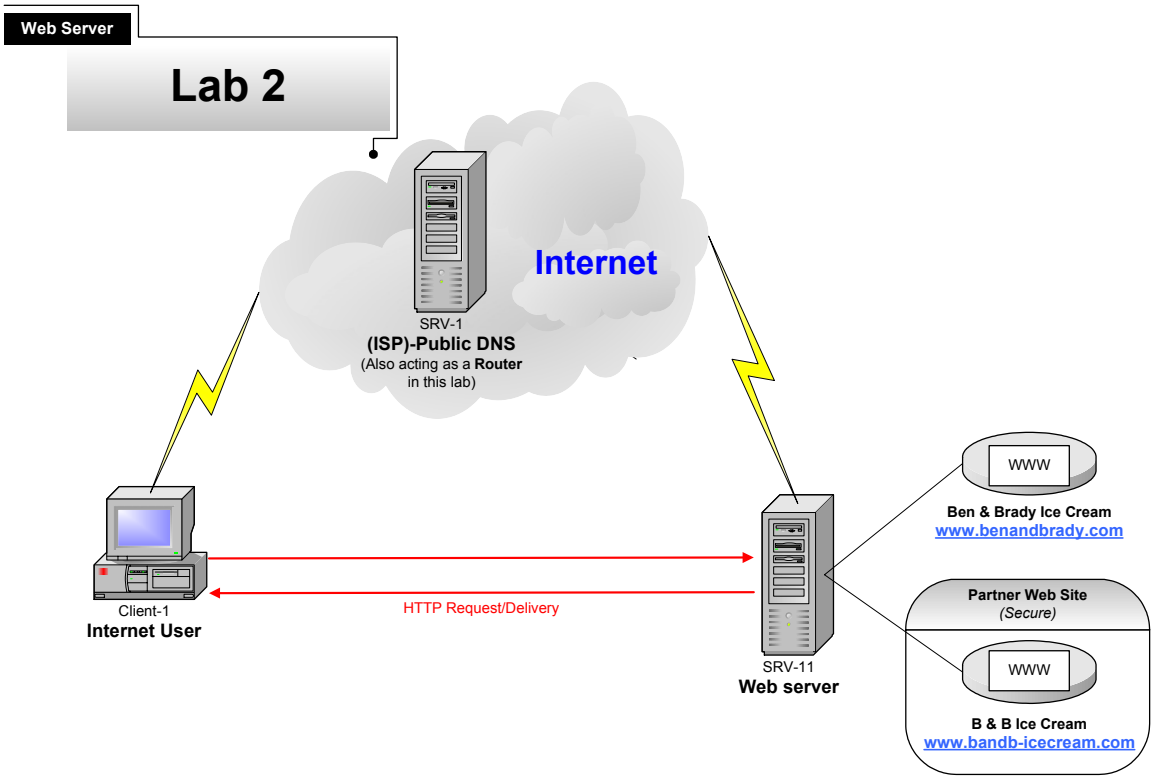
You will learn how to:

- Create & Add an additional web site to a web server
- Configure DNS to handle additional websites
- Configure host headers for web sites
- Assign site operators to manage a web site
- Add authentication to a web site
- Test and view secure web sites from a client

Scenario

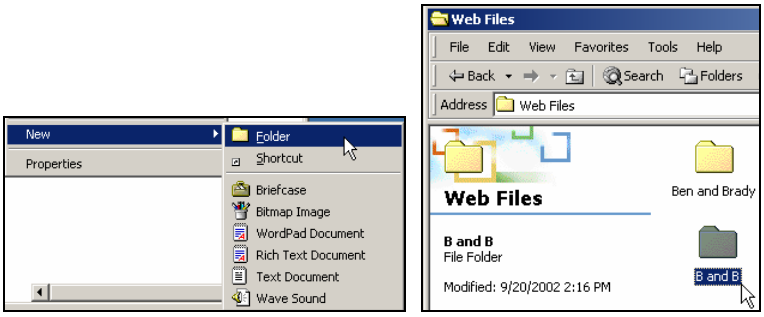
Jill calls you into her office and introduces you to Bill, the new web site designer. He has been hired to create and manage a new web site that will be hosted on Ben & Brady's web server. The new site is for Ben & Brady's partners to access information regarding wholesale prices, product information as well as marketing information on upcoming new products. Bill will be in charge of creating the site and updating it on a daily basis. She tells you that the web site will need to go live by the end of the week because the CEO is meeting with all of the partners and would like to show them the new site during their meeting. Jill explains to you both that the web site must only be accessible by partners and they don't want to allow any consumers or competitors to be able to view any of the wholesale product prices . Therefore all partners must be given secure user names and passwords to be able to access the site. Jill has registered the public domain name bandb-icecream.com to use for the secure site, but she did not get a second public IP address for this site. Therefore you must use the single public IP address that is already hosting the benandbrady.com web site. Jill is aware that there are several ways to host multiple web sites using one IP address, but she has left it up to you and Bill to decide which method will work best.

In this lab you will create a new test web site in similar fashion to Lab 1. You will also configure this site to require a username and password. Local user accounts will be created for Bill and the partners to use. Bill will be configured as a web site operator, only allowing him to manage the secure web site and not the whole web server. DNS will also be configured so that the web sites can be reached from a test computer using a URL.

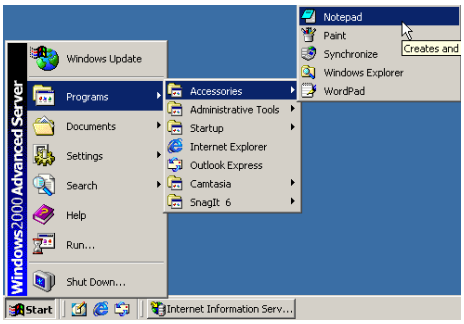


Creating a Test Web Site using a HTML file

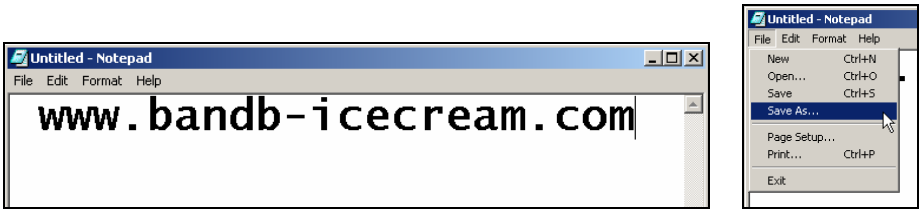
1. Log on to **SRV-11** with the administrator account and open **Windows Explorer**. On the C: drive, open the **Web Files** folder and create a new folder within it named **B and B**. This can be done by right clicking on an empty space within **Web Files** and selecting **New Folder** from the shortcut menu. You should now have two folders within Web Files, one named Ben and Brady and the other named B and B. Close **Windows Explorer** when you are finished.



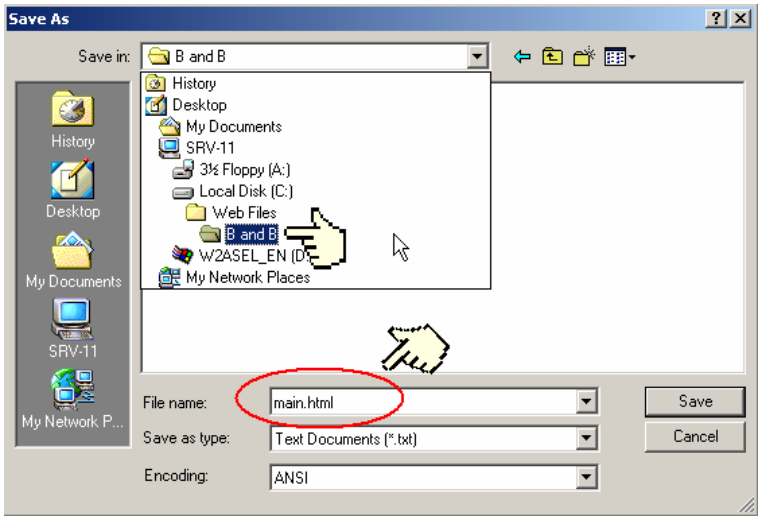
2. Next, use Notepad to create a simple HTML file that will be used for the www.bandb-icecream.com website. Go to **Start→Programs→Accessories→Notepad.**



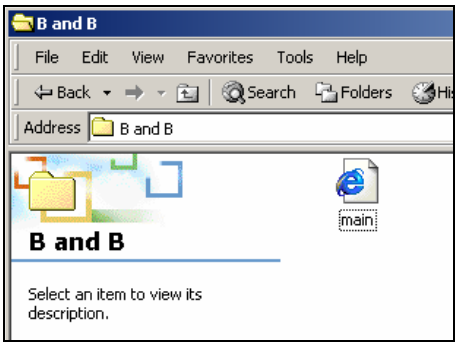
3. In Notepad**,** type in **www.bandb-icecream.com** and then select **File→Save As** from the menu.



4. On the Save As screen open the Save in **drop down menu** and select the **B and B** folder that you created earlier as the location to save this file. Once you have selected the folder, enter the filename **main.html.** Then click on the **Save** button and close **Notepad.**

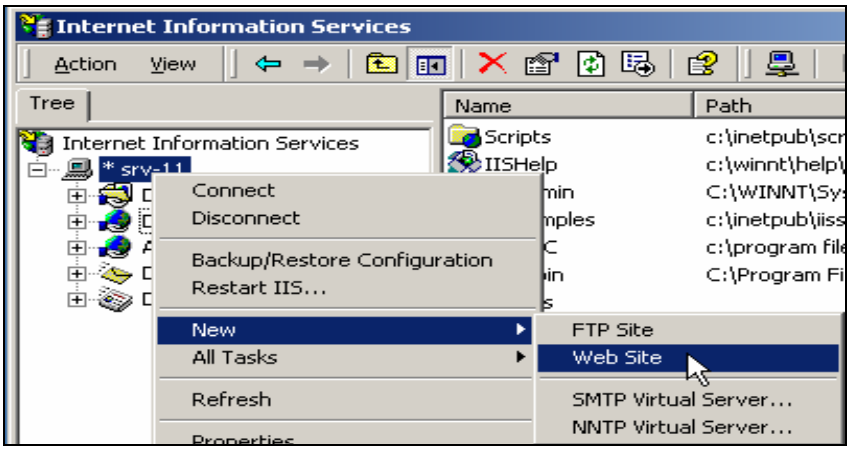


5. Now open the **B and B** folder using **Windows Explorer** to make sure that the file was saved using HTML. Close **Windows Explorer**.



Creating an additional Website on the Web Server

1. Open the **Internet Services Manager** and right click on **SRV-11.** Then select **New→Web Site** from the shortcut menu to start the new web site wizard to create a new website for www.bandb-icecream.com.



2. Within the wizard click **Next** on the welcome screen. On the next screen type in: **B and B Ice Cream** as the description for the web site and click **Next** to continue.

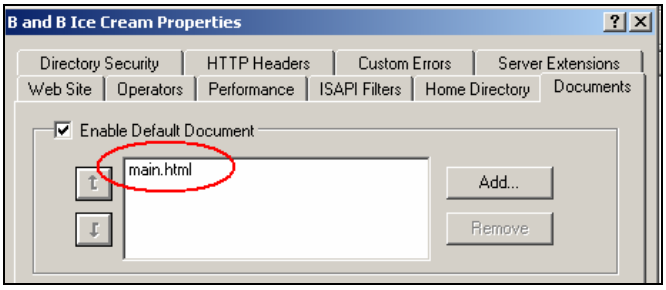
3. The next screen will first ask you to specify the IP address to use for the web site. Select **192.168.1.211** from the drop down menu for this, as it's the only one available. Leave the default port number 80. Leave the host header blank and click **Next**.

4. Specify the path to the home directory for the web content as the **B and B** folder and leave the Allow anonymous access to this Web site box checked, then click **Next**.

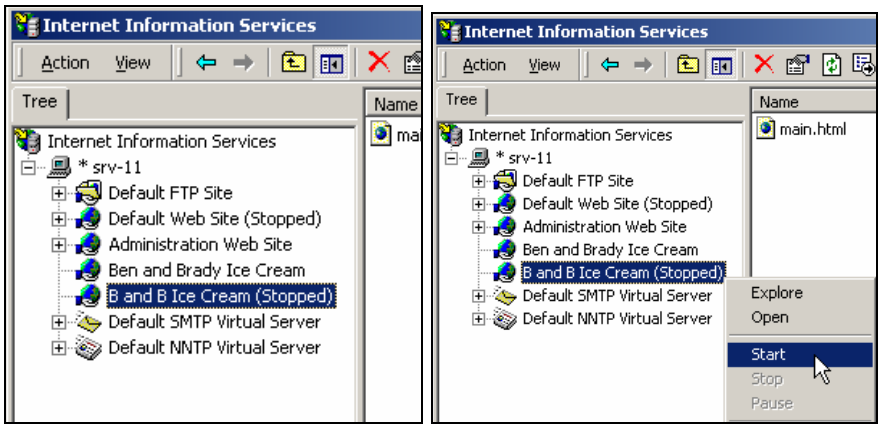
5. This web site will be used strictly for B & B's partners to read information about the company and its products. Un-check the **Run scripts** permission, leaving the Read permission as the only one selected. Click **Next**.

6. On the final screen of the wizard click **Finish** and you should now see the web site for B and B Ice Cream appear in the left pane of Internet Services Manager.

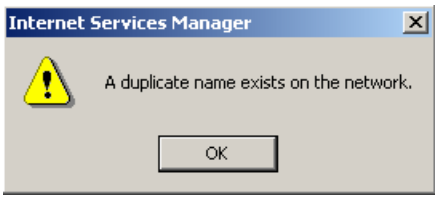
7. Next, open the **Properties** page for the B and B Ice Cream web site. Right click on **B and B Ice Cream,** select **Properties** from the shortcut menu, and then select the **Documents** tab. Click on the **Add** button and enter **main.html** into the dialog box that appears and click **OK**. Next, remove the **default.htm** and **default.asp** documents from the list. Click **OK** to close the properties for the B and B Ice Cream web site. Remember, this step is done to specify which page from the web site should be loaded first whenever a user visits the site (main.html is the name of the file created earlier in this lab).



8. Notice that, in the left pane of the Internet Services Manager, the B and B Ice Cream web site shows as being stopped. Right click on the **web site** and select **Start** to try and get it going.



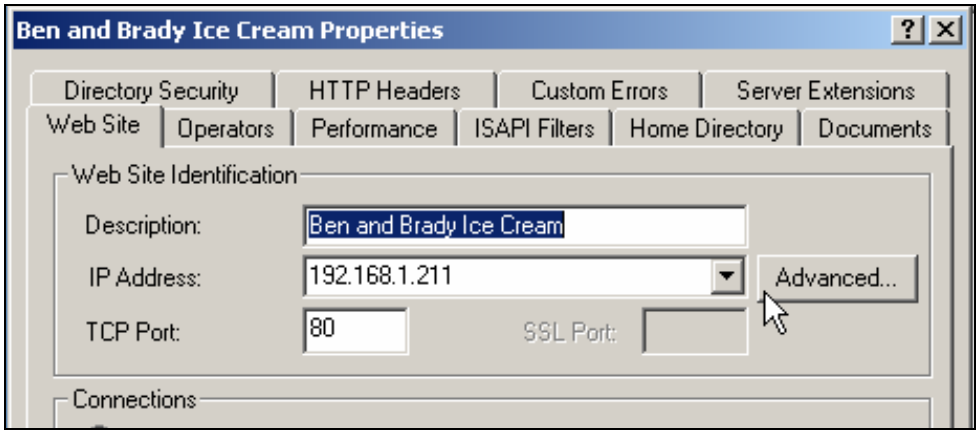
9. You will get an error message telling you that a duplicate name exists on the network. Click **OK**.



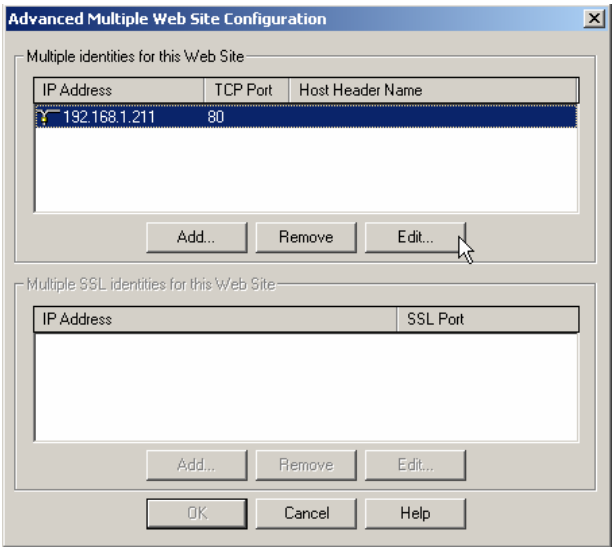
Creating host headers to differentiate between the two web sites

The reason that you are getting the error message is that you did not specify how the web server will differentiate between the two web sites. Therefore, it will not allow you to create a second website until you do so. There are a few ways to set up different web sites on the same web server. One way is by using different IP addresses for each web site - in this instance you will need to have more than one NIC or multiple IP addresses assigned to one NIC. Although this may be the easiest way to separate the two web sites, the company only has one public IP address at its disposal with no plans of getting another, so even if you add a second NIC you will still need another public IP address in order for this to work. The second way is by giving the web sites different port numbers – this can cause problems as the default port number for Internet browsers is 80. Changing the port number would mean that users trying to connect to the website would have to specify the port number after the address to get there. For example, if you change the port number for www.bandb-icecream.com to 81**,** then users will only be able to access the web site from Internet Explorer by entering **www.bandb-icecream.com:81** as the address. That would work fine in principle, but users aren't generally aware of port numbers and it would be difficult to have to remember port numbers if every website on the Internet required different port numbers. The third option is to give each web site a unique host header name. Assigning a unique host header name to each web site will allow the web server to read the name in the host header (provided by the URL that Internet users type in) and point them to the correct web site. In this case, Ben & Brady's best option is to use host headers in order for the web server to know which web site is being requested.

1. Open the **Properties** page of the Ben and Brady Ice Cream web site. On the Web Site tab click on the **Advanced** button that is located on the right of the IP address under the Web Site Identification section.

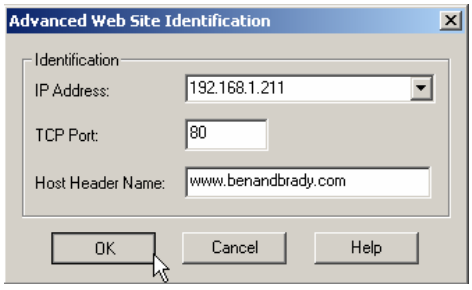


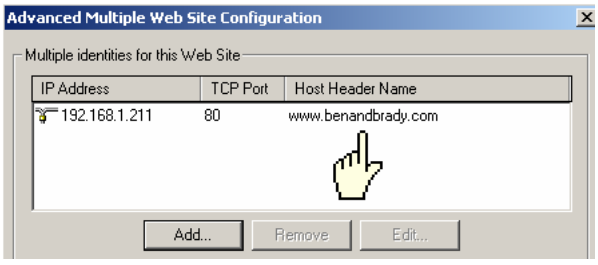
2. This will open a screen for Advanced Multiple Web Site Configuration. This is where you add or change settings for the identification of a web site. The only identity that will appear right now is the one you created in the new web site wizard. Select the only identity that appears and click **Edit**.



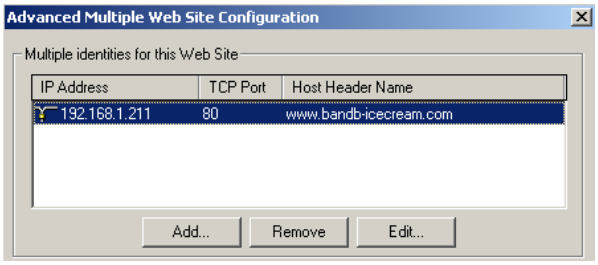
3. This opens up another screen where you can change the settings of the identity that you selected. You don't want to change the IP address or port number but you do want to add a host header name for the web server to identify it with.

   Type **www.benandbrady.com** into the space next to Host Header Name and click **OK.** This will take you back to the Advanced Multiple Web Site Configuration, where you should now see the host header name www.benandbrady.com with the only identity. Click **OK** to close and save any changes you made to the web site identification.

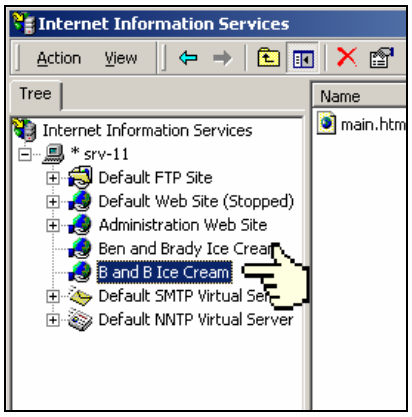




4. Next, change the Web Site identity for the B and B Ice Cream web site by adding the host header name of **www.bandb-icecream.com**. (Follow the same steps as changing the host header name for the Ben and Brady Ice Cream web site).



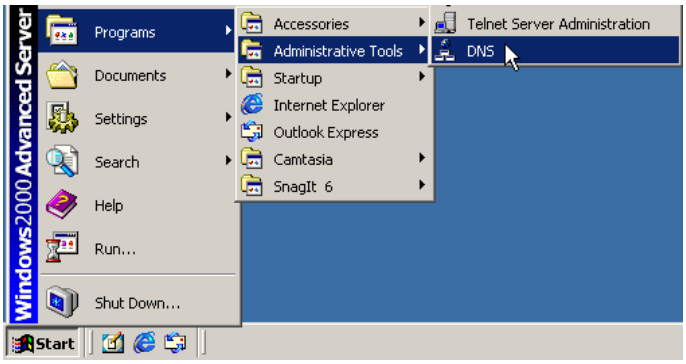
5. After adding host header names to both web sites, try to start the B and B Ice Cream web site again. You should be able to start it with no problem this time.



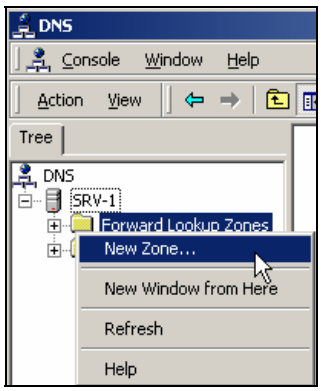
Configuring DNS for the second website

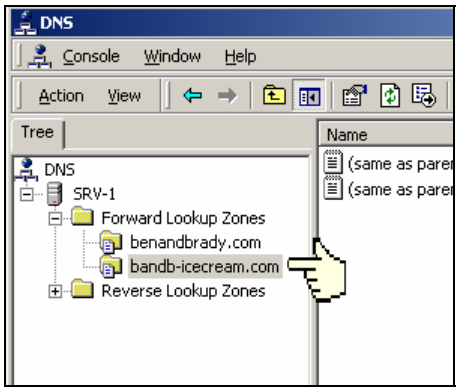
The next step in getting the web site up is to create a DNS forward lookup zone so that Internet users will be able to resolve the DNS name of www.bandb-icecream.com to an IP address and connect to it. Remember that in a real life situation it is typically best to have DNS configured on your ISP's public DNS server and this is what we are simulating in this lab as well.

1. Log on to **SRV-1** with the administrator account and open the **DNS** management console. Go to **Start→Programs→Administrative Tools→DNS.**



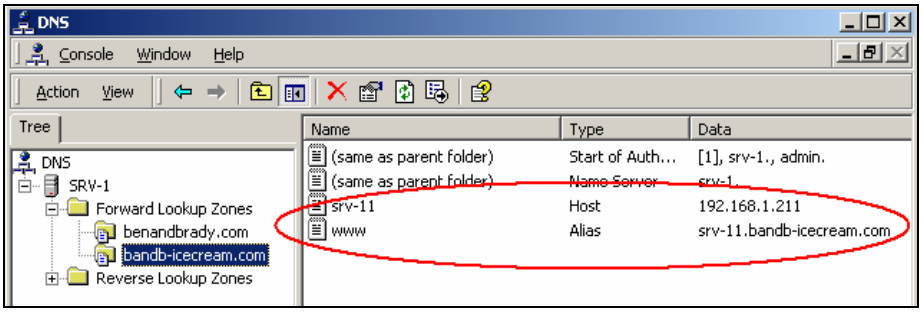
2. This time you need to create a forward lookup zone and resource records for bandb-icecream.com so the clients on the Internet will be able to resolve the DNS name to the IP address. Right click on the **Forward Lookup Zone** folder under SRV-1 and select **New Zone** from the shortcut menu. This will start the Forward Lookup Zone wizard. From the wizard select a new **Standard primary** zone, enter **bandb-icecream.com** as the new zone name, and leave the default name of bandb-icecream.com.dns for the DNS zone file. After clicking finish, you should now have two Forward Lookup Zones, one for each web site.





3. The next step is to create a host and an alias record in the bandb-icecream.com zone for the web server. Open the **bandb-icecream.com** Forward Lookup Zone and create a **New Host** record for SRV-11 by right clicking on **bandb-icecream.com** and selecting **New Host.** Next specify **SRV-11** as the name and enter **192.168.1.211** as the IP address. Follow this up by creating a **New Alias** record with **www** as the alias name pointing to SRV-11.

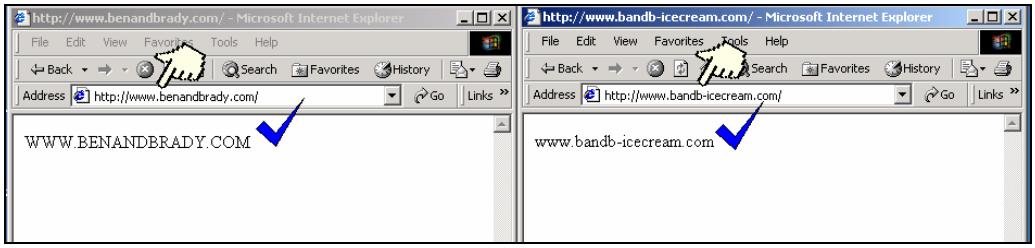
   You should now have a host record for SRV-11 and an alias record for www appear in the right pane of the DNS console for the bandb-icecream.com zone. Close the **DNS** management console.



Test and view website from client

1. Log on to **Client-1** as any user and open the **Internet Explorer** browser.

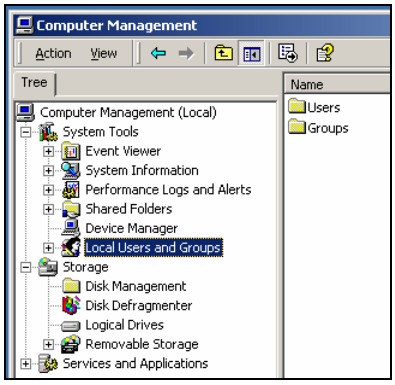
2. In the Internet Explorer address box enter **www.bandb-icecream.com** and click **Go**. You should be taken to the B and B Ice Cream web site that you created. Now open another Internet Explorer window, enter **www.benandbrady.com** into the address box and click **Go**. This should take you to the Ben and Brady Ice Cream web site that you created.



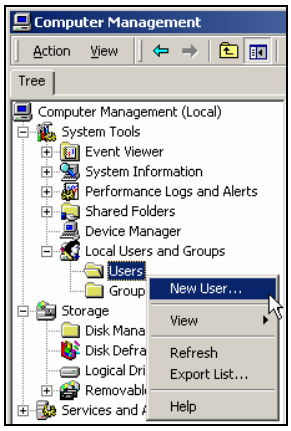
Assigning site operators

Site operators are allowed to change some but not all of the settings on the web site they are assigned to. You can make someone a site operator if you want them to manage a particular web site on a web server but **not** the web server itself. Site Operators are allowed to change the access permission, logging, default documents, HTTP headers, content ratings, footers and page content expiration. They are not allowed to change the IP address, TCP Port number, host header, bandwidth throttle, anonymous user account and password or create and modify any of the site's virtual directories. Since this web server is not part of a domain you will create a local user account for Bill, the web site developer. You will also need to create user accounts for each different partner company that you want to allow to connect to the partner web site.

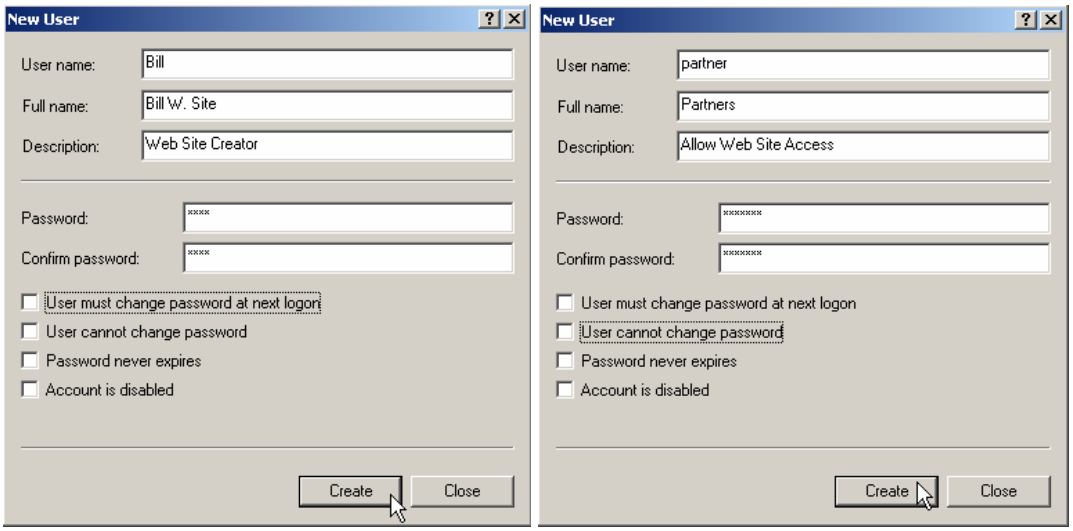
1. Log on to **SRV-11** with the administrator account and open the **Computer Management** console. Go to **Start→Programs→Administrative Tools→Computer Management**. Under system tools, open **Local Users and Groups**.



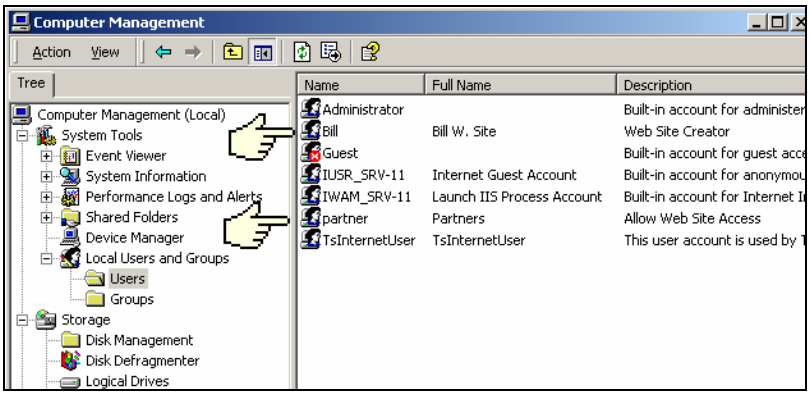
2. Right click on the **Users** folder and select **New User** from the shortcut menu.



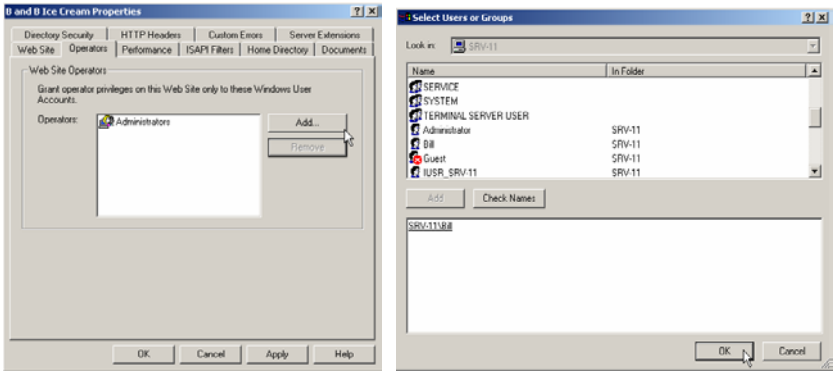
3. You will need to create users for Bill, the website designer, and a user account for each of the partners. For Bill, create an account with the User name: **Bill,** Full Name: **Bill W. Site** with a description of **Web Site Creator** and the password: **test**. For the partners, create an account with the username: **partner,** full name: **Partners** and a description of **Allow Web Site Access.** Set the password as: **vanilla**. Close the **New User** screen when you're done.



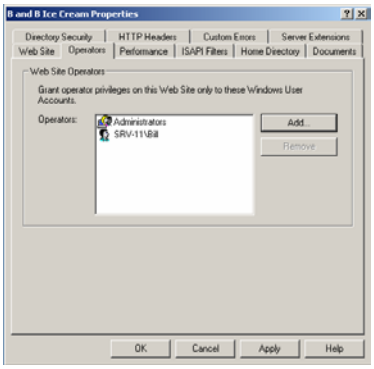
4. Now check to make sure that both users appear in the local Users container. Close the **Computer Management** console when you are done.



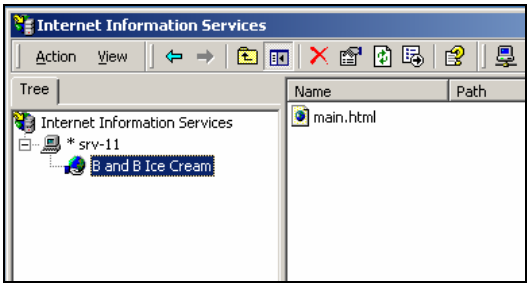
5. Open **Internet Services Manager** and open the **Properties** of the B and B Ice Cream web site. On the Properties page, select the **Operators** tab, then, on the operators tab, click on the **Add** button to add a new operator. A list of available Users and Groups will appear. Find and select the user **bill** and then click **OK**.



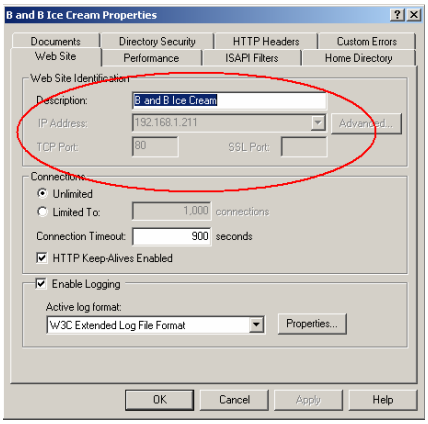
6. You should now see the user account srv-11/bill within the list of Operators. This only allows Bill to work on the B and B Ice Cream partner site and **not** the public site. Click **OK**.



7. Log off **SRV-11** and log back on with the username **bill.** Open the **Internet Services Manager.** Notice that the only site available to this user is the B and B Ice Cream web site. Even though there is another web site being hosted on the web server, this user can only access the B and B Ice Cream web site.

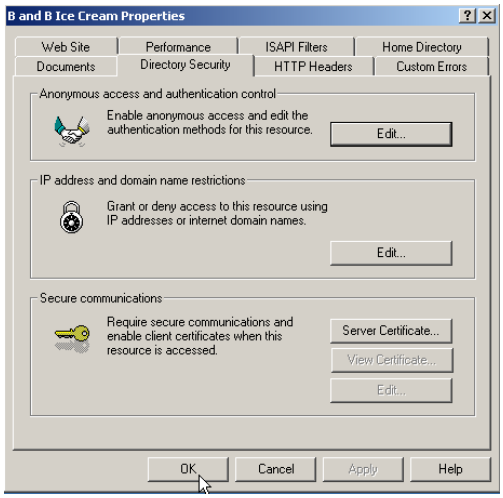


8. Open the **Properties** of the B and B Ice Cream web site. On the web site tab notice that IP address, TCP Port and the Advanced button are all grayed out – as a web site operator this user cannot modify any of these settings.



Adding security to a website

1. Select the **Directory Security** tab. On this tab you have three different choices for applying security to a web site. The first method is to select the way users will be authenticated to the site. The second is to grant or deny access to the site by using IP addresses. This method would be difficult to manage because there are so many different IP addresses on the internet making it tough to keep track of who to grant or deny access to. The third method allows you install a server certificate that will encrypt data going across the Internet. This involves Secure Socket Layer encryption and is commonly used for credit card transactions on the Internet.

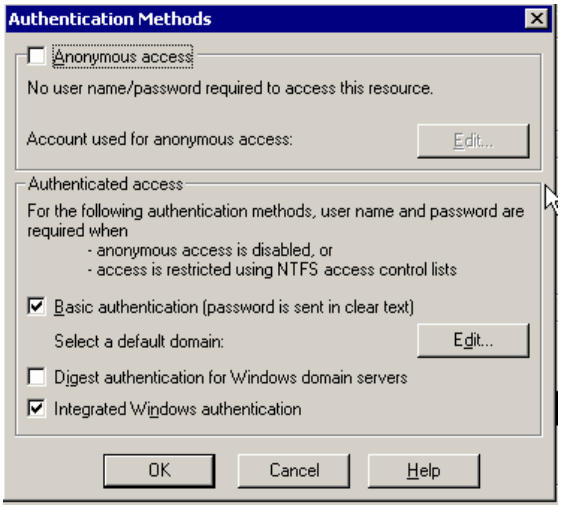


2. You want to set security so that only partners who are given permission can access the web site. Click on the **Edit** button under the Anonymous access and authentication control section. By default Internet browsers are allowed to access a web site anonymously, so the web server is set to allow anonymous access. Un-checking the Anonymous access box will prevent anonymous users from being able to access your web site. This is exactly what we are trying to accomplish for our partner site.

   Integrated Windows authentication requires the user to have a valid username and password to gain access to the site. Disabling Integrated Windows Authentication as well (all boxes are unchecked), will prevent any access to the web site. You can also select the box next to Basic authentication. Basic authentication will allow users that use a browser other than Internet Explorer (i.e. Netscape Navigator) to connect to your site as well, at the expense of unencrypted usernames and passwords being passed over the Internet.

   How do you decide? Well, Basic authentication is the most compatible solution (Internet Explorer and Netscape Navigator will work) but also provides the lowest security. Selecting only Integrated Authentication will provide you with higher security but Netscape Navigator users will be out of luck. The best alternative is to usually select both options (or require your partners to use Internet Explorer). If you select both options, Integrated Windows authentication would be attempted first and Basic authentication would only be used if Integrated authentication was unsuccessful

   If your site contained highly confidential information you would not want to use Basic Authentication at all. Check the boxes for both **Integrated Windows authentication** and **Basic Authentication** and click **OK**. Any user connecting to this site will now be required to enter a username and password.

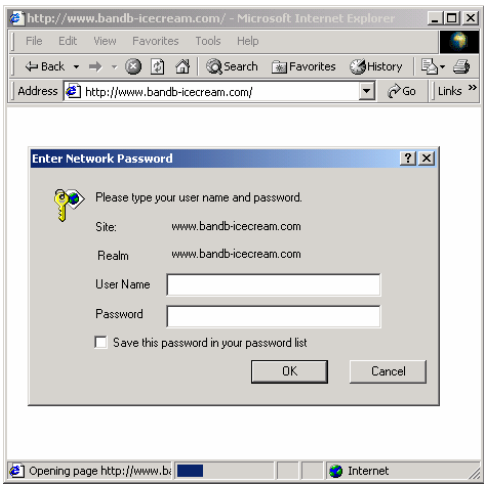


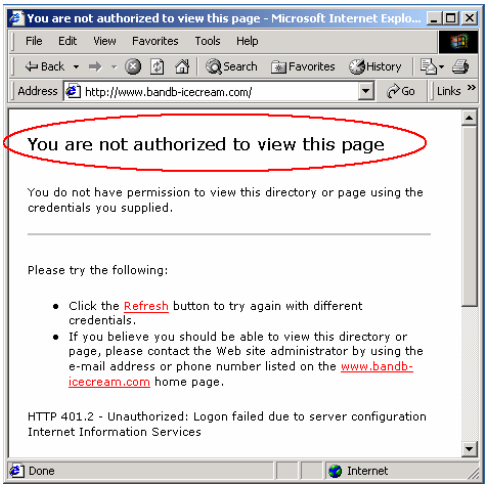
3. Remember that you still have NTFS security set on the root directory for the web site. This means that, if an unauthorized user gets a partner's user name and password, the worst thing they can do is read the information posted on the web site. Click **OK** to close the Authentications Method page. Then click **OK** on the B and B ice Cream web site Properties page to close it and have the new authentication method applied to the web site. Now whenever Internet users go to the B and B ice Cream web site they will have to enter a valid username and password. Log off **SRV-11**.

Test and view the website from a client

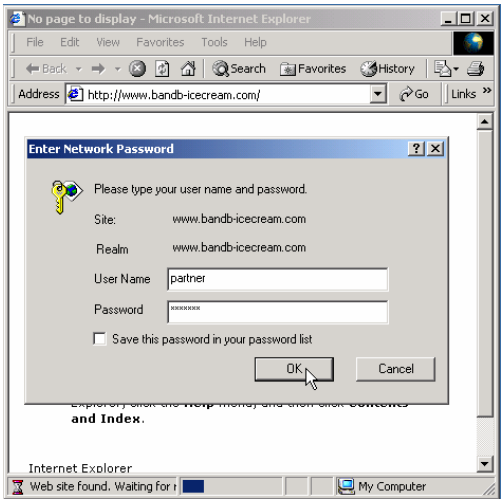
1. Log on to **Client-1** as any user and open the **Internet Explorer** browser.

2. In the Address box type in **www.bandb-icecream.com** and click on **Go**. Before you can enter the web site you will be prompted for a username and password. Click on **Cancel** until you get an error message that you are not authorized to view this web page.

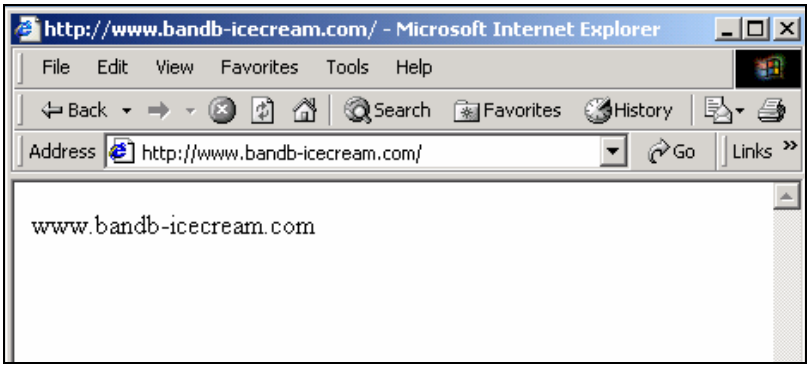




3. Next, try clicking on the **Refresh** button in the toolbar and you will be prompted to enter a username and password again. This time enter the username and password for the partners account that you created earlier. The user name is **partner** and the password is **vanilla.** Click **OK**



4. This should take you right into the main page that you created for the B and B Ice Cream web site.



Lab 3

Securing Ben & Brady's Web Server

You will learn how to:

- Download and install service packs and hot fixes
- Set NTFS permission
- Disable NetBIOS over TCP/IP
- Download and run the IIS lockdown tool from Microsoft
- Enable and view Logging

Scenario

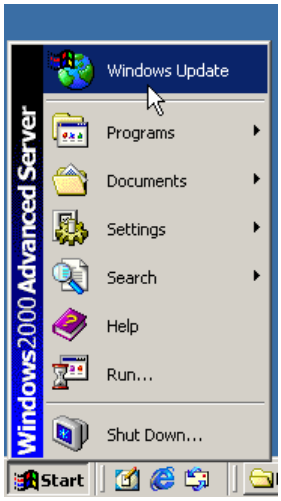
In your weekly meeting with Jill she brings up the issue of security on the web server. You tell her that you have set up some basic security but you haven't fully gone through and locked down the server. She wants to implement some new corporate security policies now that the company is hosting its own web server, so you both agree to do some more research and discuss any new policies in next week's meeting. In the meantime she wants you to lock down the web server as much as possible and also look for other potential problems. She gives you a few ideas of how to lock down the server including a URL on Microsoft's web site where you can download a tool to help lock down the web server.

In this lab you will learn some common and basic steps to securing a web server. You will also use a tool that can be downloaded from Microsoft to help you lock down the web server. Lastly, we will cover some security policies that will help keep the web server secure. Keep in mind that security is a very complex topic and the suggestions in this lab are just a start. To keep your network secure, you will have to be diligent in staying on top of the latest security briefings and hot fixes, especially with a web server.

Downloading and Installing Service Packs and Hot Fixes

The best way to keep your server up to date with service packs and security hot fixes is to periodically check the Microsoft website. Windows 2000 comes with a link on the Start menu named Windows Update that will take you directly to the Windows update web page. There you have the option of scanning your computer to see if there are any updates that your computer may need to download and install.

1. Log on to **SRV-11** with the administrator account and go to **Start→Windows Update** from the desktop.



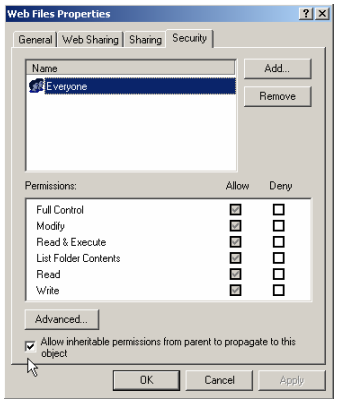
2. This will open up Internet explorer and take to you to windowsupdate.microsoft.com, Microsoft's automated update site. From there you can have your machine scanned to see which updates your server needs. Some of the updates may not apply to you, so make sure that you investigate what each download will do to your system before installing it. You have the option of removing or adding any downloads that you want. Some downloads may need to be downloaded and installed separately from others, which requires you to reboot your machine and go back to the Windows Update site several times before you completely update your system. Although this is time consuming and it may seem like a pain, you should make sure to do this on a regular basis. Keeping up with any new service packs and security hot fixes is especially important on a web server.

Setting NTFS permissions

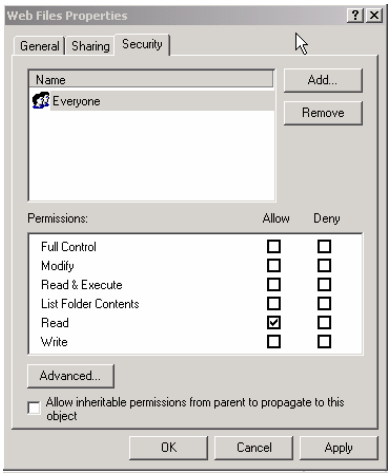
After installing all of the updates, your next basic step for web server security is to set NTFS permissions. You should set the permissions on the root directory where your web site files are stored. This will allow the permissions to automatically flow down and apply to all web sites files within the web site's directory. If any file or directory within your web site needs a different set of permissions you can set them individually on the specific folder or file, which will override any permissions set on the root directory.

1. Log on to **SRV-11** with the administrator account and open **Windows Explorer.** Open the **C: drive** and right click on the **Web Files** folder, which is the root directory for the web site files being hosted on this server.

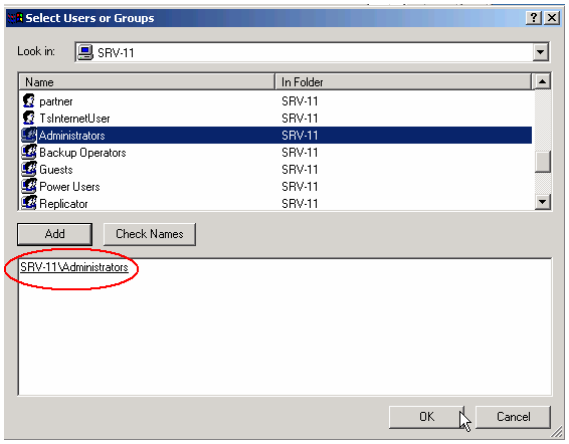
2. On the properties page select the **Security** tab. Notice that there is only one group on the security list. That group is the Everyone group, which has Full Control permissions by default. Full Control permissions are inherited from the parent directory (the drive in this case) that the folder resides in, the C: drive. In order to change the permissions on this folder you must first remove the option that allows inheritable permissions. Un-check the box at the bottom of the security tab that says **"Allow inheritable permissions from parent to propagate to this object.**"

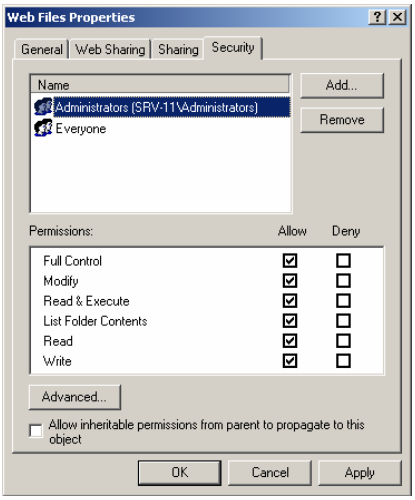


3. A small screen will appear asking what you would like to do with the propagating permissions. You are given 3 options, one is to Copy the permissions to this folder, the second is to Remove all permissions and assign them yourself and the third option is to simply Cancel the removal of inheritable permissions and not change anything. Click on **Copy.** This will bring you back to the Security tab where you should still have the Everyone group on the security list, only now the box at the bottom is empty and you can now change the permissions for the Everyone group. Select **Everyone** and give the group only **Read** permission to this folder then click **OK** when finished.

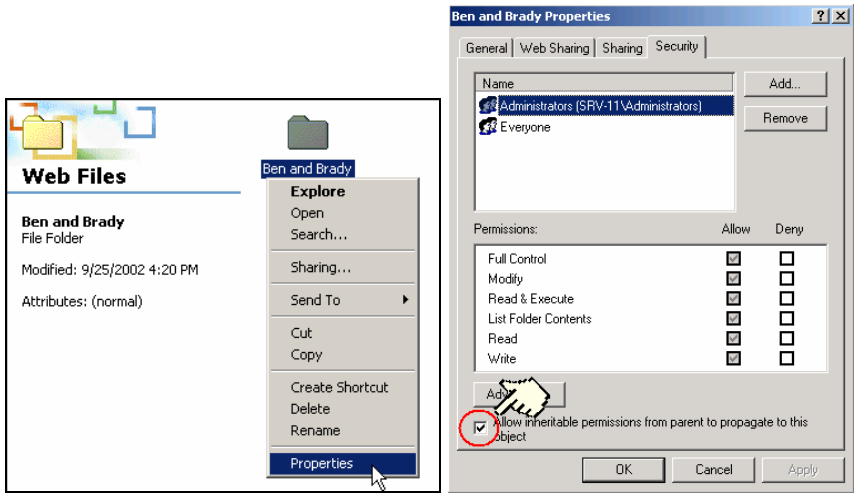


4. Click on the **Add** button and select the **Administrators** group from the user and group list, then click **OK.** Next, give the Administrators group **Full Control** permissions for this folder. Then click **OK** to close the Properties page for the Web Files folder.

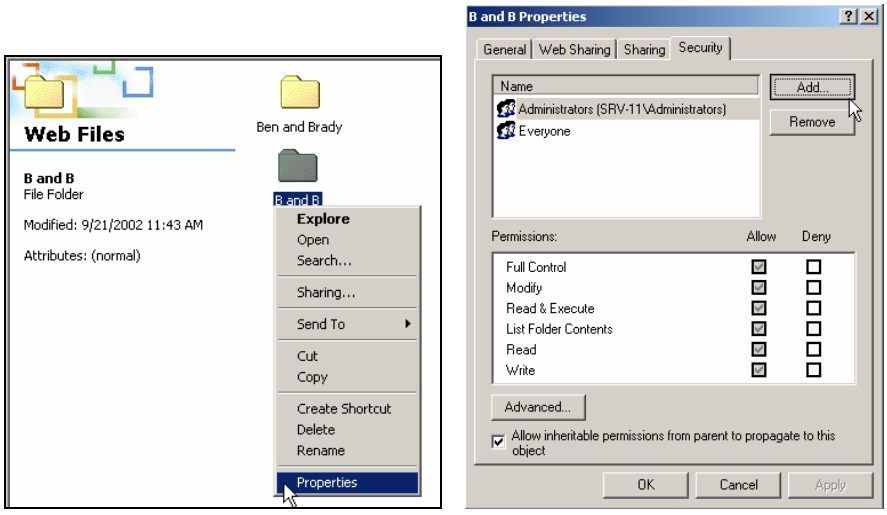




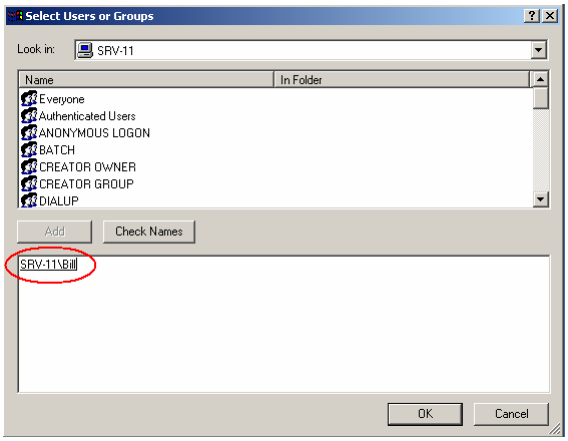
5. In Windows Explorer open the **Web Files** folder and open the **Properties** page for the Ben and Brady folder that contains the files for the Ben and Brady Ice Cream web site. Click on the **Security** tab and notice that the permissions are identical to the permissions set on the Web Files folder. This is because the permissions are being inherited from the parent folder. Leave the permissions as is and click **OK** to close the Properties page.

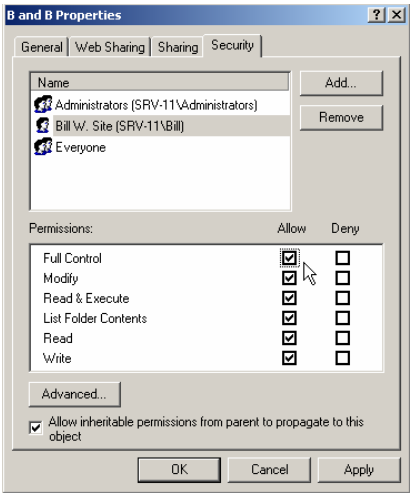


6. Now open the **Properties** for the B and B folder that contains the files for the B and B Ice Cream web site. Click on the **Security** tab and notice that the permissions are also the same as the Web Files folder because it is also inheriting the permissions from the parent folder.



7. The next step is to assign the user account Bill permissions to this folder so that he can manage the web site for B and B Ice Cream. First click on the **Add** button**,** then find the user account named Bill (created in Lab 2) from the user and group list, then click **OK**. Bill should be assigned Full Control permission for this folder. By giving this user full control permissions to this sub-folder instead of **the Web Files** folder, you will be limiting him to Full Control only within this folder, instead of having Full Control over all of the web sites. Click **OK** and close **Windows Explorer**.

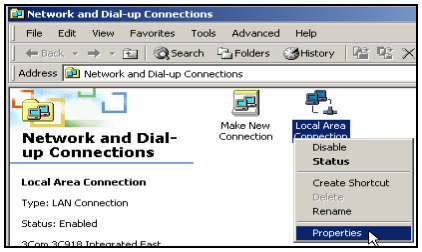




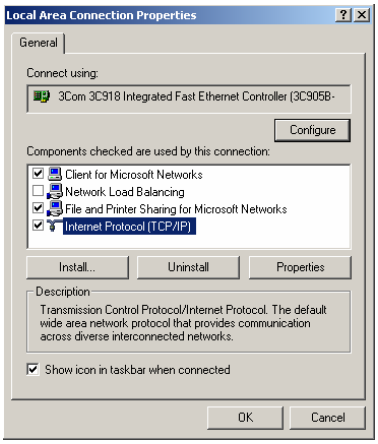
Disabling NetBIOS over TCP/IP

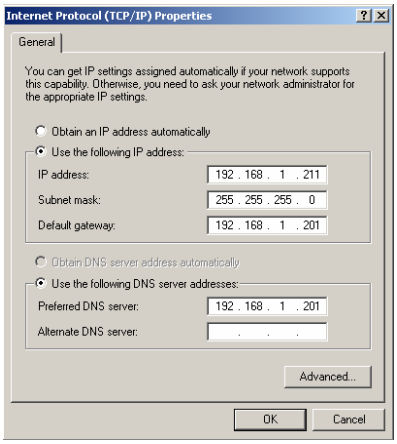
For a Web Server on a public network it is good practice to disable NetBIOS over TCP/IP. NetBIOS is an Application Program Interface (API) that is used to allow Microsoft computers to communicate on a network. Windows 2000 computers enable NetBIOS as part of the default installation, which allows them to communicate with legacy clients such as W95/98 or NT4. It is not necessary for a Web Server (in most cases) to be running NetBIOS and disabling it will make your system more difficult to attack. NetBIOS can be disabled individually on a system or in mass, through DHCP. You also want to unbind the TCP/IP protocol from the client for Microsoft Network service in the Advanced Settings to make sure that NetBIOS is completely disabled.

1. Right click on **My Network Places** and select **Properties** to open the Network and Dial up Connections. Right click on the **Local Area Connection** and select **Properties**.



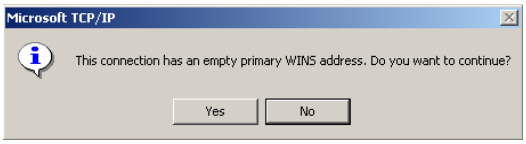
2. On the Properties page select **Internet Protocol (TCP/IP)** and then click on the **Properties** button to open the Properties page of Internet Protocol (TCP/IP). On the Properties page for Internet Protocol (TCP/IP) click on the **Advanced** button to open the Advanced Settings page for TCP/IP.



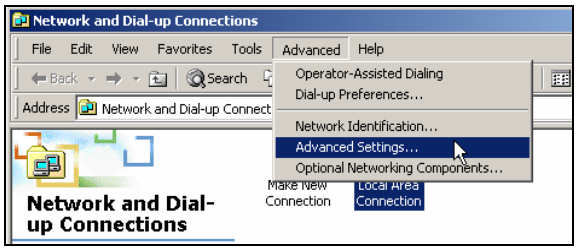


3. On the Advanced TCP/IP settings screen select the **WINS** tab. On the WINS tab remove the check that is placed in the box next to Enable LMHOSTS lookup because there are no LMHOSTS being used on this server. Then select **Disable NetBIOS over TCP/IP**, and click **OK**.

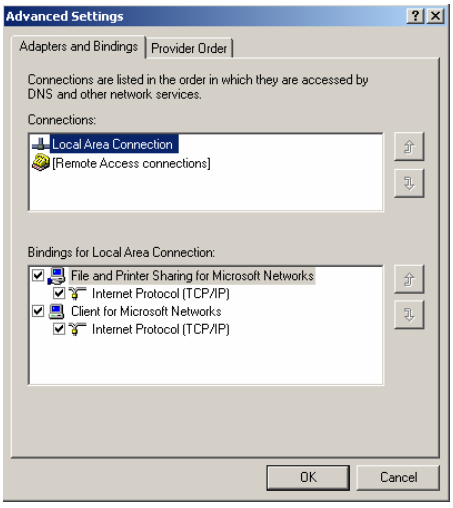
4. After you click **OK** you will get a warning telling you that the connection has an empty primary WINS address. This warning does not concern you because NetBIOS is now disabled and the web server does not require a WINS server to function. Click on **Yes** to continue and then click **OK** until you get back to the Network and Dial-Up connections page.

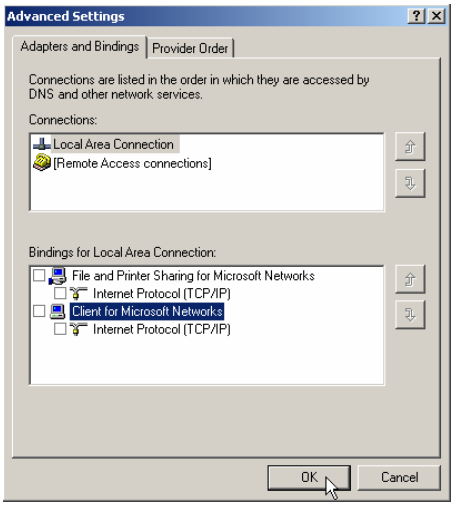


5. From the Network and Dial-Up connections page select **Advanced→Advanced Settings** from the menu**.**



6. From the advanced settings you can unbind different protocols and services that may be used on this computer. Un-check the boxes with **Internet Protocol (TCP/IP),** notice that it will automatically un-check the box in the tree above it as well. In this case the only protocol that is being used is TCP/IP. Therefore, removing it from the binding list will also disable the network service that is using it. File and Printer Sharing for Microsoft Networks and Client for Microsoft Networks will now be disabled. Click **OK**.





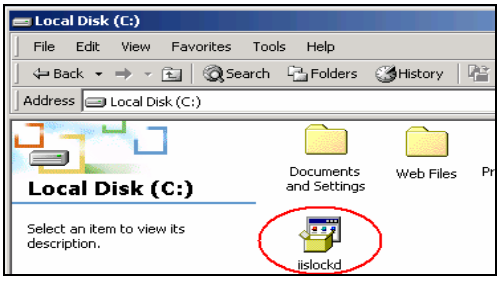
Download and run the IIS lockdown tool from Microsoft

Now that you have disabled NetBIOS over TCP/IP you should download and run the IIS lockdown tool from the Microsoft website to take a look at a more automated approach to locking down your Web Server. You can find the tool by doing a search on their website or the tool is currently available at this link:

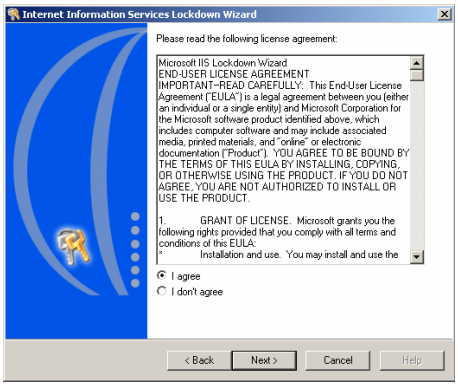
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=43955.

This tool is a wizard that will walk you through the basic steps of locking down your web server. You can always go through and make all the necessary security settings yourself but this wizard makes it a lot easier to ensure that you have at least all of the basics covered. The nice thing about this wizard is that it helps you secure your server by asking questions but you still have the final say on what to keep or what to get rid of.

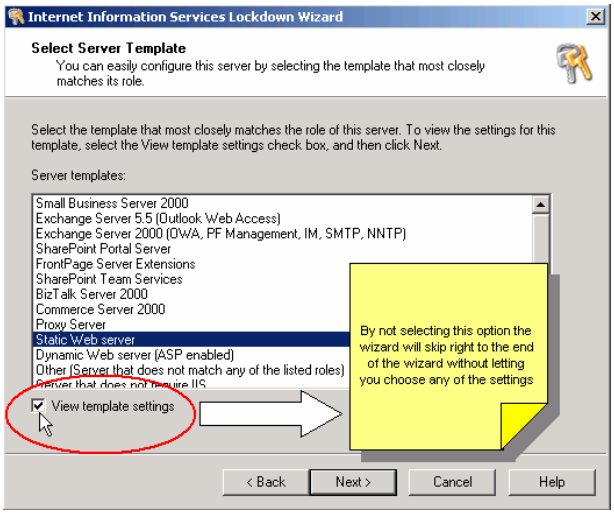
1. Download the IIS lockdown (**iislockd)** tool to your **C: drive**. Then double click on the file to run the tool on the server.



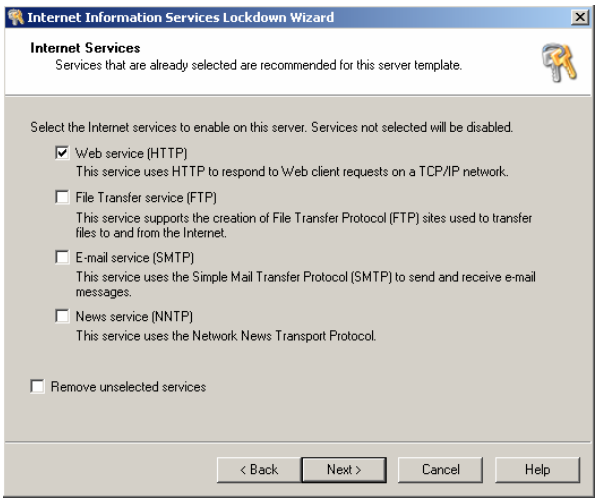
2. The first screen is a welcome screen giving you a description of the wizard you are about to run. Click **Next** on the next screen and you will be asked to read and agree to the End-User license agreement for Microsoft. Read the agreement and select **I agree.** Remember that if you don't agree to the license agreement you will not be able to continue. Click **Next**.



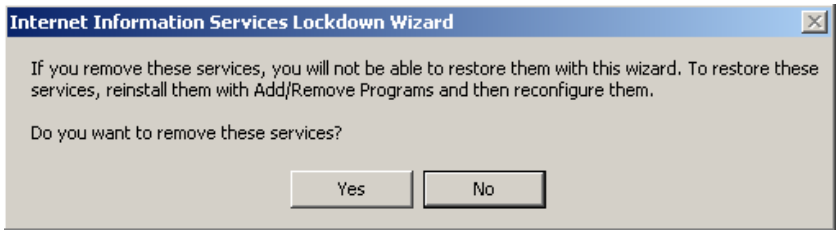
3. The next screen will ask you to select the template that matches the role of your server. In this case the template that best matches your server is the Static Web server. Select **Static Web server** and then check the box on the bottom of the screen that says **View template settings** next to it. Click **Next**.



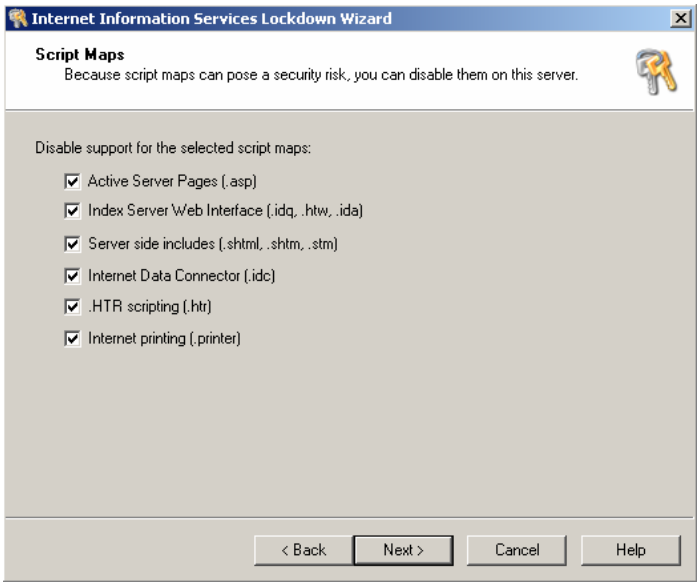
4. The next screen of the wizard will ask you to choose which Internet services you would like enabled for this server. This server will only be running the Web service so the other services must be disabled or removed. Make sure that **Web service (HTTP)** is selected from the list of Internet services. Then select the box next to **Remove unselected services**.



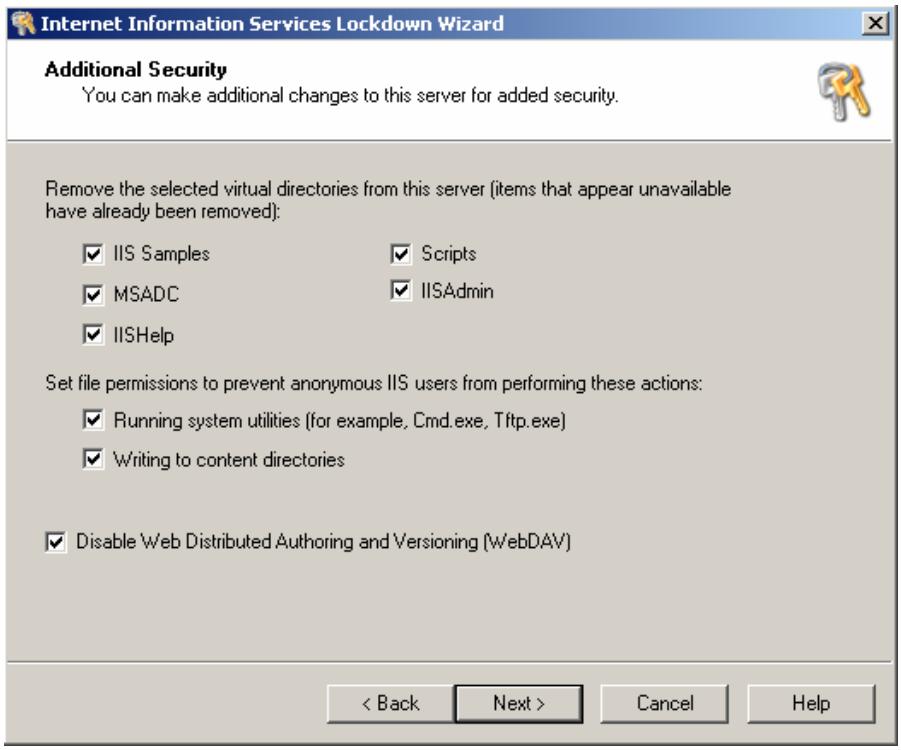
5. A warning will appear telling you that selecting this option will remove the services from the server and that the only way to restore these services will be by reinstalling them through the Add/Remove Programs applet. If you select No, the services will just be disabled on the server. Selecting Yes will uninstall the services completely. For a more secure server you will be better off removing any services that are not used. It is simple to reinstall any services from the Add/Remove Programs applet if the company ever decides to use one of these services in the future. Click on **Yes** then **Next** on the wizard to continue.



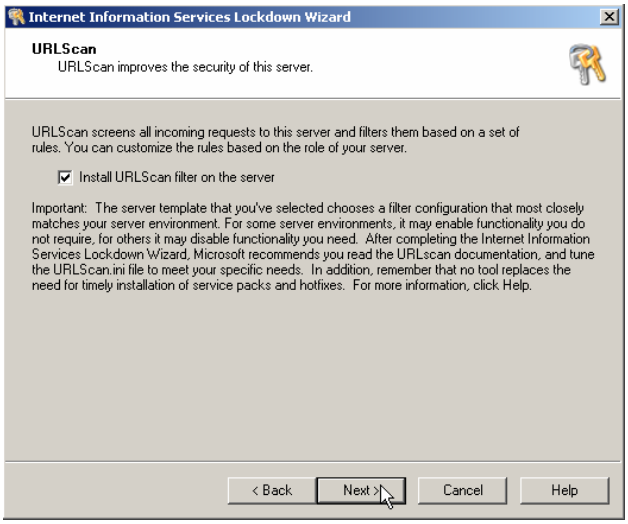
6. The next screen of the wizard will ask you to specify which script maps you would like to disable. Script maps can be used to run malicious codes that can do harm to a web server. Because they therefore can pose a security risk you should disable any that are not being used. Both web sites that are being run are simple and do not require any script maps to be used. So select **all** of the script maps on the list and disable them. You can always go into the properties of the web site and add any script maps you may need in the future. Click **Next** to continue.



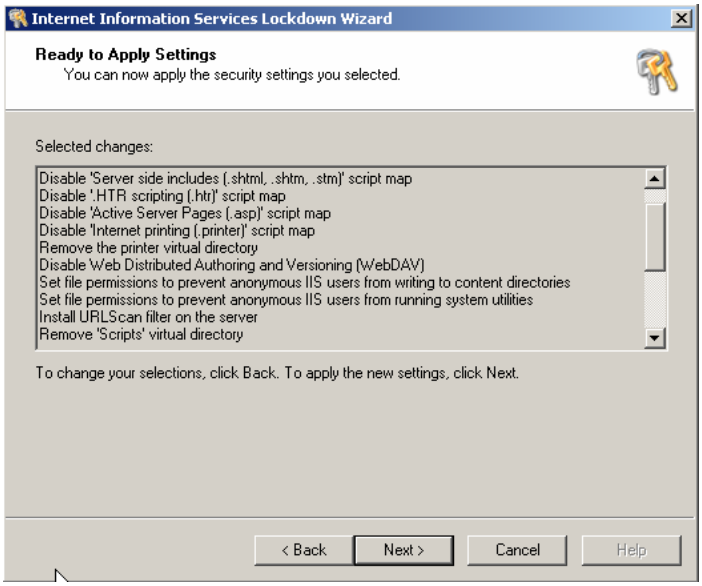
7. The next screen of the wizard allows you to configure additional security on the web server. The first portion will remove any virtual directories that are not being used. In most cases it will be directories that were created by default when IIS was originally installed. These include the virtual directories for IIS Samples, IIS Help, IIS Admin, Scripts and MSADC. Select **all** of the virtual directories that appear on the wizard for removal. The next section allows you to set permission in order to restrict anonymous IIS users from running any system utilities or from writing to any of the directories. Select **both** of the file permissions that prevent the users from running applications and writing to the web server. The last option that you have the ability to disable is WebDAV. WebDAV allows for online collaboration between different people. Users can publish their files and other users (with the proper permissions) can access these files and make changes if necessary. Unless you are specifically using this feature on your web site you should disable it. The only users who should be able to make changes to the web sites hosted by Ben & Brady's Ice Cream are the local administrator on SRV-11 and the user account Bill. Select the **Disable Web Distributed Authoring and Versioning** option and click **Next** to continue.



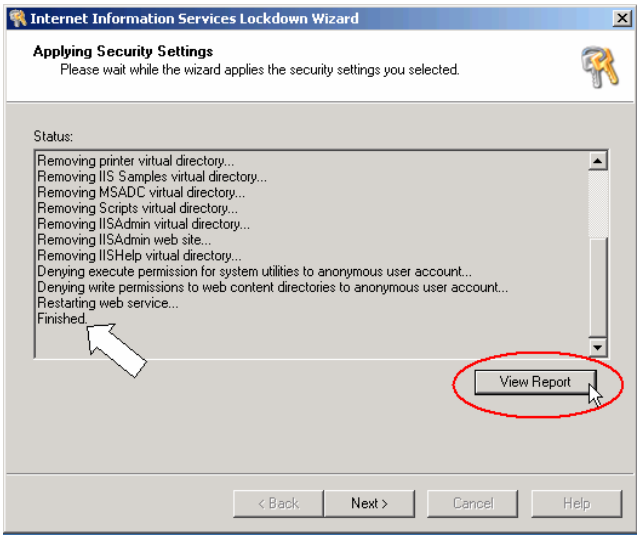
8. The next screen of the wizard will ask if you would like to install URLScan, which filters all incoming traffic by a set of rules. The wizard will automatically set rules for you based on the configuration that you selected earlier in the wizard (Static Web Server). You can always change the rules later to fit whatever needs you may have for the web server. The default option is to install URLScan. Leave it selected and click on **Next** to continue.



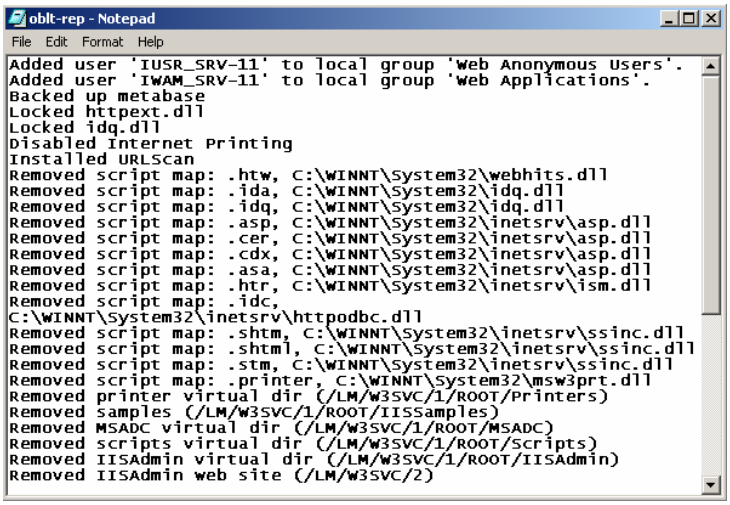
9. On the next screen, you will be shown all of the changes that will be made to the web server based on the information you provided in the wizard. Review the changes to make sure they're all correct and click **Next** to for the wizard to make the changes.



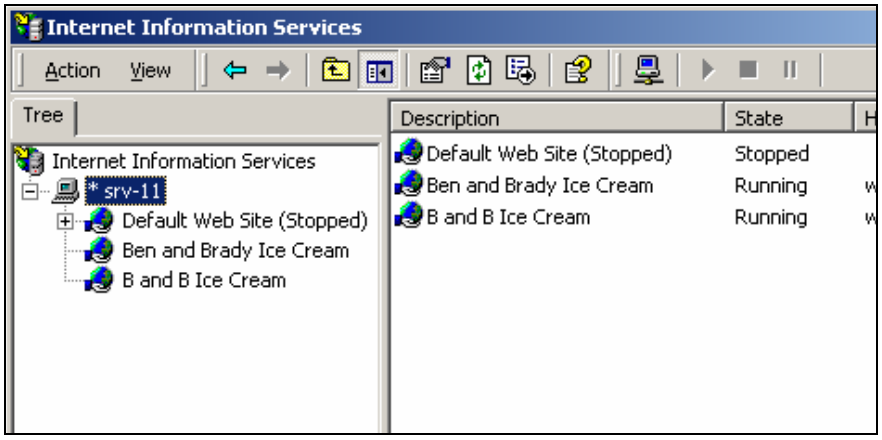
10. The wizard will inform you when it is done making the changes with the message Finished in the Status window. It will also have the option of showing you a report in the form of a text document that shows all of the changes that were made. Take a look at this by clicking on the **View Report** button.



11. This will open a text document using Notepad. From here you have the ability to print the report so that you can have documentation as to what was done to the server with this wizard. Close **Notepad** and click **Next** on the wizard to continue. This will take you to the last page of the wizard, which just tells you that you have successfully completed the IIS lockdown wizard and tells you the location (%windir%/system32/inetsrv) of the report file (oblt-log) that you just viewed. Click on **Finish** to end the wizard.



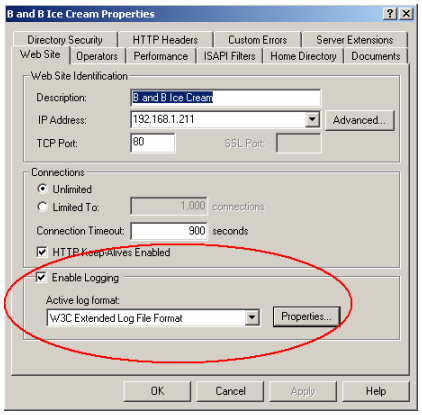
12. Next, open the **Internet Services Manager** to see if you notice any of the changes made in the wizard. The first difference you should see is that only web services appear in the left pane. The other services don't appear anymore because the wizard removed them.



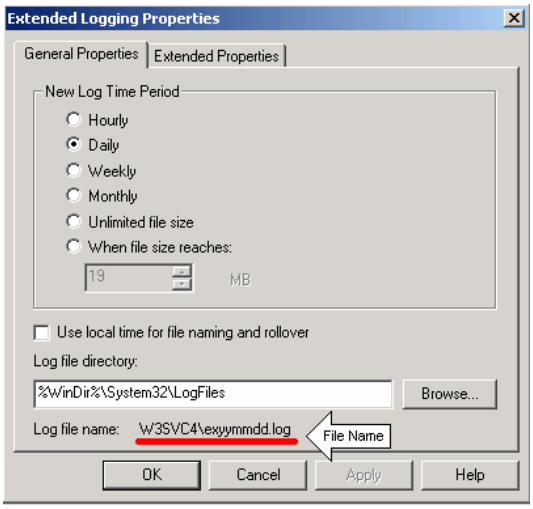
Enable and view logging

Logging is enabled by default when IIS 5.0 is installed. Logging is a great way to monitor if your server is being or has been attacked.

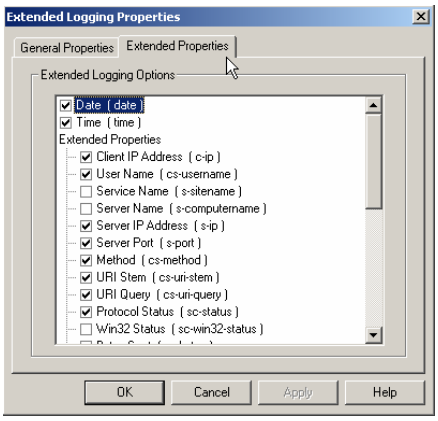
1. On the Internet Services Manager, right click on the **B and B Ice Cream** web site and select **Properties**. On the Properties page notice that logging is enabled using the W3C Extended Log File Format. There are three different formats that you can choose from on the drop down list but the W3C format is the most used log format because it lets you log more information than the other formats and is more flexible with specifying what information to log. Leave the default W3C Extended Log File Format and then click on the **Properties** button.



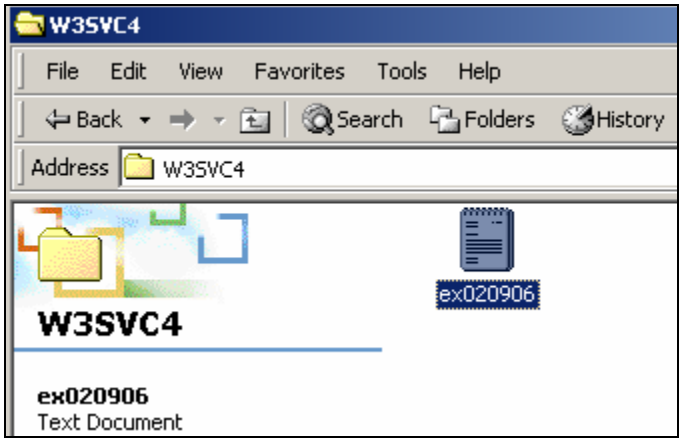
2. On the Logging Properties page, under the General Properties tab, you can specify how often a new log should be started and where the log file should be stored. By default the New Log Time Period is set to Daily and the Log file directory is %WinDir%\system32\LogFiles. Below the Log file directory location is the name of the folder the file is placed in and the naming scheme that is given to the log files. in this case the folder it's located in is W3SVC4 and the log file will be exyymmdd.log. The file name will start with ex, yy stands for the year, mm stands for the month and dd stands for the day of the log.



3. Next, click on the **Extended Properties** tab. On the Extended Properties tab you can select the information that you want to log. You should have the Date and Time selected by default as well as a few other basic options. Here is a list of some basic options you should select if they are not already selected already: **Client IP Address, User Name, Method, URL Stem, HTTP Status, WIN32 Status, User Agent, Server IP Address** and **Server Port.** Click **OK** and close the B and B Ice Cream web site **Properties** page.



4. Open **Windows Explorer** and go to **C:\WINNT\system32\logfiles\W3SVC4.** You should find a log file for the B and B Ice Cream web site. The log file will have a name that matches the days you have been working with this lab. If there isn't a log file there already open **Internet Explorer** and go to the **B and B Ice Cream** web site to give it some traffic and then restart the server.



5. Open one of the log files by double clicking on it. The results in your log will be different from the results that are logged in this file but the type of information that is logged should be the same. The first thing you will see on the log is the date and time of the event, then the client IP address of the computer that was trying to access the web site, the user name that was used to try to access the site followed by the web server IP address that it was accessing. After the server IP address will be the port number that was used to try to access the web site followed by the method (the type of action the client was trying to perform). After this, you will see the protocol status for the event in HTTP terms, for example a protocol status of 401 was unauthorized to view the site. You should research and get a list of all the HTTP protocol statuses and what they stand for to properly identify the events. At the end of the event logged you will see the user agent (Internet Browser) that was used to access the web site.