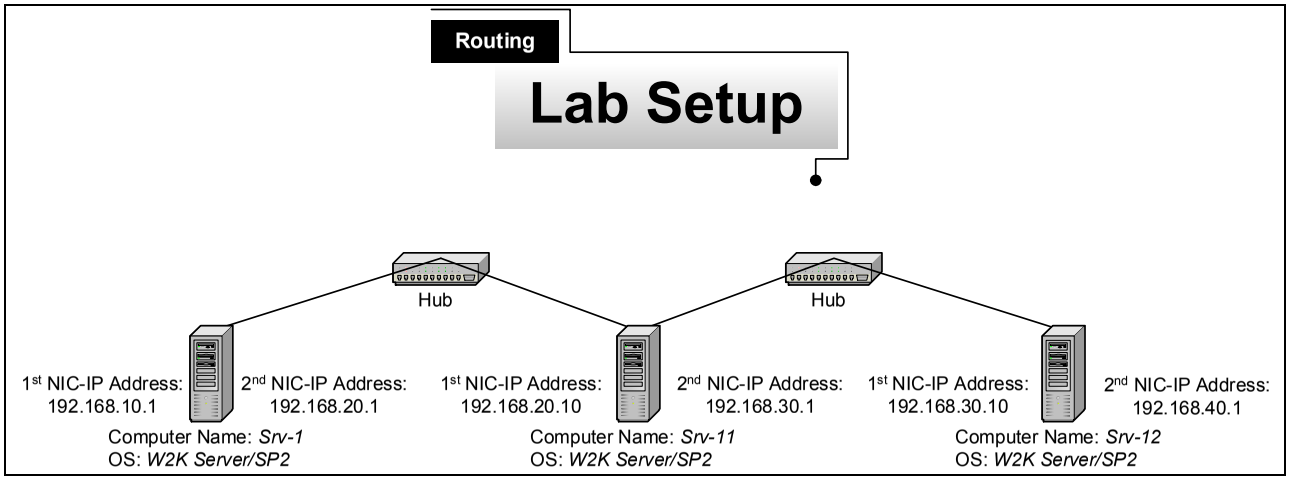
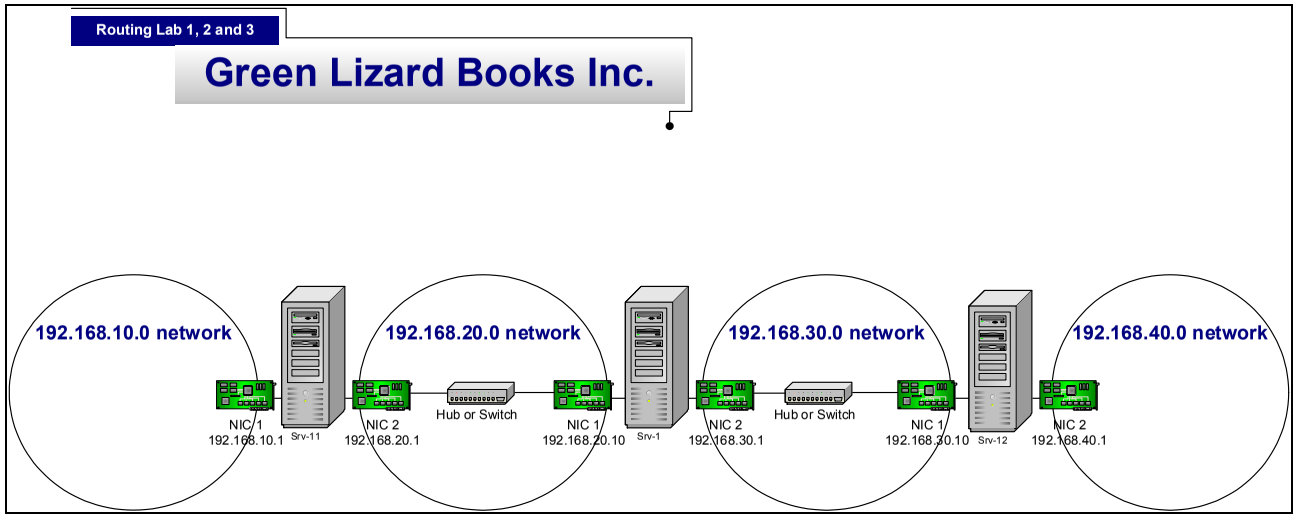
Configuring Routers, Routing Protocols and Packet Filters for Green Lizard Books, Inc.

Mega Lab 9

Part 3 of 3 in the Windows 2000/2003 Routing & Remote Access Series

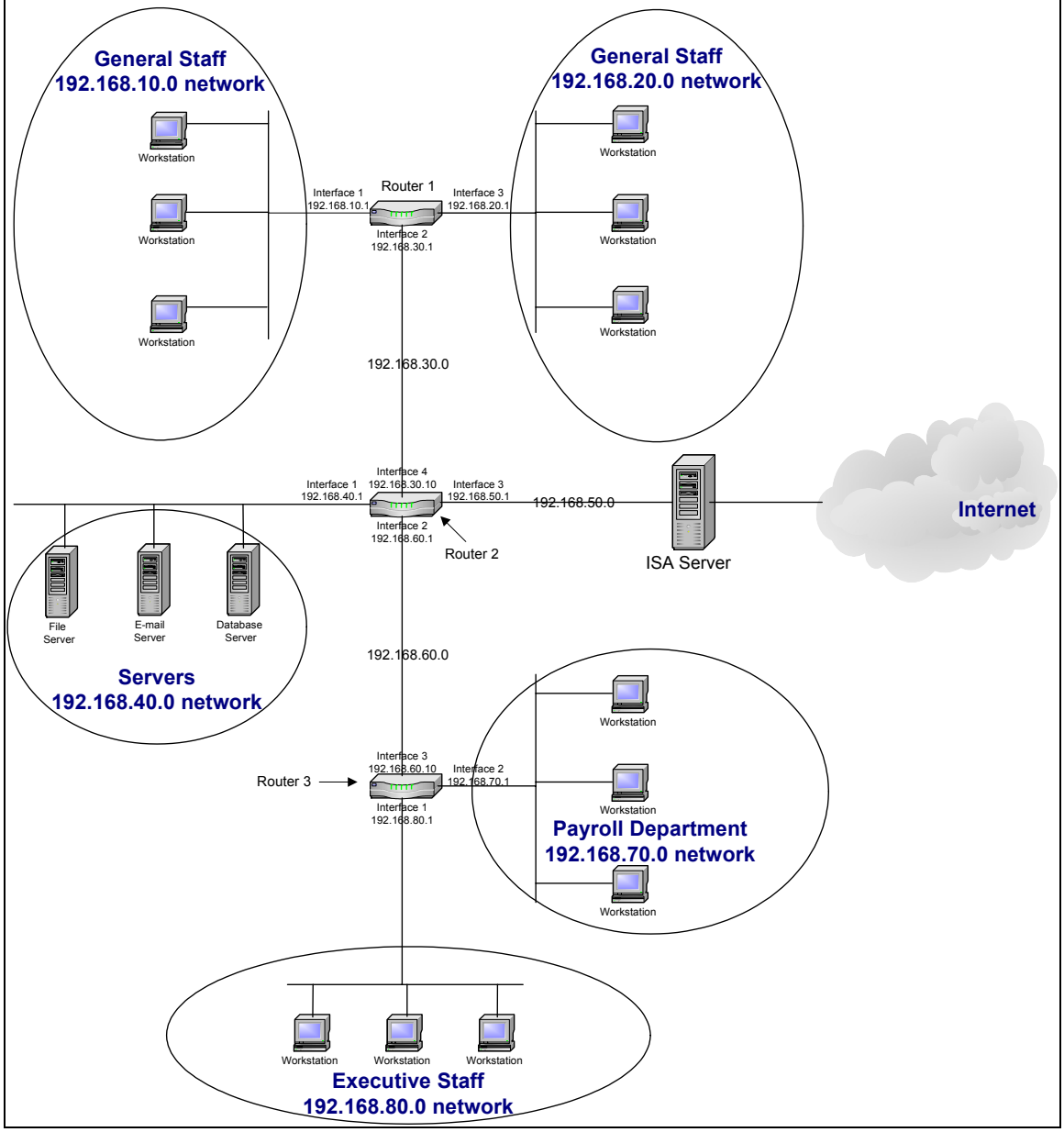




Company Environment

Green Lizard Books Inc.

Green Lizard's Network (Future Plan)



Configuring Routers, Routing Protocols and Packet Filters for Green Lizard Books, Inc

Mega Lab 9

Part 3 of 3 in the Windows 2000/2003
Routing & Remote Access Series

About the Authors

Scott Skinger (MCSE, CNE, CCNP, A+) is the owner of Train Signal, Inc. and is an experienced Windows 2000 instructor. He has also worked in the trenches as a Network Engineer, Director of Technology and currently as an Independent Consultant through his own company, SAS Technology Advisors. As an instructor, he has taught over 50 courses, covering topics such as Windows 2000, NT 4, Novell NetWare, Cisco Routers and security.

Wilson Chan (MCSA) is responsible for content development for the Routing and Remote Access Mega Lab Series. He also does network support, computer hardware repair and software support for a computer consulting company.

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 2000/2003 is designed to give you detailed, hands-on experience working with Windows 2000/2003. 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 2000/2003.

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 at least 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	2/machine	2/machine
Hubs	2	2
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 or another source, for around $400 (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 sorts of other 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-11	SRV-1	SRV-12
IP Address	192.168.10.1/24 & 192.168.20.1/24	192.168.20.10/24 & 192.168.30.1	192.168.30.10/24 & 192.168.40.1
OS	W2K Server	W2K Server	W2K Server
Additional Configurations	SP2	SP2	SP2

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 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 Website, http://www.trainsignal.com/legalinfo.html

Computer 1

Computer 1 will be named SRV-11 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 Website.

SRV-11 will have 2 network cards, each with a static IP address. One will be configured with the IP address of 192.168.10.1 with a 255.255.255.0 subnet mask. This NIC should be renamed NIC 1 for easy identification. The second NIC will be configured with an IP address of 192.168.20.1 with a 255.255.255.0 subnet mask. This NIC should be renamed NIC 2, also for easy identification. The default gateway field and the DNS Server fields should be left blank. See figure 1, next page.

Computer 2

Computer 2 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 Website.

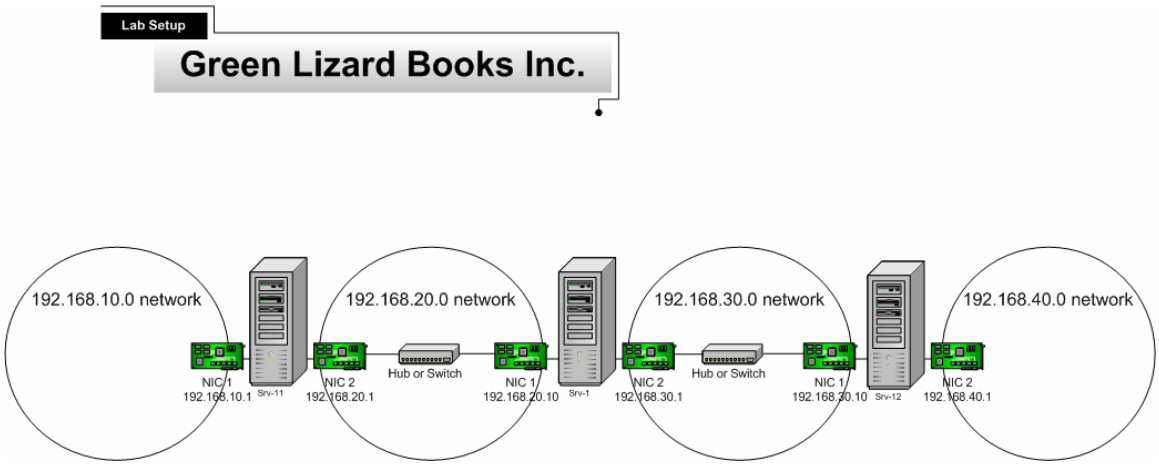
SRV-1 will have 2 network cards, each with a static IP address. One NIC should have the IP address of 192.168.20.10 with a 255.255.255.0 subnet mask. This NIC should be renamed NIC 1. The second NIC should have an IP address of 192.168.30.1 with a 255.255.255.0 subnet mask. This NIC will be renamed to NIC 2. The default gateway field and the DNS Server fields should be left blank. See figure 1, next page.

Computer 3

Computer 3 will be named SRV-12 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 Website.

SRV-12 will have 2 network cards, each with a static IP address. One NIC should have the IP address of 192.168.30.10 with a 255.255.255.0 subnet mask. This NIC should be renamed NIC 1. The second NIC should have an IP address of 192.168.40.1 with a 255.255.255.0 subnet mask. This NIC will be renamed to NIC 2. The default gateway field and the DNS Server fields should be left blank. See figure 1, next page.

Important - 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

Configuring a Windows 2000 Server as a Router for Green Lizard Books, Inc.

You will learn how to:

- Differentiate between hardware and software routing
- Assess when and where a router is needed on a network
- Configure a router using RRAS on a Windows 2000 Server
- Test access between routers on a network

Scenario

Green Lizard Books, Inc. is a book publishing company headquartered in Chicago, IL. This company has expanded tremendously over the past year. It currently has over 500 employees in its Chicago location. The client computers on Green Lizard's network run Window 2000 Professional (400 systems). They also have close to 20 servers, all running Windows 2000 Server and performing assorted duties.

You have been hired as Green Lizard's independent computer consultant for more than a year. In the weekly meeting that you have with the owner, Bill, he mentions to you that some of his employees have been complaining about slow network performance in recent months. They feel that the network performance is not as fast as it used to be, since more users are added to the network weekly. Bill also informs you that his company will expand further in the near future. He wants you to not only resolve the current problem, but also to prepare the company network to accommodate upcoming growth.

You tell Bill that his company used to be a small network with less than 50 computers and network performance was not a problem. Since his network has grown, however, performance has suffered as a result of the limitations of Ethernet networks. There is not an exact number of computers that an Ethernet network can support, but noticeable degradation of network performance can occur with as few as 10 computers on a low bandwidth network. Using modern devices (100 Mbps switches), a more realistic number of computers on an Ethernet segment is between 150 and 250. The ultimate performance test, however, is how the network performs when doing normal day to day tasks, such as accessing files, browsing the network or logging on.

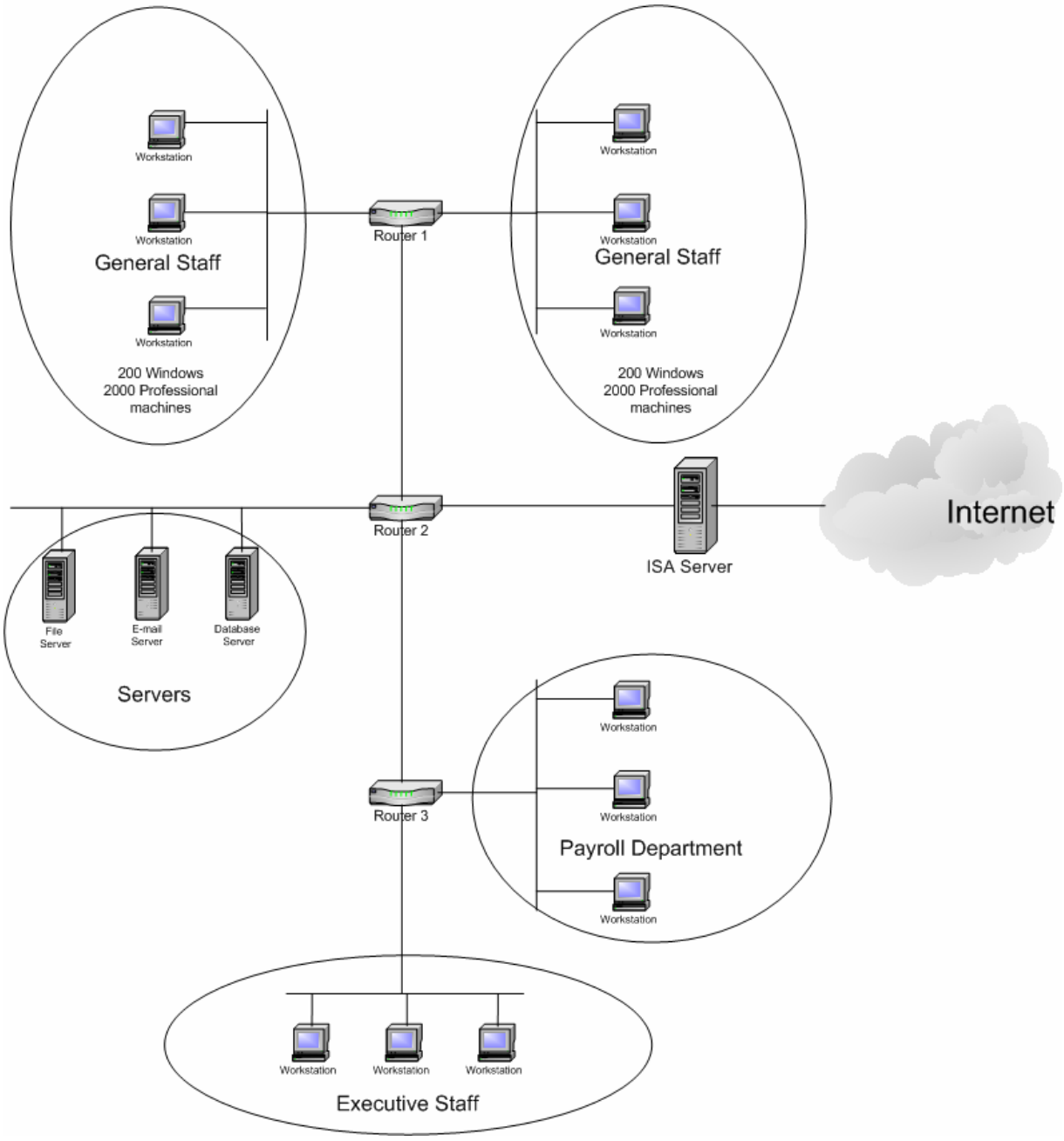
Green Lizard's network will require routers to help split up the network into several segments. This will cut down on traffic and will also help to better organize the network for further expansion. After examining Green Lizard's network in more detail, you notice that several Windows 2000 Servers are very lightly used. With a second network card, these servers will make perfect routers in addition to the current services they are running.

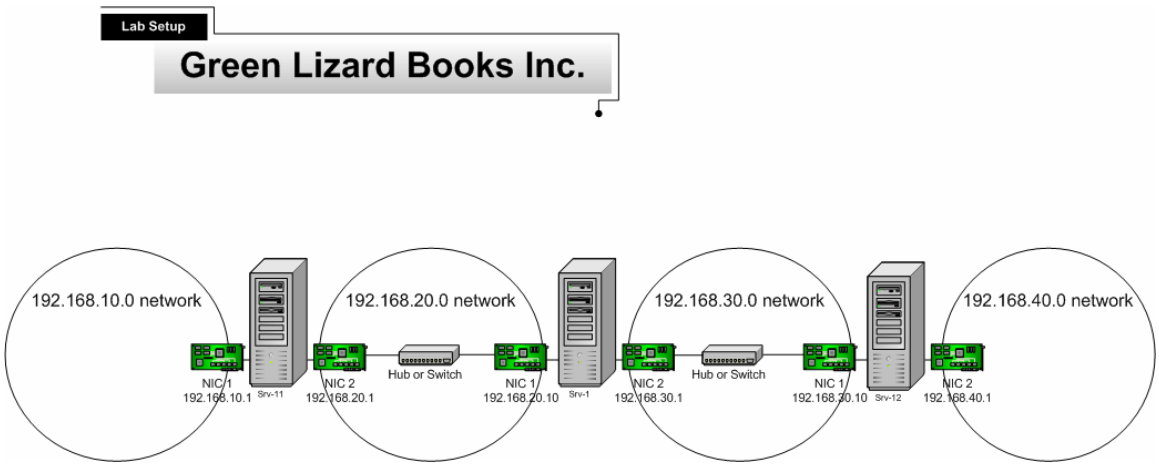
In this lab, you will install routers through the RRAS wizard on 3 Windows 2000 servers for Green Lizard Books Inc. You will then test connectivity between different network segments.

Company Environment

Green Lizard Books Inc.

Green Lizard's Network (Future Plan)





What is Routing?

This lab is not designed to go into the theory of routing in depth, but it is important to understand the general purpose of routing. A router's most basic function is to connect two networks together and forward data back and forth between them. In addition to this basic functionality, routers are also used to reduce network traffic, provide security, connect networks with different network protocols (i.e. TCP/IP, IPX/SPX) and a lot more. There are a lot of different companies that manufacture routers and each company typically has numerous types to choose from. In general though, there are 2 different kinds of router, hardware routers and software routers.

A hardware router is a physical piece of hardware that is designed and optimized for routing. It performs very few functions when compared to a computer, but it does its job - routing, well. Cisco is the first company that most people think of when you mention a hardware router. They are the industry leader but there are many more companies that produce routers as well.

A software router, on the other hand, is not dedicated to just routing but also runs other services and is capable of running applications. A software router has routing capability that installs on top of an operating system, such as Windows 2000. Typically, a software router routes traffic but it also performs other duties, such as acting as a DHCP Server or as a file server. The Routing and Remote Access Service in Windows 2000 Server is used to enable routing on a computer. There are advantages and disadvantages to both software routing and hardware routing. Some of the advantages are detailed below:

Hardware routing (Cisco)

Major Advantages:

- Faster and more efficient.
- Supports a wide range of network protocols.
- Provides many advanced routing features.

Software routing (Windows 2000 Server)

Major Advantages:

- Allows you to run multiple software applications/services on the same machine.
- Integrated with many features and benefits in Windows 2000.
- More user friendly than a hardware router. Less time is needed to learn vendor-specific commands that are present on a hardware router.
- Costs less than a hardware router.

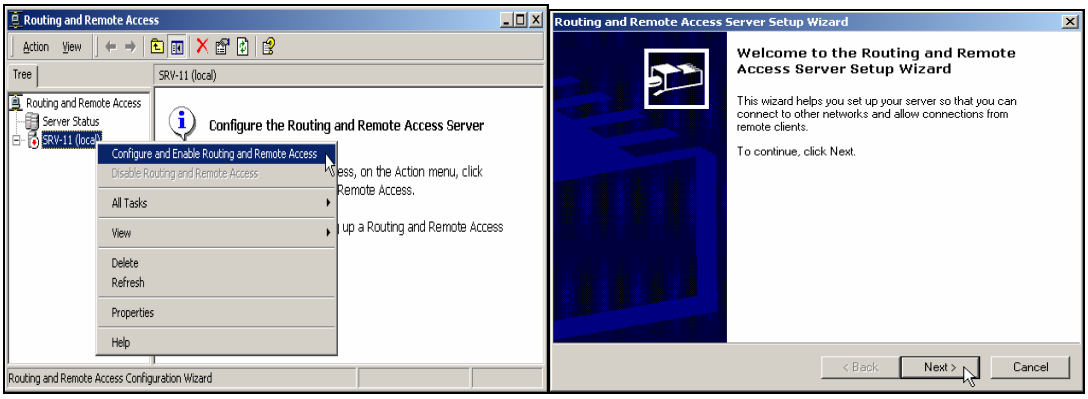
A Router is necessary for many reasons besides just routing between different network segments. Some of the reasons you may need to implement a router in your network are:

- To better organize and optimize your company's departments.
- To segment a network in order to reduce network traffic.
- To connect your network to the Internet
- To connect your Ethernet network to a different topology (i.e. Token Ring)
- To connect networks running different network protocols (i.e. IPX/SPX)
- To provide added security to a network segment

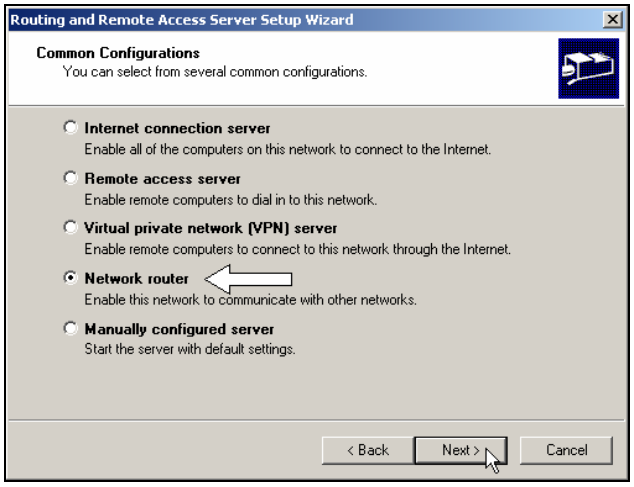
Setting up RRAS server as a Router

To connect Green Lizard's networks together you need to configure your Windows 2000 servers as routers. First, you will need to configure and enable the Routing and Remote Access Server (RRAS). By default, RRAS is installed as part of the Windows 2000 server installation, but it is not enabled.

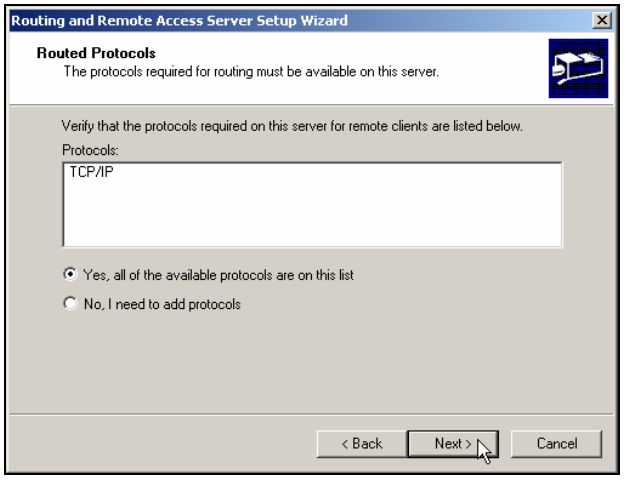
1. Log on to **SRV-11,** go to **Start→Programs→Administrative Tools** and click on **Routing and Remote Access**. Right click **SRV-11** and click **Configure and Enable Routing and Remote Access**. This will bring up the Routing and Remote Access Server Setup Wizard. Click **Next** to continue.



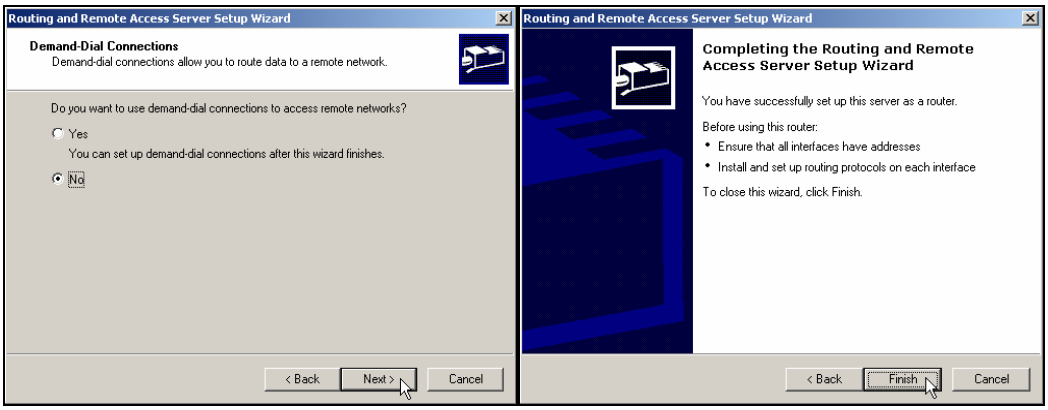
2. On the Common Configurations page, there are 5 common configurations for you to choose from. There are many services that you can choose from within RRAS, other than just creating a router. You can turn your computer into a NAT server or a VPN server, to name a few. These other services are covered in great detail in both Lab 7 and Lab 8. For now, select **Network router** and click **Next** to continue with the installation.



3. This will bring you to the Routed Protocols screen. For Green Lizard's network, TCP/IP is the only protocol that is being used and required for routing through this network router. This protocol should be installed by default. As well as TCP/IP this router can also route Internetwork Packet Exchange (IPX) and AppleTalk traffic. For now, just verify that TCP/IP is listed in the **Protocols** list and click **Next** to continue.



4. Once you are on the Demand-Dial Connections screen, you will be asked if you want to use demand-dial connections to access remote networks. Demand-dial connections will typically be used only when data is sent to a remote location across a dialed line, such as a 56K modem or ISDN. These connections will be automatically dropped after a specified amount of time or inactivity on the line. Since this network router will be for Green Lizard's LAN and you are using Ethernet network cards, demand-dial connections are not necessary. Select **NO** and click **Next** to continue. This will bring you to the last screen of the wizard - just click **Finish** to complete the network router configuration.

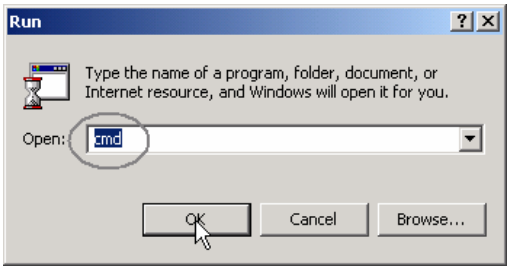


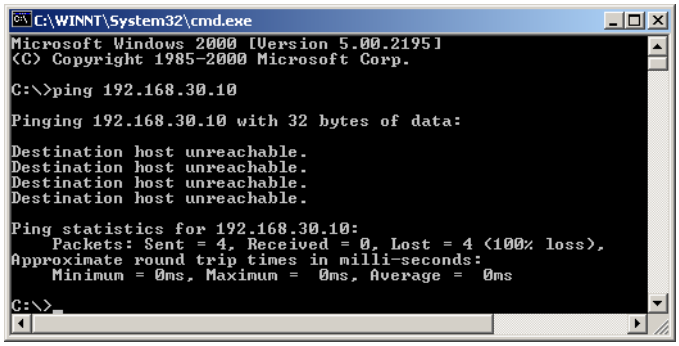
5. You should now repeat these same steps to setup the network router for **SRV-1** and **SRV-12.**

Testing network access to the different networks

In order to see if you have access to other network segments, you can conduct a test from SRV-11.

1. On SRV-11, go to **Start→Run,** type in **cmd** and click **OK** to open the command prompt. From the command prompt, type in **ping 192.168.30.10** and press **Enter**. The Ping utility is used to test the connectivity between any two machines on the network. You should not get a reply from the SRV-12 IP address (192.168.30.10). Although you have enabled routing on all 3 servers, further configuration is necessary before they are capable of forwarding data from one network to another. In Lab 2, we will cover these configurations in greater detail.



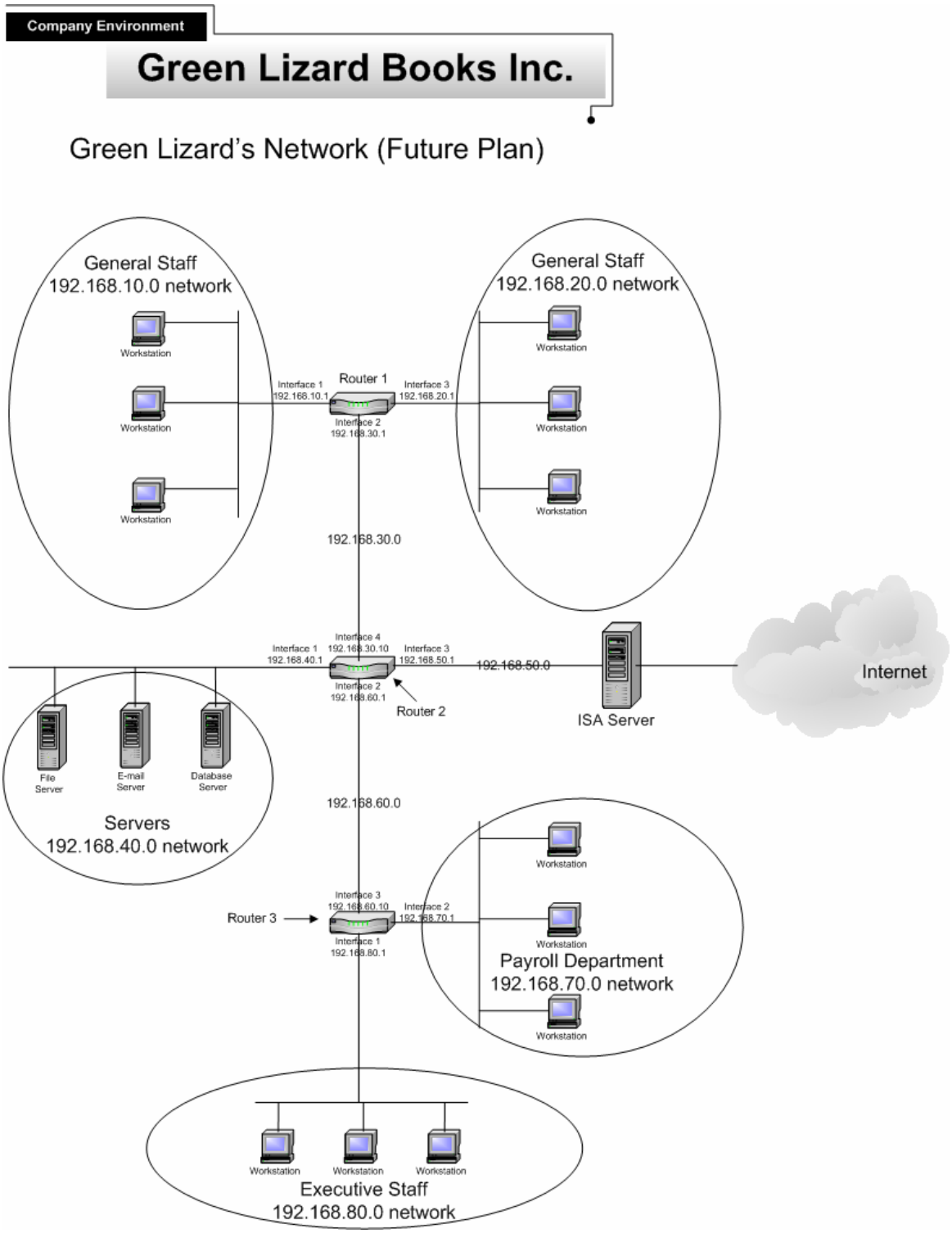


Lab 2

Configuring Green Lizard's Routers using Static Routes & Routing Protocols

You will learn how to:

- Add and configure static routes on a Windows 2000 Router
  - Install and configure the RIP routing protocol
- Examine RIP and assess data found within the routing table
  - Troubleshoot conflicts between RIP and static routes



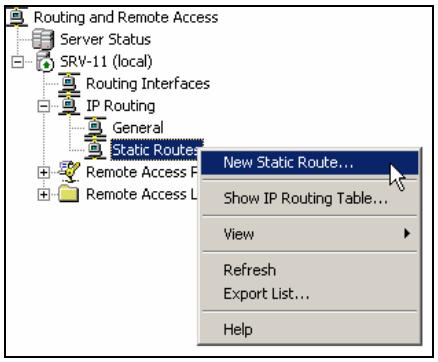
Static Routes

Even though routing is configured on each of the servers in Lab 1, you will not be able to access different networks until the routers are "educated" with a route to each of the different networks. A route is kind of like giving somebody driving directions (i.e. drive 5 miles past the gas station and take a left). Routes tell routers exactly where to send data when they receive it. If there is no route in a router's routing table, then the router gets "lost" and it will not be able to forward the data. All of a router's routes (directions to other networks) are stored in the router's routing table.

Referring to the Green Lizard's network (Future Plan) diagram, the entire network is divided up into eight different network segments, with five of these containing actual computers. Networks 192.168.30.0, 192.168.50.0 and 192.168.60.0 are the backbones of the network. In other words, they are the main arteries of the network. The majority of Green Lizard's network traffic will pass through these lines and therefore these lines may be running at 1000 Mbps for improved performance.

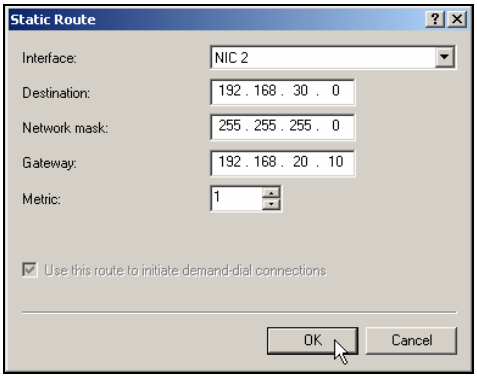
In order to allow network traffic to reach all of the network segments in Green Lizard's network, each router (Router 1, Router 2 and Router 3) must contain the necessary route information to forward network traffic. Each router must have routes in their routing tables that "teach" the router how to get to the destination network. Under Routing and Remote Access server in Windows 2000 server, static routes can be added by right clicking on **Static Routes** and selecting **New Static Route**.

Due to the limitations of the hardware for this lab (lack of computers and NICs), your lab setup is different than Green Lizard's network (Future plan). For now though, let's take a closer look at Green Lizard's network (Future plan) diagram and walk through the steps necessary to configure static routes and routing protocols.



To correctly configure Static Routes, you should be familiar with all of the different fields within the Static Route dialog box. The table below shows the configurable parameters and an explanation of what each is for.

Parameter	Explanation
Interface	The network interface that the data will exit from when it is leaving the router on its way to the destination address.
Destination	The Network ID of the network that you would like to reach. For example, 192.168.1.0 would be configured if you are trying to reach a subnet of computers that have IP address like 192.168.1.1/24.
Network mask	The corresponding destination network subnet mask.
Gateway	The IP address of the next router's interface on the way to the destination network. The "near-side" interface.
Metric	The cost of a route, used to set a preferential route. The metric is only applicable when multiple routes exist to the same destination. The route with the lower metric will be used.



According to the Green Lizard's network (Future Plan) diagram, static routes will have to be added to each router in order to have network traffic flow across the entire network. The tables shown below are the static routes that need to be added to the routing table on each router.

1. Router 1's static routes configuration

Interface	Destination	Network mask	Gateway	Metric
NIC 2	192.168.40.0	255.255.255.0	192.168.30.10	1
NIC 2	192.168.50.0	255.255.255.0	192.168.30.10	1
NIC 2	192.168.70.0	255.255.255.0	192.168.30.10	1
NIC 2	192.168.80.0	255.255.255.0	192.168.30.10	1

2. Router 2's static routes configuration

Interface	Destination	Network mask	Gateway	Metric
NIC 4	192.168.10.0	255.255.255.0	192.168.30.1	1
NIC 4	192.168.20.0	255.255.255.0	192.168.30.1	1
NIC 2	192.168.70.0	255.255.255.0	192.168.60.10	1
NIC 2	192.168.80.0	255.255.255.0	192.168.60.10	1

3. Router 3's static routes configuration

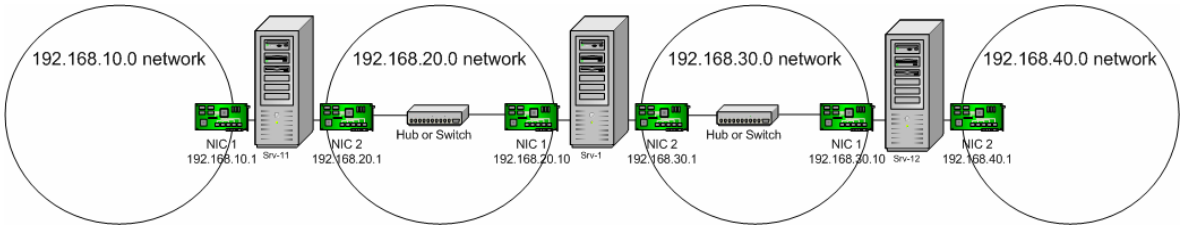
Interface	Destination	Network mask	Gateway	Metric
NIC 3	192.168.10.0	255.255.255.0	192.168.60.1	1
NIC 3	192.168.20.0	255.255.255.0	192.168.60.1	1
NIC 3	192.168.40.0	255.255.255.0	192.168.60.1	1
NIC 3	192.168.50.0	255.255.255.0	192.168.60.1	1

These static routes are entered into the Routing and Remote Access Server's routing table. They are used to determine the data packet's route. Notice, that static routes are not created for networks that are directly attached to the router. For example, on Router 1, static routes were not created for the 192.168.10.0, 192.168.20 or 192.168.30.0 networks. But, routes for these networks still appear in Router 1's routing table. This is because Router 1 has interfaces that are directly connected to these networks. If a router is directly connected to a network, then it is aware of this network and it will add the appropriate information to its routing table. Also, understand that each router is not responsible for the end-to-end delivery of any packet. They are only responsible for forwarding the packet to the next

router in line, much like an assembly line. If one of the routers goes down for any reason, "work" is halted and the packet will not be forwarded to its destination.

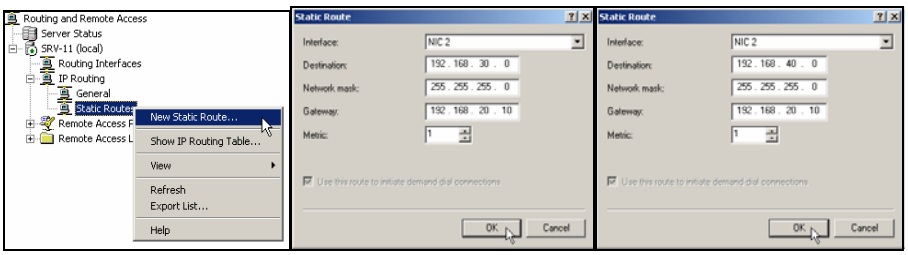
Adding Static Routes

To further understand how routers work, you will first need to learn how to add static routes to each of the routers in this lab and then test connectivity between the different network segments. Now, referring back to your Lab Setup, you will see that there are 4 different network segments and 3 routers/computers connecting them. Recall from Lab 1, that you configured all of your servers as routers. Now, it's time to add static routes on each router.

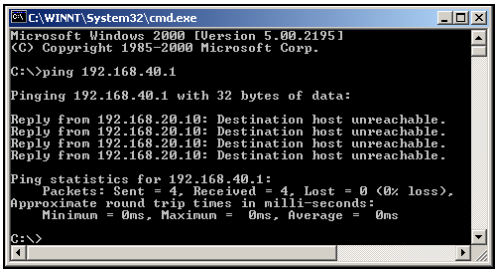


1. First, log on to **SRV-11**, and open **Routing and Remote Access** by going to **Start→Programs→Administrative Tools→Routing and Remote Access**, double click **IP routing**, right click on **Static Routes** and select **New Static Route**. This will bring you the Static Route dialog box. Refer to your Lab Setup and you will see that SRV-11 has 2 interfaces with one (NIC1) connected to the 192.168.10.0 network and the other (NIC2) connected to the 192.168.20.0 network. In order to have data packet forwarded to the 192.168.30.0 and 192.168.40.0 networks, you will have to add 2 static routes to the routing table on SRV-11. The 192.168.30.0 route will use the interface NIC2, to send data packets through the gateway 192.168.20.10. The 192.168.40.0 route will also use the interface NIC2 and send data packets through the gateway 192.168.20.10. SRV-11's static route configurations are shown in the table below.

Interface	Destination	Network mask	Gateway	Metric
NIC 2	192.168.30.0	255.255.255.0	192.168.20.10	1
NIC 2	192.168.40.0	255.255.255.0	192.168.20.10	1

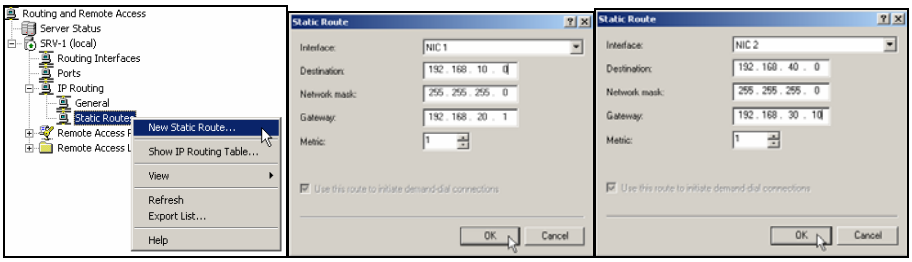


2. After adding these static routes on SRV-11, attempt to access the other network segments by pinging them. On SRV-11, go to **Start→Run**, type in **cmd** and click **OK** to open the command prompt. From the command prompt, type in **ping 192.168.40.1**, to attempt access to the 192.168.40.0 network. You should see a message similar to the one below, indicating that the destination host is unreachable. You are only getting a reply from the gateway, 192.168.20.10, letting you know that it can not help you out. Basically, the static routes that you have added to SRV-11 work, but they only get you part way to your destination. Before you can successfully ping this IP address, static routes will have to be added on each router. Remember, as was discussed earlier, each router is only responsible for passing packets from one router to the next.

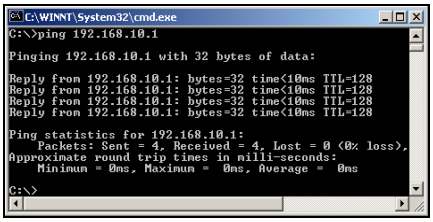


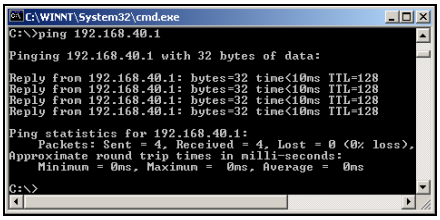
3. Next, log on to **SRV-1**, and open **Routing and Remote Access** by going to **Start→Programs→Administrative Tools→Routing and Remote Access**, double click **IP routing**, right click on **Static Routes** and select **New Static Route**. Again, this will bring you to the Static Route dialog box. On SRV-1 there are 2 interfaces with one interface (NIC1) connected to the 192.168.20.0 network and the other (NIC2) connected to the 192.168.30.0 network. When you refer to the lab diagram, you will see that, in order to have data packets forwarded to the 192.168.10.0 network and the 192.168.40.0 network, 2 static routes will be needed on SRV-1. One will use interface (NIC1) to send data packets through gateway 192.168.20.1 to the 192.168.10.0 network, and the other will use interface (NIC2) to send data packet through gateway 192.168.30.10 to the 192.168.40.0 network. SRV-1's static routes configurations are shown in the table below.

Interface	Destination	Network mask	Gateway	Metric
NIC 1	192.168.10.0	255.255.255.0	192.168.20.1	1
NIC 2	192.168.40.0	255.255.255.0	192.168.30.10	1



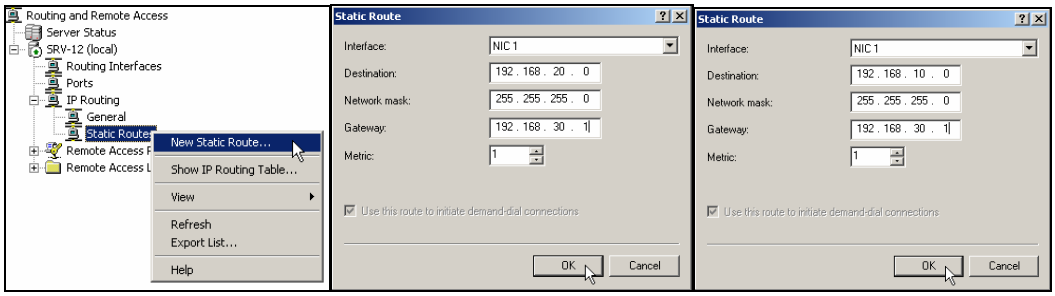
4. Our next step is to test networks access again. On SRV-1, open the **command prompt** and type in **ping 192.168.10.1**, which is an IP address on the 192.168.10.0 network, and press **Enter**. You should be getting a reply from this IP address. Now, test access to the 192.168.40.0 network by typing in **ping 192.168.40.1**. Again, you should be able to access this network from SRV-1. However, if you now try to access the 192.168.40.0 network from SRV-11, you should not have access. Although you have already configured a static route to forward data packets from SRV-1 to the 192.168.40.0 network, you still need to add static routes to the last router, SRV-12, in order to have traffic return from SRV-11.





5. The remaining router, SRV-12, also has 2 interfaces. One of SRV-12's interfaces (NIC1) is connected to the 192.168.30.0 network and the other is (NIC2) connected to the 192.168.40.0 network. In order for data packets to be forwarded to the 192.168.10.0 network and the 192.168.20.0 network, 2 static routes will be needed. One route will use interface (NIC1) to send data packets through gateway 192.168.30.1 to the 192.168.10.0 network, and the other will use interface (NIC1) to send data packets through gateway 192.168.30.1 to the 192.168.20.0 network. SRV-12's static route configurations are shown in the table below. **Add these static routes into SRV-12** to complete the configuration.

Interface	Destination	Network mask	Gateway	Metric
NIC 1	192.168.10.0	255.255.255.0	192.168.30.1	1
NIC 1	192.168.20.0	255.255.255.0	192.168.30.1	1



All of the necessary static routes have been configured on the routers. You should now be able to **ping from one side of the network to the other**.

Routing Protocols

When you have a small network, routing tables are very easy to update by manually adding static routes. But, in a larger network, it becomes very difficult to manage all of the different routes using static routes on each router. Another alternative is to use dynamic routing, which involves the use of routing protocols. After being enabled, routing protocols work on each router to keep it posted with the most up to date information on available route and network status. Routing protocols provide the means of automatically updating routing tables. They reduce administrative overhead tremendously. In Windows 2000, there are 2 types of routing protocols, **Routing Internet Protocol (RIP)**, which is a Distance Vector routing protocol and **Open Shortest Path First (OSPF)**, which is a Link State routing protocol. These two routing protocols each have their own advantages:

1. Routing Internet Protocol (RIP) Advantages:

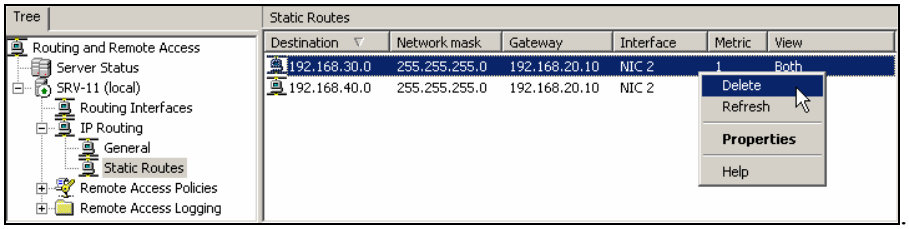
   - Easy to configure and manage.
   - Low administrative overhead.
   - Designed to use in small to medium network, networks with up to 50 servers.

2. Open Shortest Path First (OSPF) Advantages:

   - Designed for large-scale internetworks and able to scale to very large networks
   - Operates more efficiently with smaller routing tables in large networks
   - Lower convergence time

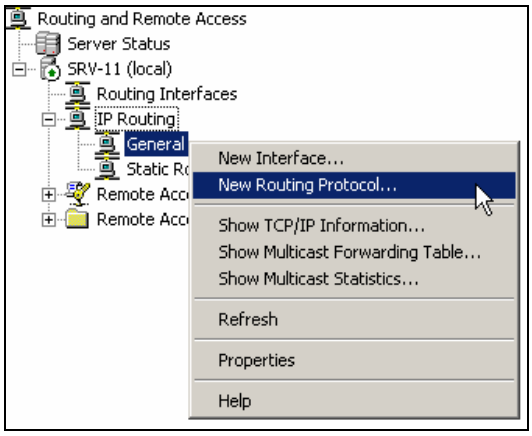
In order to show you how RIP works, you will have to delete all of the static routes you added on your routers.

1. To do this, open **Routing and Remote Access** by going to **Start→Programs→Administrative Tools→Routing and Remote Access** on each of your routers, double click **IP routing** and click on **Static Routes**. Just right click on the **static route** and select **Delete** to delete it. Repeat the same steps on other routers to delete all static routes.

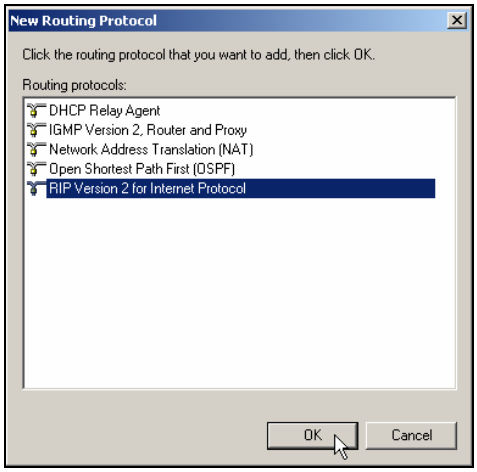


Adding the RIP Protocol

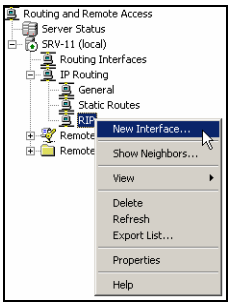
1. To add RIP as the routing protocol, first log on to **SRV-11** and **open Routing and Remote Access** by going to **Start→Programs→Administrative Tools→Routing and Remote Access**, double click **IP routing**, right click on **General** and select **New Routing Protocol**.

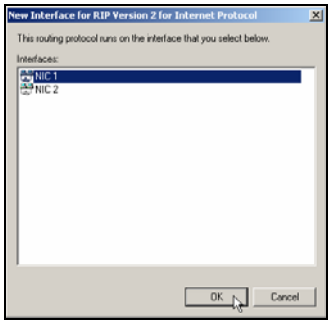


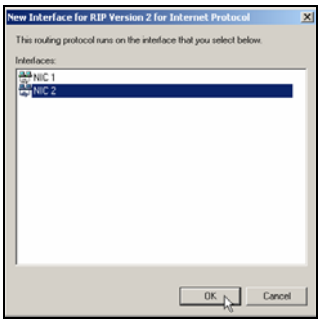
2. This will open up the New Routing Protocol dialog box. Just highlight **RIP Version 2 for Internet Protocol** as the routing protocol and click **OK** to complete adding the new routing protocol.



3. You have now added RIP as the routing protocol on SRV-11. You will also need to add the interfaces which will support RIP. Again, within the RRAS tool, right click on **RIP** under IP Routing and select **New Interface**. This will bring you to the **New Interface for RIP Version 2 for Internet Protocol** dialog box. Select **NIC 1** and click **OK** to close the dialog box, and click **OK** on the RIP properties dialog box to complete adding the interface. Repeat the same steps to add the remaining interface, NIC2 as the second interface to support RIP.

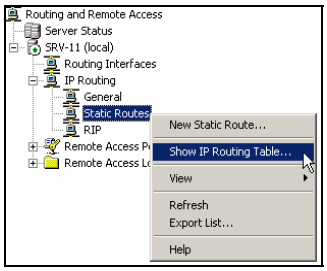


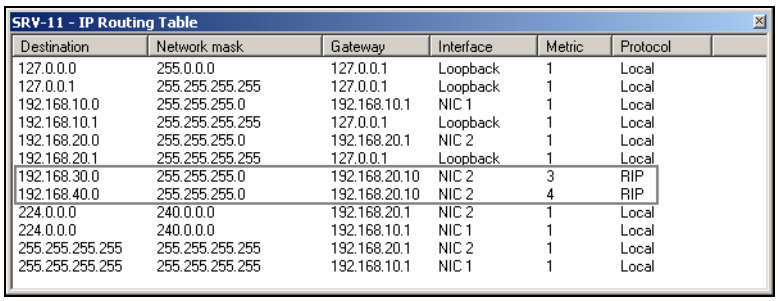




4. Not only do you need to have RIP added on SRV-11, you also need it added on SRV-1 and SRV-12. Repeat **the same steps above** to add RIP as the routing protocol on SRV-1 and SRV-12. Also be sure you remember to add **both NIC1 and NIC2 interfaces** to support RIP on SRV-1 and SRV-12.

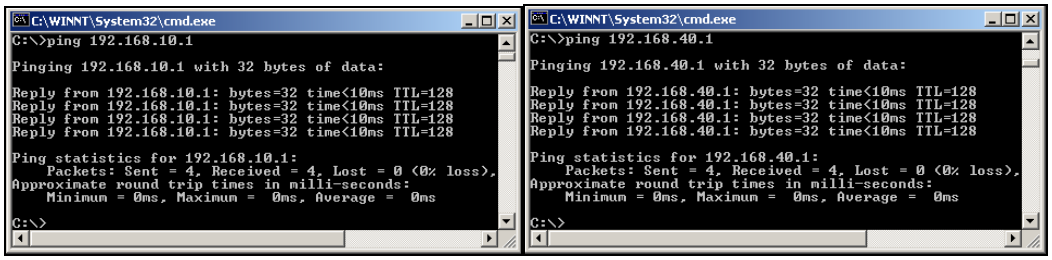
5. Now, let's take a look at the routing table from SRV-11. In Routing and Remote Access, right click on **Static Routes** under IP Routing and select **Show IP Routing Table**. This will bring you to the SRV-11 – IP Routing Table. Notice that there are routes added automatically to the routing table with RIP as the protocol. As you see, RIP has dynamically added routes to your routing table in SRV-11. Routes are also dynamically added in SRV-1 and SRV-12.





Destination	Network mask	Gateway	Interface	Metric	Protocol
127.0.0.0	255.0.0.0	127.0.0.1	Loopback	1	Local
127.0.0.1	255.255.255.255	127.0.0.1	Loopback	1	Local
192.168.10.0	255.255.255.0	192.168.10.1	NIC 1	1	Local
192.168.10.1	255.255.255.255	127.0.0.1	Loopback	1	Local
192.168.20.0	255.255.255.0	192.168.20.1	NIC 2	1	Local
192.168.20.1	255.255.255.255	127.0.0.1	Loopback	1	Local
192.168.30.0	255.255.255.0	192.168.20.10	NIC 2	3	RIP
192.168.40.0	255.255.255.0	192.168.20.10	NIC 2	4	RIP
224.0.0.0	240.0.0.0	192.168.20.1	NIC 2	1	Local
224.0.0.0	240.0.0.0	192.168.10.1	NIC 1	1	Local
255.255.255.255	255.255.255.255	192.168.20.1	NIC 2	1	Local
255.255.255.255	255.255.255.255	192.168.10.1	NIC 1	1	Local

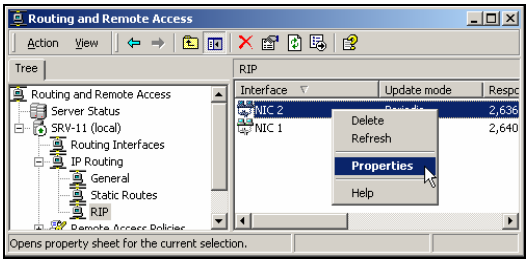
6. All of your routing tables have been dynamically updated with new routes. You now need to use the ping utility again to test connectivity. You should have access between all 4 networks.

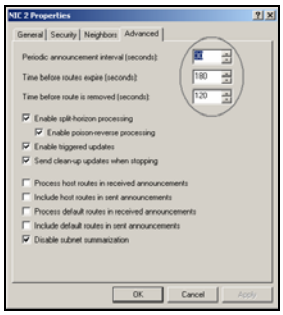


Demonstrate how RIP updates the routing table dynamically

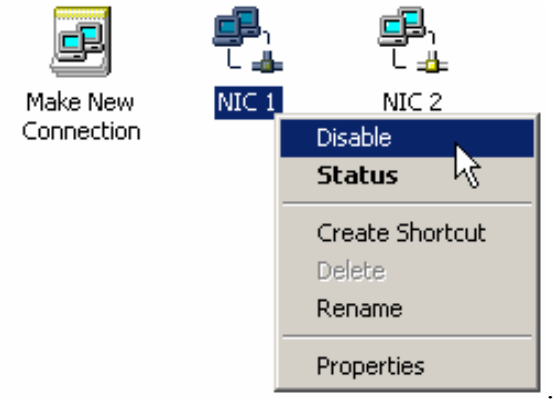
Before showing you more on how RIP actually updates the routing tables, let's take a look at the properties on one of the RIP interfaces first.

1. In Routing and Remote Access on SRV-11, double click **IP routing** and click on **RIP**. Just right click on **interface (NIC2)** and select **Properties**. This will bring you the NIC 2 Properties dialog box. Just click on the **Advanced** tab for information on how RIP updates routes in the routing table. As you can see in this configuration, RIP sends out an announcement to update routes every 30 seconds, which is the default. If a route is not updated with another RIP announcement within 180 seconds, the route will be expired and marked as an invalid route. After another 120 seconds, the expired route will be removed from the routing table.





2. Now, let's see exactly how it works. You will first disable an interface on one of the routers and see how RIP updates each routing table. Log on to **SRV-12**, go to **Start→Settings→Network and Dial-up Connections**, just right click **on NIC1 interface** and select **Disable**.



3. After 180 seconds, the route to the 192.168.40.0 network will expire and become an invalid route on both SRV-11 and SRV-1. After another 120 seconds, this route will be completely removed from the routing table on SRV-11 and SRV-1. As you see from SRV-1's routing table below, the route to the 192.168.40.0 network has been removed.

SRV-1 - IP Routing Table

Destination	Network mask	Gateway	Interface	Metric	Protocol
192.168.10.0	255.255.255.0	192.168.20.1	NIC 1	3	RIP
255.255.255.255	255.255.255.255	192.168.30.1	NIC 2	1	Local
255.255.255.255	255.255.255.255	192.168.20.10	NIC 1	1	Local
224.0.0.0	240.0.0.0	192.168.30.1	NIC 2	1	Local
224.0.0.0	240.0.0.0	192.168.20.10	NIC 1	1	Local
192.168.30.1	255.255.255.255	127.0.0.1	Loopback	1	Local
192.168.30.0	255.255.255.0	192.168.30.1	NIC 2	1	Local
192.168.20.10	255.255.255.255	127.0.0.1	Loopback	1	Local
192.168.20.0	255.255.255.0	192.168.20.10	NIC 1	1	Local
127.0.0.1	255.255.255.255	127.0.0.1	Loopback	1	Local
127.0.0.0	255.0.0.0	127.0.0.1	Loopback	1	Local

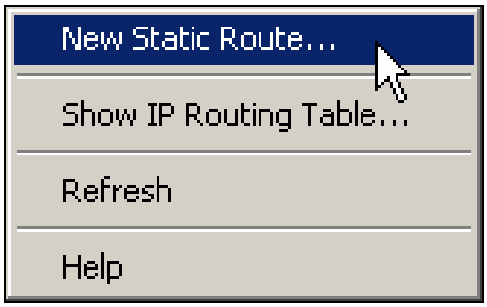
Routing conflicts between RIP and Statically configured routes

In this section of the lab, you will examine what happens when conflicting routes in the routing table between RIP and a statically configured route exist. In other words, what happens if you have RIP turned on and it learns a route to Network 192.168.1.40, but you also create a static route to 192.168.1.40 that directs data in a different direction? To test this out, first, make sure that you **re-enable the interface on SRV-12** and wait for all of the routers to fully converge (learn routes to every network).

1. Once your routing tables contain all of the routes that they are supposed to, log on to **SRV-1** and go to **Start→Programs→Administrative Tools→Routing and Remote Access**. Before you add a new static route, look at the routing table by simply right clicking on **Static Routes** under IP Routing and selecting **Show IP Routing Table.** You should see 2 routes, both discovered by RIP (last column). One route uses interface (NIC1) to send data packets through the gateway 192.168.20.1 to the 192.168.10.0 network, and the other uses interface (NIC2) to send data packets through gateway 192.168.30.10 to the 192.168.40.0 network.

Destination	Network mask	Gateway	Interface	Metric	Protocol
192.168.10.0	255.255.255.0	192.168.20.1	NIC 1	3	RIP
192.168.40.0	255.255.255.0	192.168.30.10	NIC 2	3	RIP
127.0.0.0	255.0.0.0	127.0.0.1	Loopback	1	Local
127.0.0.1	255.255.255.255	127.0.0.1	Loopback	1	Local

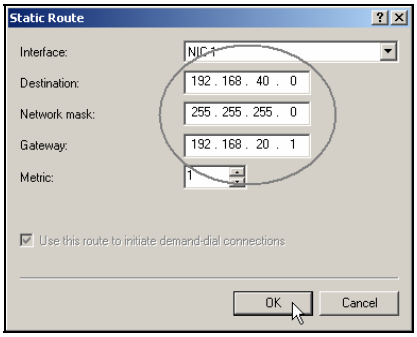
2. Close the routing table, right click on **Static Routes** again and select **New Static Route** to add a new static route.



3. Within the Static Route dialog box, type in the **configuration** shown in the table below.

Interface	Destination	Network mask	Gateway	Metric
NIC 1	192.168.40.0	255.255.255.0	192.168.20.1	1

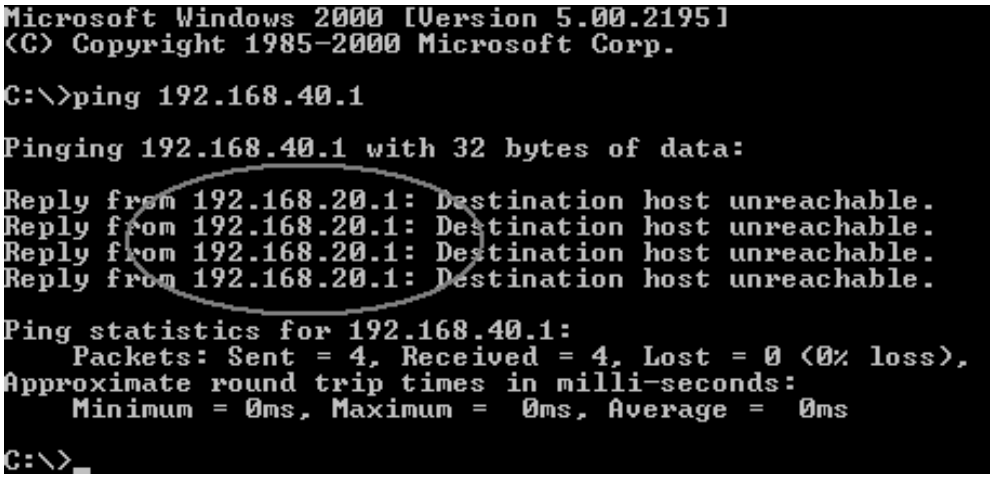
4. This static route tells the interface (NIC1) to send data packet through gateway 192.168.20.1 to the 192.168.40.0 network. Referring to the lab diagram, this route will be an invalid route. Just click **OK** to complete adding this static route.



5. Now, right click on **Static Routes** and select **Show IP Routing Table** to view the routing table again. In the routing table, there are 2 routes going to the same destination network, 192.168.40.0, but they are using different gateways. One is going through gateway 192.168.20.1 with static as the protocol and the other is going through gateway 192.168.30.10 with RIP as the protocol.

Destination	Network mask	Gateway	Interface	Metric	Protocol
192.168.40.0	255.255.255.0	192.168.20.1	NIC 1	1	Static (non demand-dial)
192.168.40.0	255.255.255.0	192.168.30.10	NIC 2	3	RIP
192.168.10.0	255.255.255.0	192.168.20.1	NIC 1	3	RIP
255.255.255.255	255.255.255.255	192.168.30.1	NIC 2	1	Local
255.255.255.255	255.255.255.255	192.168.20.10	NIC 1	1	Local

6. To see which route is being used to the 192.168.40.0 network, go to the command prompt, type in **ping 192.168.40.1**, an IP address on the 192.168.40.0 network, and press **Enter**. As you see, you are not getting any reply from the destination IP address. Instead, you are getting a reply from the gateway, 192.168.20.1, indicating that the destination host is unreachable. As a result, when there are conflicting routes in the routing table, statically configured routes will be used over RIP.



Lab 3

Configuring Packet Filters within Windows 2000 to secure Green Lizard's network

You will learn how to:

- Configure packet filters on a network interface in Windows 2000 professional or Server
- Set up a web server and a FTP server in IIS
- Choose the appropriate transport protocol and port number
- Configure packet filters in Routing and Remote Access Server

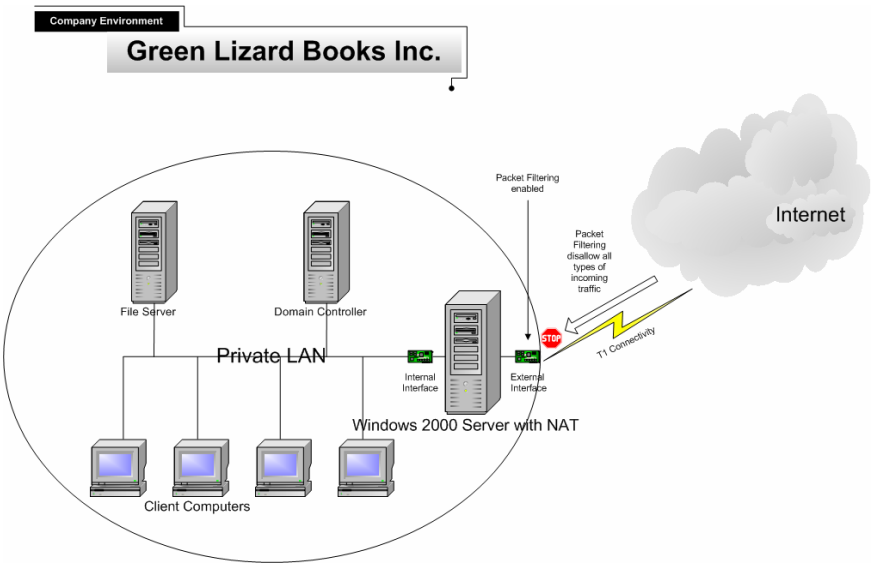
Packet Filtering

In Windows 2000, you have the ability to specify what type of network traffic is to be allowed into and out of the IP router. This feature is called packet filtering. Packet filtering can be applied on a network interface directly or through Routing and Remote Access in Windows 2000 server. When you enable packet filtering on a network interface directly, you can only filter incoming network traffic. This type of packet filtering is available in both Windows 2000 Professional and Server. In order to filter both incoming and outgoing traffic, you will have to configure packet filtering within Routing and Remote Access, which is only available on a Windows 2000 Server.

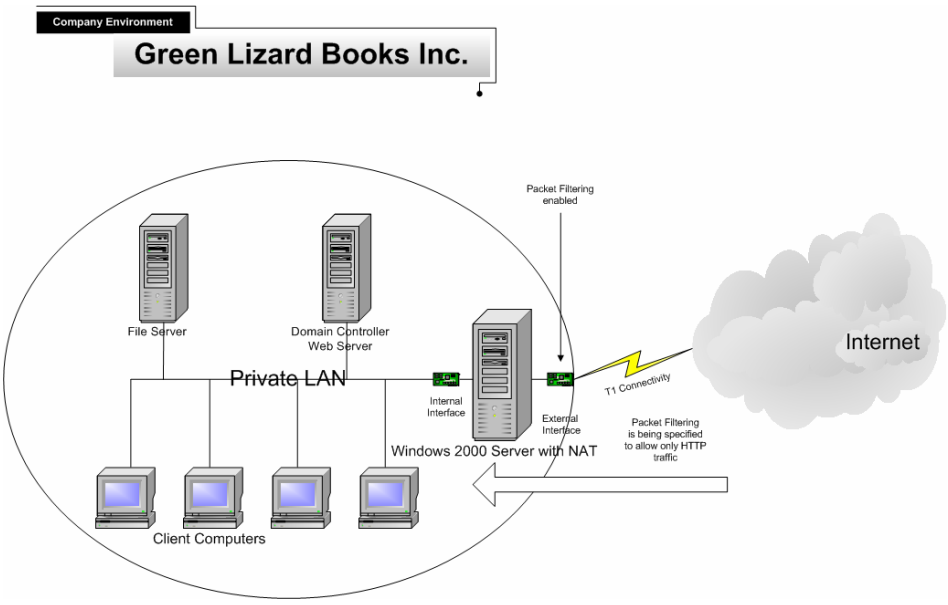
Packet filters allow or deny network traffic based upon protocol and port number. The protocols used within packet filters are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). Both of these protocols are part of the TCP/IP suite of protocols and exist at the transport layer (layer 4) of the OSI model. TCP features guaranteed delivery. A connection is established with the destination computer and acknowledgements are sent confirming the delivery of the packet. HTTP and FTP are examples of protocols that use TCP to do their job. Application layer protocols (such as TFTP & DNS) that use UDP do not establish a connection and delivery of the data packets is not confirmed. This results in more efficient but less reliable delivery of data.

In this lab, you will first learn how to setup a web server, a simple test web site and a FTP site. You will then test access to the web site and the FTP site through Internet browser from different network segments. Lastly, you will configure packet filter in Routing and Remote Access to allow only HTTP traffic to the network segment that contains this web site and block all other traffic.

In the diagram below, packet filtering is enabled on the external interface of the Windows 2000 server. It is configured to disallow all type of incoming network traffic to the Local Area Network.



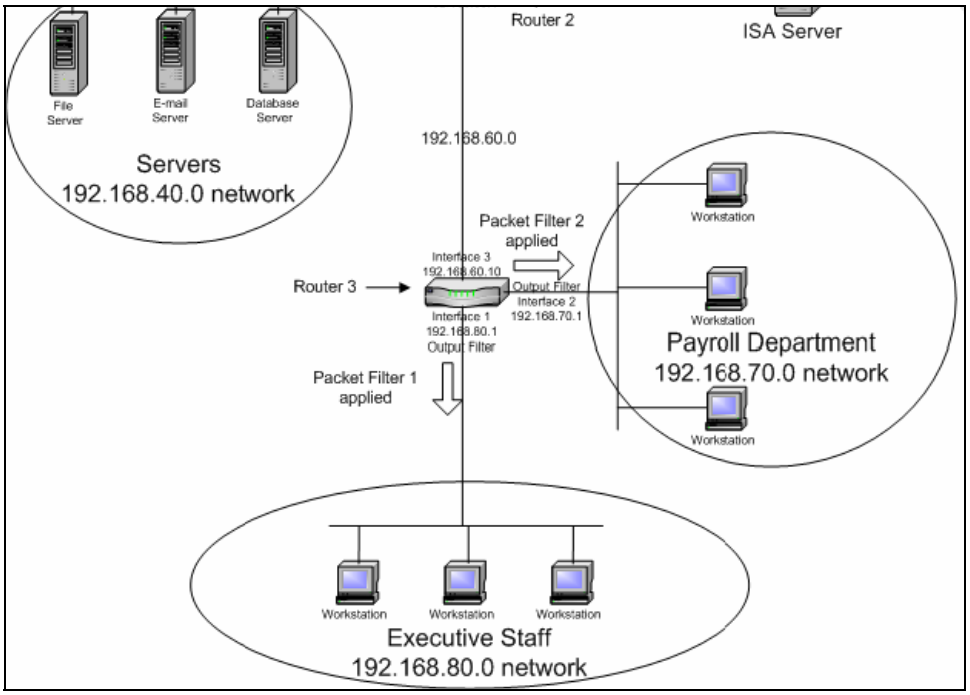
In the diagram below, packet filtering is also enabled on the external interface of the Windows 2000 server. It is now configured to allow HTTP traffic to access the internal web server. All other types of traffic are disallowed into the LAN.



Packet Filters can also be used on the internal network to secure different network segments. Referring to Green Lizard's network (Future Plan) diagram below, network traffic is allowed only from certain network segments to the Executive Staff segment and the Payroll Department segment. In order to secure these segments, packet filters need to be applied to outbound traffic on both interface 1 and interface 2 within Router 3.

Packet Filter 1 – Green Lizard wants to add additional security to their network by filtering all data that enters into the Executive network segment. The only data that will be allowed is data that sources from the Servers network segment. To accomplish this, a packet filter will be needed on router 3 to filter traffic destined for the Executive Staff network, 192.168.80.0. The best location for this filter will be on interface 1 of Router 3. It needs to be configured to block all network traffic exiting interface 1 except traffic with a destination Network ID of 192.168.80.0.

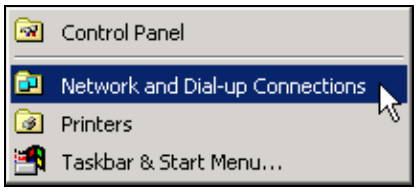
Packet Filter 2 – Green Lizard also wants to secure the Payroll Department network segment. The only traffic that should be allowed to enter the Payroll Department network is traffic sourcing from the Servers network or the Executive Staff network. Packet filters will be needed to filter all traffic exiting Router 3's interface 2. The packet filters should only allow traffic that sources from the 192.168.40.0 and 192.168.80.0 networks.

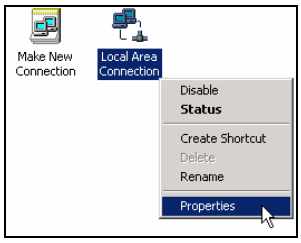


Configuring Packet Filters directly on the Interface

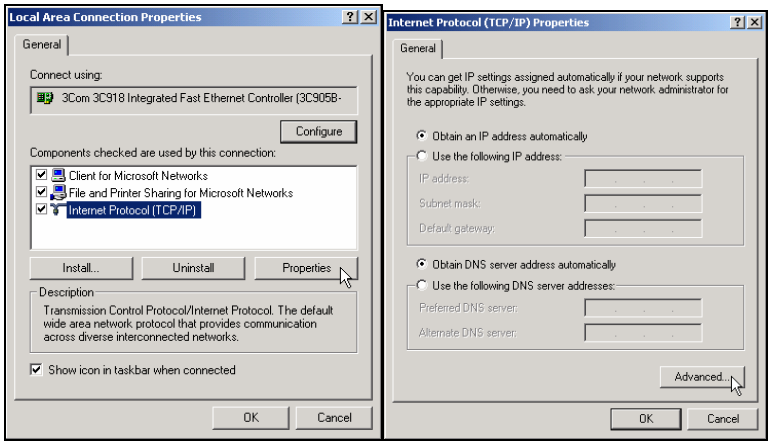
You can enable packet filtering on a network interface in either Windows 2000 Professional or Server. As mentioned before, configuring packet filters on a network interface only allows filtering of incoming network traffic (incoming, from the interface's perspective). In order to filter both incoming and outgoing network traffic, you will have to configure packet filters within Routing and Remote Access, which is only found within Windows 2000 Server. You will start with configuring a packet filter on the NIC directly.

1. To apply a packet filter on a network interface card in either Windows 2000 Professional or Server, first go to **Start→Settings→Network and Dial-up Connections.** Right click on the network interface that you want to apply the filter to and select **Properties**.

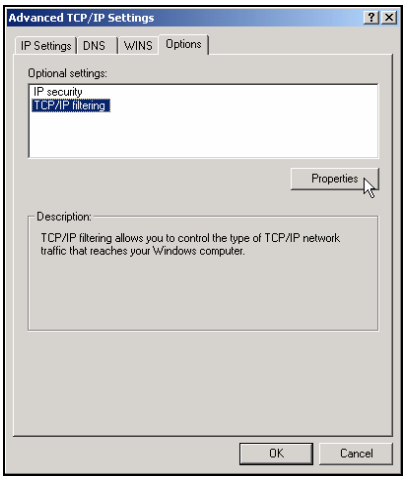




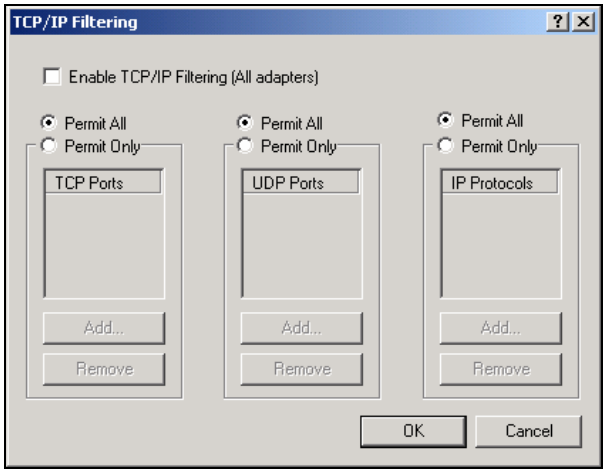
2. This will bring up the Properties dialog box. Highlight **Internet Protocol (TCP/IP)** and click on the **Properties** button. In the Internet Protocol (TCP/IP) Properties dialog box, click on the **Advanced** button.



3. Within the Advanced TCP/IP Settings dialog box, there are 4 tabs available. Select the **Options** tab, then select **TCP/IP filtering** and click **Properties** to continue.



4. This will bring up the **TCP/IP Filtering** dialog box. This is where you can allow or deny network traffic by specifying transport protocols (TCP, UDP), IP protocols and port numbers. Remember, these settings only apply to network traffic that enters **IN** this specific network interface.

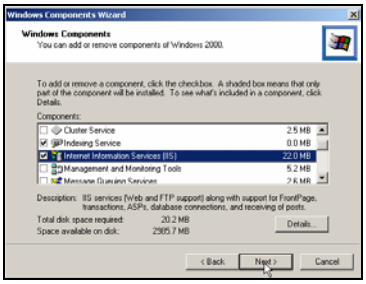


Setting up a web server and a FTP server

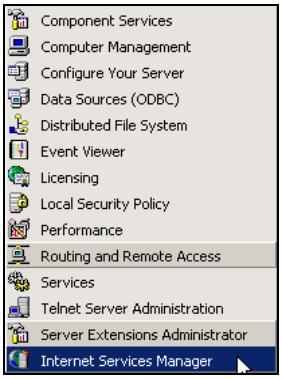
Installing IIS

In order to set up a web server and a FTP server, you will first have to install Internet Information Services (IIS). IIS should already be installed by default along with your Windows 2000 server installation. If for any reason it is not installed, just walk through the following procedures.

1. On SRV-12 go to **Start→Settings→Control Panel**. Double click on the **Add/Remove Programs** icon and click on **Add/Remove Windows Components** on the left column. This will bring up the Windows Components Wizard. Place a check mark in the box next to **Internet Information Services (IIS)** and click **Next** to begin the installation. Make sure that you have your Windows 2000 server disk handy because you will be asked for it during the installation. The installation should take about 5-10 minutes. You will eventually get a screen letting you know that the installation is done. Click on **Finish** to complete the installation.

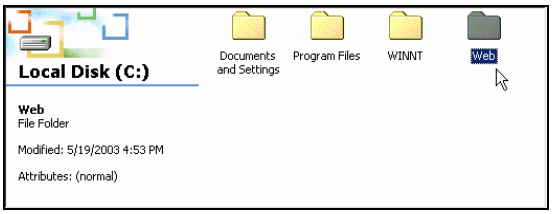


2. To confirm that Internet Information Services (IIS) is successfully installed on SRV-12, go to **Start→Programs→Administrative tools** and open **Internet Services Manager**. If your server (SRV-12) shows up within the Internet Services Manager console you should be all set.

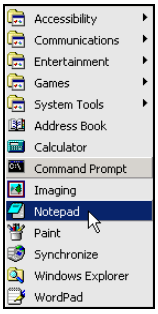


Creating a test web page for Green Lizard Books Inc

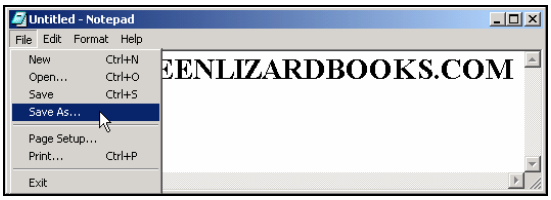
1. Open **Windows Explorer** and, within the C: drive, create a new folder named **Web**. This can be done by right clicking on an **empty space** within the C: drive and selecting **New Folder** from the shortcut menu. Close **Windows Explorer** when you are finished.



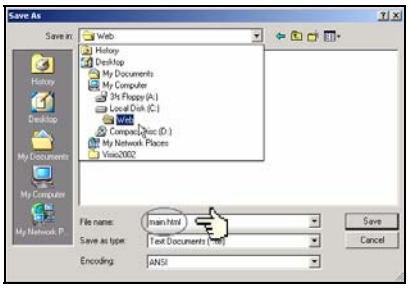
2. Next, use Notepad to create a simple HTML file that will be used for Green Lizard's web site. Go to **Start→Programs→Accessories→Notepad**.



3. In Notepad, type in **WWW.GREENLIZARDBOOKS.COM** and then select **File→Save As** from the menu.



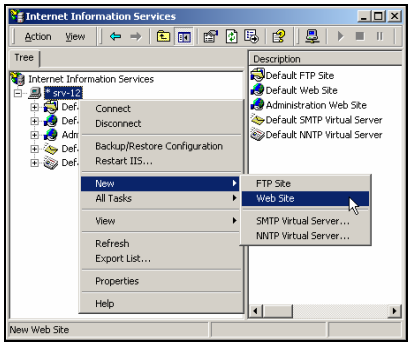
4. On the Save As screen, open the **Save in** drop down menu and select the **Web** folder that you created earlier as the location to save this file. Once you have selected the folder, enter the filename **main.html**. Next, click on the **Save** button and close **Notepad**.



5. Next, open the **Web** folder using **Windows Explorer** to make sure that the file was saved as a HTML file (see the picture below). Close **Windows Explorer**.

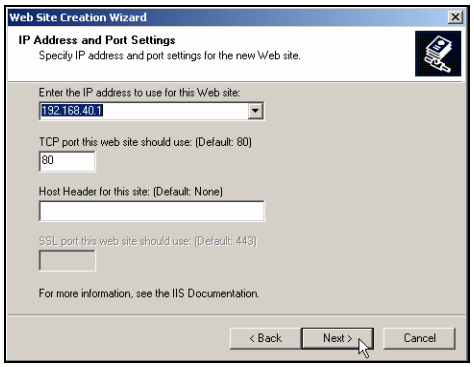
Hosting the Website on the Web server

1. Now, open **Internet Service Manager** and right click on **SRV-12**. Select **New→Web Site** from the shortcut menu to start the new web site wizard to create a new website.

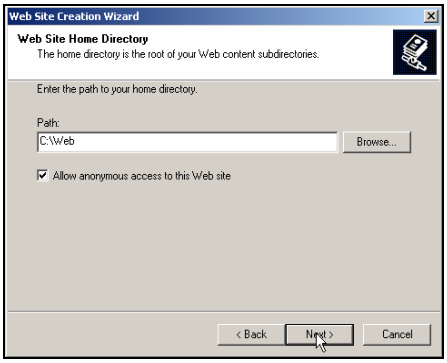


2. Within the wizard, click **Next** on the welcome screen. On the next screen type in: **GreenLizardBooks** as the description for the web site and click **Next** to continue.

3. The next screen will ask you to specify the IP address to use for the web site. The drop down menu gives you 2 IP addresses (192.168.40.1 and 192.168.30.10) to select from. Select **192.168.40.1** as the IP address to use for this web site. Leave the default port number at **80**, and the host header field **blank**. Click **Next**.

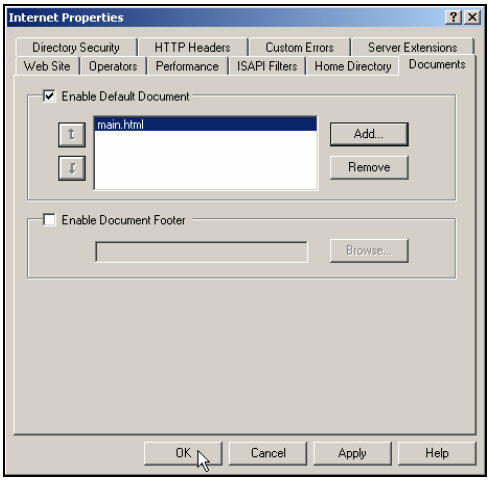


4. This will bring you to the Web Site Home Directory screen. Specify the path to the home directory for the web content, as the Web folder that you created earlier. Leave the **Allow anonymous access to this Web site** box checked and click **Next**.

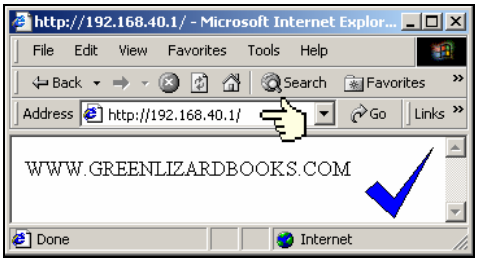


5. On the next screen, leave the **Read permission** and **Run scripts** permission checked and click **Next**. Also click **Finish** on the final screen of the wizard. You should now see the web site for GreenLizardBooks appear in the left pane of Internet Services Manager. Also be sure that the Default Web Site is stopped. If the Default Web Site is not stopped, you can just right click on the **Default Web Site** and select **Stop** to stop the site.

6. Next, open the **Properties** page for the GreenLizardBooks site. Right click on **GreenLizardBooks**, 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**. This is the name of the web page file that you created earlier. By specifying this page, you are telling the web server which page to open first - your home page. You should remove **default.htm** and **default.asp**, the other file names in this box, because they do not pertain to your site. Click **OK** to close the properties for the Green Lizard Books web site. If the Green Lizard Books web site shows as being stopped in the left pane, you can just start the site by right clicking on **GreenLizardBooks** and selecting **Start**.

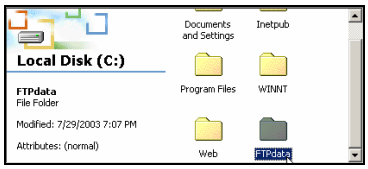


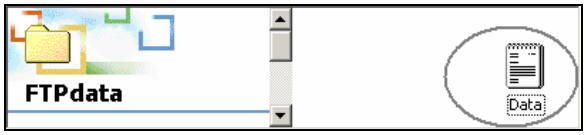
7. To test this web site, open **Internet Explorer** on any one of your servers (SRV-11, SRV-1, or SRV-12)**,** enter **192.168.40.1** and hit **Enter**. You should be able to view this test web site.



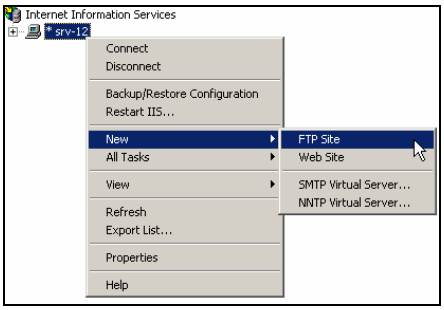
Creating a test FTP site for Green Lizard Books

1. Open **Windows Explorer** again. Within the C: drive, create a new folder named **FTP data**. This can be done by right clicking on an empty space within the C: drive, and selecting **New Folder** from the shortcut menu. Close **Windows Explorer** when you are finished. Next, create a simple data file named **Data** within the FTPdata folder (this data file can be any type of file, as you are only using it for testing purposes). This folder will be used for the Green Lizard Books FTP site.

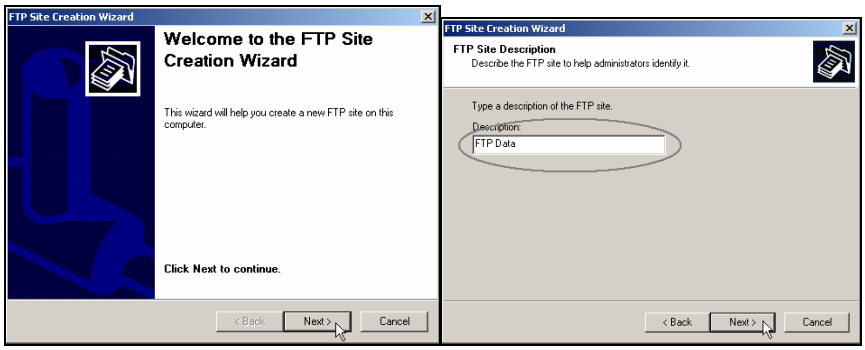




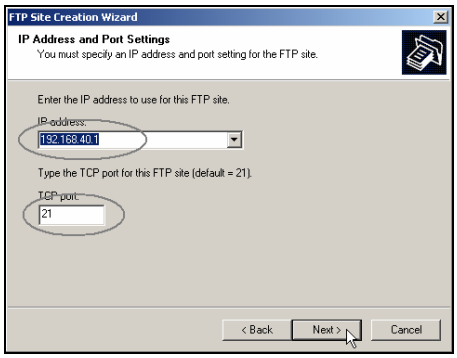
2. Now, open **Internet Service Manager** and right click on **SRV-12**. Select **New→FTP Site** from the shortcut menu to start the new FTP site wizard to create a new FTP site.



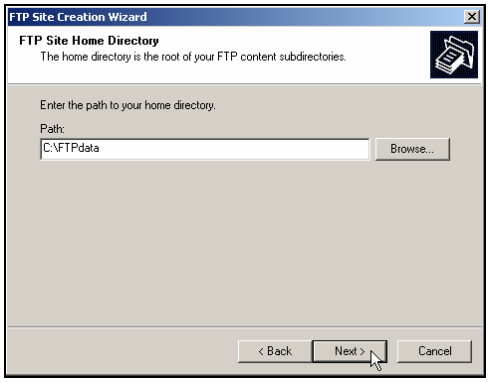
3. Within the wizard, click **Next** on the welcome screen. On the next screen, type in **FTP Data** as the description for the FTP site and click **Next** to continue.



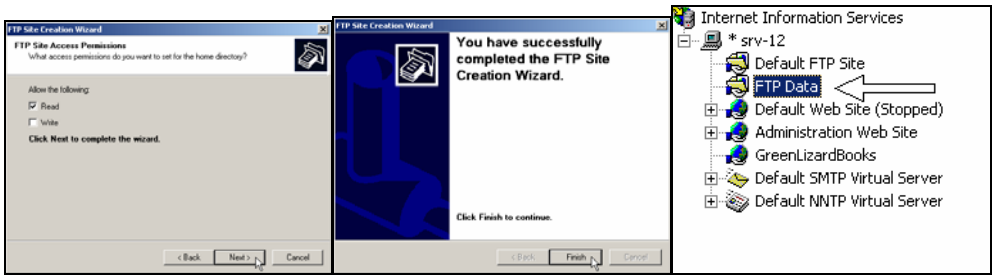
4. The next screen will ask you to specify the IP address to use for this FTP site. The drop down menu gives you 2 IP addresses (192.168.40.1 and 192.168.30.10) to select from. Select **192.168.40.1** as the IP address to use for this FTP site. Leave the default TCP port number at **21** and click **Next** to continue.



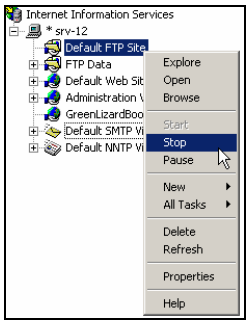
5. This will bring you to the FTP Site Home Directory screen, just specify the path to the home directory for the FTP content as the FTPdata folder that you created earlier and click **Next** to continue.



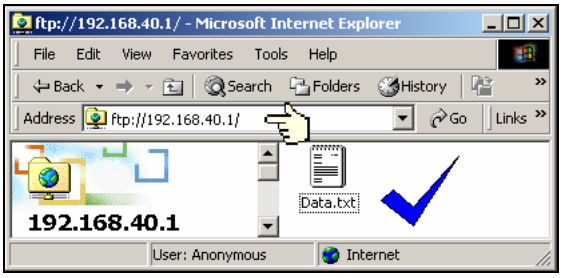
6. At the FTP Site Access Permissions screen, just leave the **Read permission** checked and click **Next** to continue. Also click **Finish** on the final screen of the wizard. You should now see the FTP site for the Green Lizard Books appear in the left pane of Internet Services Manager.



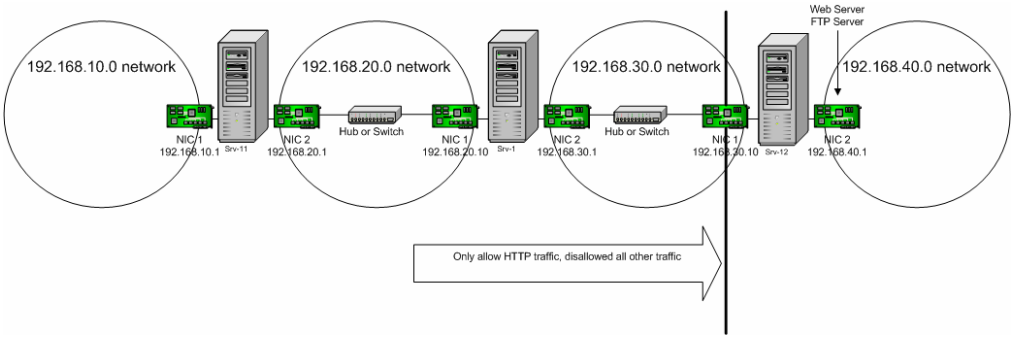
7. Next, make sure that the Default FTP Site has been stopped. If not, you need to stop it by right clicking on **Default FTP Site** and selecting **Stop.**



8. To test this FTP site, open **Internet Explorer** from any one of your servers (SRV-11, SRV-1, or SRV-12)**,** enter **ftp://192.168.40.1** and hit **Enter**. You should be able to view your test FTP site.

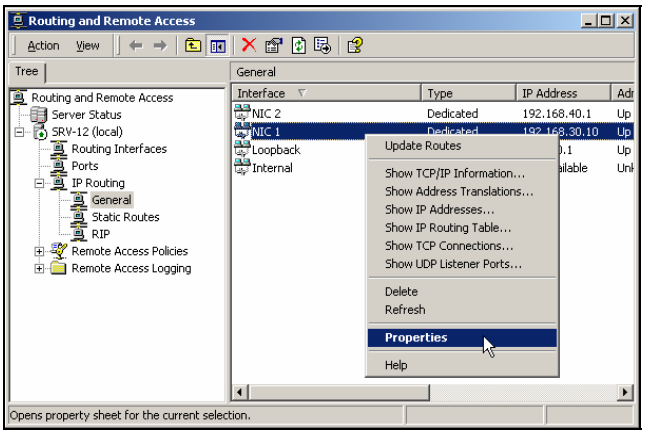


Configuring Packet Filters within RRAS

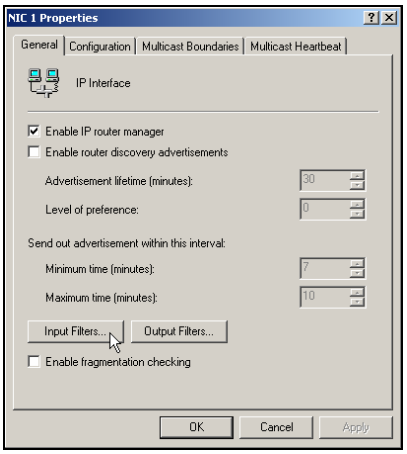


As demonstrated above, you should be able to view both your FTP site and Web site located at IP address, 192.168.40.1, from any of your servers. In order to allow only HTTP traffic and to block all other traffic (including FTP) to this address, you will setup a packet filter on SRV-12's interface (NIC1).

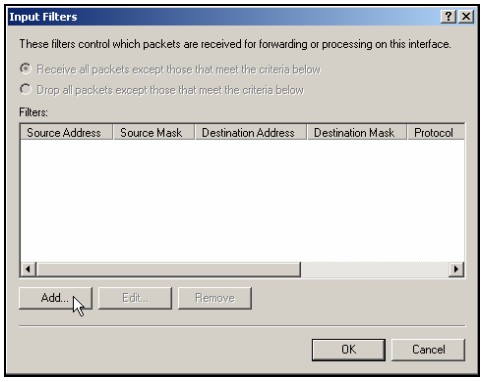
1. Log on to **SRV-12** once again. Open **Routing and Remote Access** by going to **Start→Programs→Administrative Tools→Routing and Remote Access**, double click **IP routing** and click on **General**. Right click on **interface (NIC 1)** and select **Properties**.



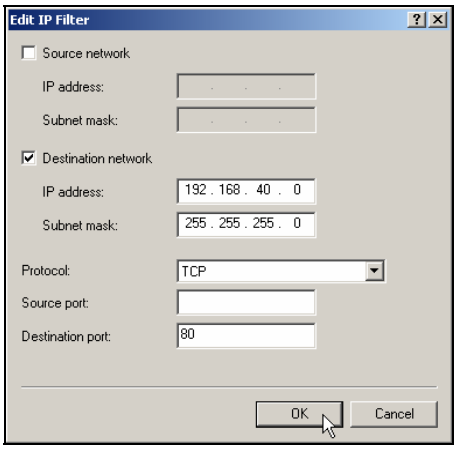
2. This will bring up the NIC1 Properties dialog box. As you see, there are 2 "filters" buttons on the General tab. One is the Input Filters button and the other is the Output Filters button. The Input Filters button is for filtering incoming traffic to this network interface. The Output Filters button is for filtering outgoing network traffic from this network interface. If you refer to the diagram above, you'll see that you only want to allow HTTP traffic and block all other incoming traffic to SRV-12's 192.168.40.1 interface. Therefore, you will have to setup an input filter on interface (NIC1). Click on the **Input Filters** button to begin setting up a packet filter.



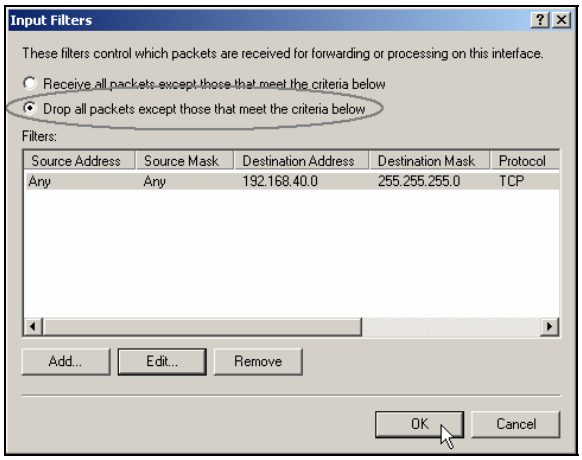
3. On this Input Filters dialog box you will add your filter. First click **Add** to add your input filter.



4. This will bring up the Edit IP Filter dialog box. In this dialog box, you will have to identify the source network, destination network, protocol, source port and destination port for this filter. For the purposes of this lab, you will not need to specify source network because traffic will be blocked from any network segments. Your destination network will have to be specified as the **192.168.40.0** network with **255.255.255.0** as the subnet mask. **TCP** will be the protocol type allowed and port **80 (HTTP)** should be configured as the destination port. Once again, you do not need to configure the source port because it can be from any port. Click **OK** when you are done with the configuration.



5. You now should have one filter in the Filters list. On this Input Filters dialog box, you can specify how this filter is applied. You can either select to receive all packets except those that meet the criteria of your filter or to drop all packets except those that meet the criteria of your filter. Since you only want HTTP traffic to be allowed, select **Drop all packets except those that meet the criteria below** and click **OK** to complete the configuration of the input filter.



6. Once this filter is applied to interface (NIC 1) on SRV-12, no network traffic, except for HTTP traffic, will be allowed to the 192.168.40.0 network. Therefore, you should still be able to view your test web site from SRV-1, but the FTP site and PING should no longer be functional.