Report Number: C4-016R-01

Microsoft Windows 2000? Router Configuration Guide

Architectures and Applications Division
of the
Systems and Network Attack Center (SNAC)

Author:
Florence L. Richburg, Capt, USAF

Updated: May 1 2001
Version 1.02 Draft

National Security Agency
9800 Savage Rd. Suite 6704
Ft. Meade, MD 20755-6704

410-854-6191
securew2k@dewnet.ncsc.mil

This Page Intentionally Left Blank

Warnings

- **Do not attempt to implement any of the settings in this guide without first testing in a non-operational environment.**
- This document is only a guide containing recommended security settings. It is not meant to replace well-structured policy or sound judgment. Furthermore this guide does not address site-specific configuration issues. Care must be taken when implementing this guide to address local operational and policy concerns.
- The security changes described in this document only apply to Microsoft Windows 2000 Server systems and should not be applied to any other Windows 2000 versions or operating systems.
- SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE EXPRESSLY DISCLAIMED. IN NO EVENT SHALL THE CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
- This document is current as of May 1, 2001. See Microsoft's web page http://www.microsoft.com/ for the latest changes or modifications to the Windows 2000 operating system.

This Page Intentionally Left Blank

Acknowledgements

The author would like to acknowledge the NSA authors of the "*Router Security Configuration Guide"* versions 1.0d.

The author would like to acknowledge the NSA authors of the "*Microsoft Windows 2000 Network Architecture Guide"* versions 1.0.

The author would like to acknowledge Neal L. Ziring and Trent H. Pitsenbarger for their help reviewing the document.

Trademark Information

Table of Contents

Table of Figures

Introduction

The purpose of this guide is to provide technical guidance to network administrators of small to medium size networks in the configuration and integration of Microsoft Windows 2000 Server Router features. This guide will also inform the reader about additional security features that are available in the Microsoft Windows 2000 Server Router environment. This guide is not intended to provide individual security settings for the network devices. Instead, it is designed to provide the reader an idea of what functionality is recommended in the integration of the Windows 2000 router within a TCP/IP network.

The Microsoft Windows 2000 Router Configuration Guide presents a general overview of the routing features, recommended routing protocol, and filtering services. This overview is designed to show the recommended functionality in various locations within a network. The author intends for this guide to be used to help the planning phase of a small to medium sized network with typically less than 50 LAN segments. This guide should not be used on its own as an all-encompassing blueprint for router configuration.

This document is intended for Microsoft Windows 2000 network administrators and network designers. However, it should be useful for anyone involved with designing a routable network that includes Microsoft Windows 2000 hosts and/or servers.

Recently, within the DoD community, increased emphasis has been placed on the importance of mitigating impacts of a Distributed Denial of Service (DDOS) attack and mitigating the possibility of DoD networks being used as an agent of an attack against itself, commercial organizations, or even foreign governments. Focus has also been placed on the deterrence of these type activities. Using the Windows 2000 Server Routing features is recommended as a possible solution to this ongoing network concern for small organizations already within a DoD domain or remote locations.

It is important to have a basic understanding of routing before beginning to configure the Windows 2000 Router features. To assist in this understanding, the first section of this guide briefly covers the basics of IP routing.

NOTE: This guide does not address specific security issues for the Microsoft Windows 2000 operating system or any of the other network operating systems or services mentioned.

Getting the Most from this Guide

The following list contains suggestions to successfully secure Windows 2000 Router Configuration according to this guide:

WARNING: This list does not address site-specific issues and every setting in this book should be tested on a non-operational network.

- Read the guide in its entirety. Omitting or deleting steps can potentially lead to an unstable system and/or network that will require reconfiguration and reinstallation of software.
- Perform pre-configuration recommendations:
  - Perform a complete backup of your system before implementing any of the recommendations in this guide

✍✍ Follow the security settings that are appropriate for your environment.

Windows 2000 Routing Focus

This guide will focus on how to configure and use Windows 2000 Server routing features. If your organization is small to medium and cannot support the budget for a dedicated hardware router, but still requires network routing and traffic filtering for enhanced security, Windows 2000 routing may be a viable option. A medium sized network typically has less than 50 network segments. The Windows 2000 Server routing provides multi-protocol LAN-to-LAN, LAN-to-WAN, virtual private network (VPN) and network address translation (NAT) routing services. **Figure 1** displays the recommended configuration environment, which represents a contained domain (reference the Microsoft Windows 2000 Network Architecture Guide). The configuration consists of a Windows 2000 Server computer with two network cards (one card for connection to each separate local network) and two four-port hubs. The recommended configuration does not extend across any networks that are outside the control of the organization.

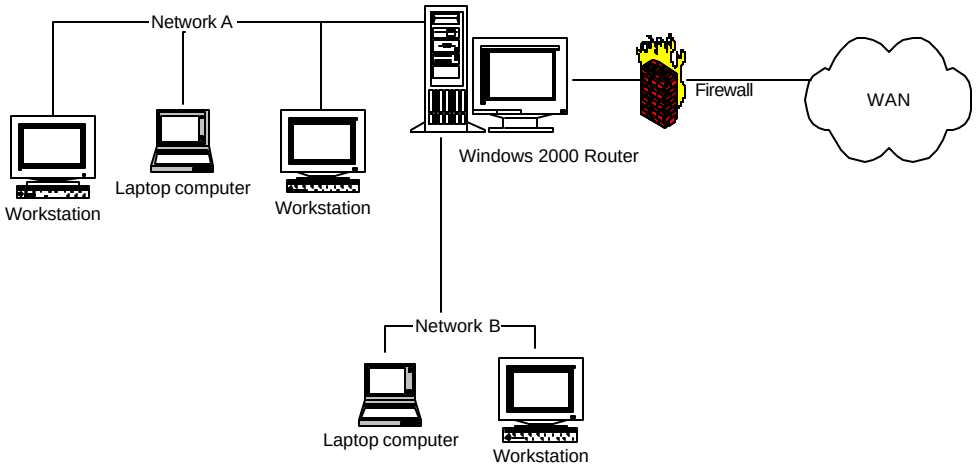

Figure 1 - Recommended Windows 2000 Contained Domain Router Environment

About the Microsoft Windows 2000 Router Configuration Guide

This document consists of the following chapters:

Chapter 1, "Windows 2000 Methods of Routing," contains information on static and dynamic routing, the two standard methods of defining routes between networks.

Chapter 2, "Windows 2000 Routing Configuration," presents a brief introduction to router configuration, step-by-step directions to navigate through the Routing and Remote Access Configuration Wizard, and details on router interfaces for Router Information Protocol (RIP) Version 2.

Chapter 3, 'Windows 2000 Routing Security Configuration," presents details on password authentication, peer security, IPSec, packet filtering configuration, and audit & logging.

Appendix A, "References," contains a list of resources cited.

[redacted]

[redacted]

This Page Intentionally Left Blank

Chapter

1

Windows 2000 Methods of Routing

Routing is the term used to describe the means of directing data from one network segment to another or for communicating with hosts outside a local network if no specific or direct route is known. In the OSI model, routing takes place in the Network Layer (Layer 3) following the Physical and Datalink Layers. At the Network Layer, the router will look at the destination of a given packet to determine either the most efficient or possibly the only route the packet can be delivered. At this point there is a possibility that a packet could be lost or dropped if the destination connection is unavailable or if an undetected link failure occurs at the destination. A packet could also be dropped if a device refuses the packet. Routing is beneficial to a network because it allows the network the ability to handle increased users and data without sacrificing performance. More importantly, routing enables the capability to filter certain traffic for security.

The Windows 2000 Router supports several different routable protocol suites including TCP/IP and IPX Routing. These routing options give Windows 2000 the capability to integrate into an existing network. In general, IP routing may be configured with static routes, dynamic routes, or a mixture of both. Dynamic routes require support for routing protocols. Two of the most common IP routing protocols are Open Shortest Path First (OSPF) and Routing Information Protocol (RIP). Of these two IP routing protocols, RIP is more common and much easier to configure than OSPF. This guide will focus more on the RIP protocol.

The Windows 2000 router can be configured to integrate into an already existing environment consisting of Cisco or other dedicated routing devices. The recommended environment is intended to be representative of a contained DoD infrastructure.

Static and Dynamic Routing

Static and dynamic routing are the two standard methods of defining routes between networks. Static routing manually defines the network routes. Dynamic routing is where the network routes are defined automatically and any changes are also made and updated automatically. Both methods have advantages and disadvantages and can be used with Windows 2000 routing.

The advantage of static routing is that for remote sites or a subnet with only one link to outside connectivity, all non-local traffic can be directed to the next subnet or router. This is an advantage for remote office networks because the routing is simplified by routing all non-local traffic over the single line, which completely eliminates the need for any routing updates. This also reduces network traffic compared to dynamic routing where updates continually put traffic on the network. The main disadvantage of static routing is that the router will not respond to any changes in the network topology. For example, if a primary router is no longer available dynamic changes will not occur. Dynamic routing can, if properly configured, automatically forward traffic along a new route if the primary link becomes unavailable.

In dynamic routing, routing protocols such as RIP (Routing Information Protocol) or OSPF (Open Shortest Path First) communicate the changes and updates between the routers.

The main advantage to dynamic routing is that if any communication link goes down, a new route is automatically defined and is virtually transparent to the users.

In this guide, both Static and Dynamic routing methods are discussed. For example, in **Figure 1**, one could use static routing on the backside of the router with dynamic routing on the side of the router adjacent to the WAN interface. The method used depends on the individual site's network size and requirements.

Chapter

2

Windows 2000 Router Configuration

Configuration Introduction

The first things to do in configuring Windows 2000 Server to function as a router are enabling the Routing and Remote Access Services (RRAS) and adding the routing interfaces. This process will be covered in detail in the next section. With RRAS, your Windows 2000 server can also be configured to function as a remote access server, a Virtual Private Network (VPN) server, a gateway, or a branch-office router. This guide focuses on configuration of the Windows 2000 Server strictly as a gateway router.

Once RRAS has been enabled and the interfaces added, the next step will be to determine which routing protocols and routing features of the Windows 2000 router will be required by your network. For an existing network, determine which protocols and routing features you will need to enable to ensure compatibility. The features that are available at this step are deploying static IP routing, RIP or OSPF protocol.

The last step is to install and configure the protocols. Although not discussed in this guide, you can also configure the DHCP Relay Agent, configure IP multicast support, design and deploy network address translation, configure IPX packet filter, or design and deploy demand-dial routing. An additional routing benefit that will be discussed later is the configuration of IP packet filters that enhances security by filtering certain types of traffic or blocking specific segment destinations.

Although configuring Windows 2000 routing features is fairly simple, it is intended for use by system administrators who are already familiar with routing protocols and services.

NOTE: While any Windows 2000 Server can act as a router, Domain Controllers (DC) should not be used as routers. In the case where a Windows 2000 server is used as the enclave boundary "external" router, the server should not be a member of any domain, but should be administered as a stand-alone host.

For further information on integrating Windows 2000 Services into your environment, please refer to the **Microsoft Windows 2000 Network Architecture Guide**.

Enable Routing and Remote Services

NOTE: While this document briefly introduces Routing and Remote Access Services (RRAS) setup, the reader is referred to the NSA Guide "Remote Access Services" for a more in-depth presentation

The first time Windows 2000 Server is started, you will see the Windows 2000 **Configure Your Server** window. To begin configuration from there, click **Networking**? **Routing**, which will bring up the Windows 2000 Routing Configuration dialog box as shown below in **Figure 2**.

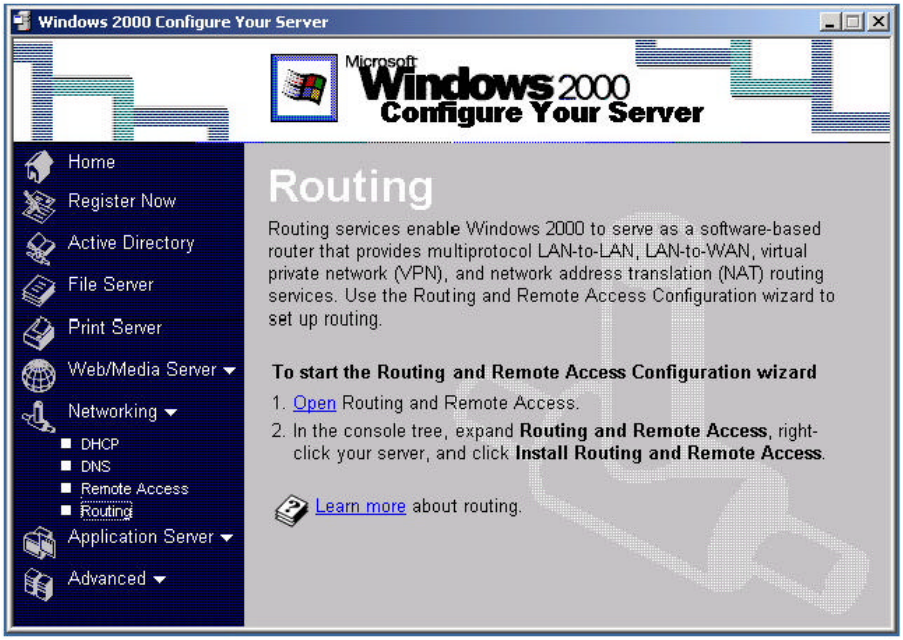

Figure 2 - Windows 2000 Server Router Configuration Dialog Box

From the Routing window, start the Routing and Remote Access Configuration wizard at Step 1. This will bring you to the Routing and Remote Access window shown below in **Figure 3**.

To enable RRAS if you are already running Windows 2000 Server:

- Click **Start**? **Programs**? **Administrative Tools**? **Routing And Remote Access**
- Right click your server name in the left pane of the RRAS console
- Click on the **Configure and Enable Routing and Remote Access**. This will also bring you to the Routing and Remote Access dialog box as shown in below in **Figure 3**.

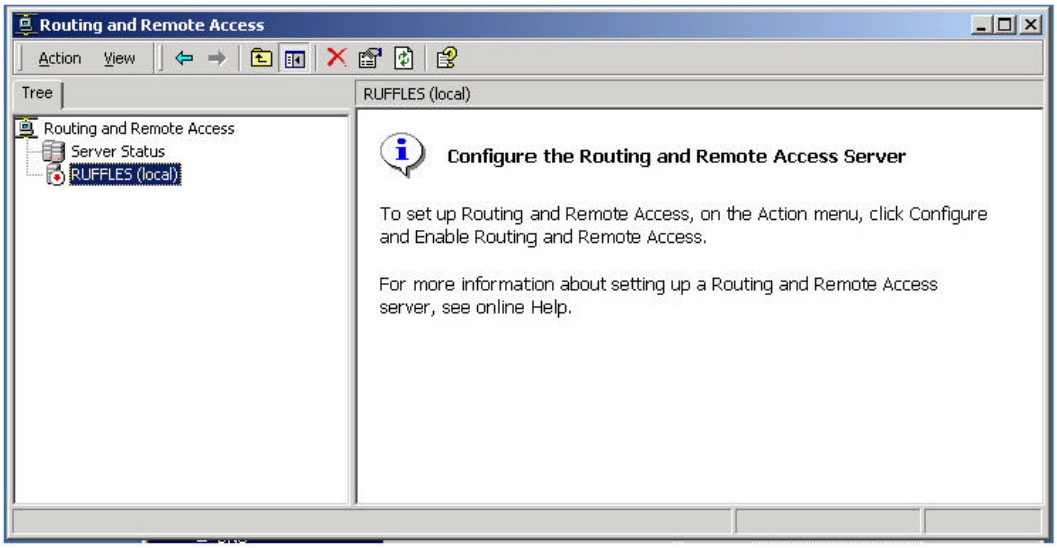

Figure 3 - Routing and Remote Access Configuration Dialog Box

Once the Routing and Remote Access Server wizard has been started, there are several configurations to choose from within the wizard. Select the **Network Router** configuration as shown in below in **Figure 4**. This will enable your network to communicate with other networks as a router.

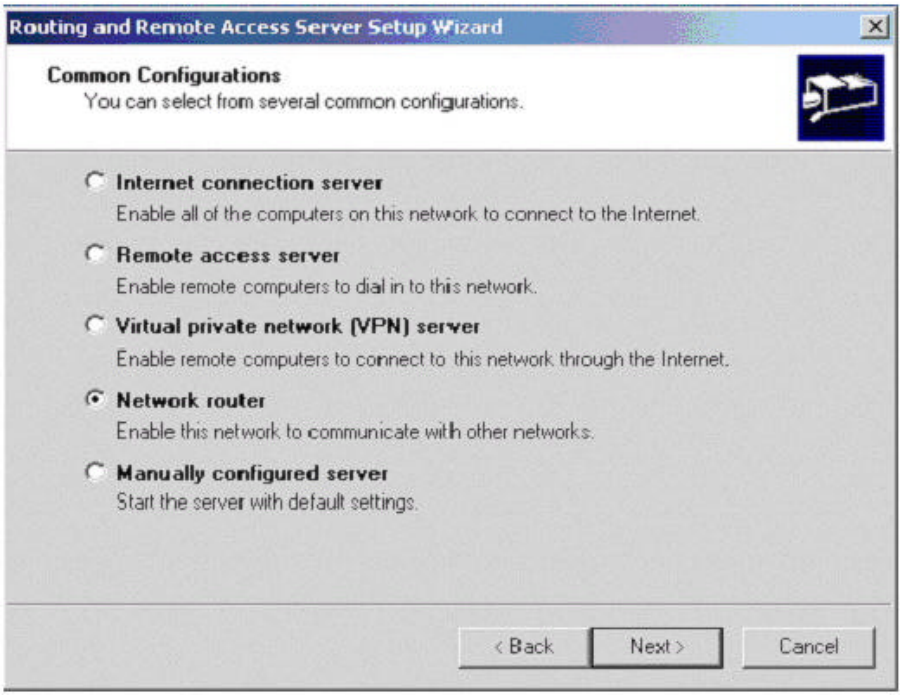

Figure 4 - Routing and Remote Access Server Setup

Continue following the wizard. When you have completed the routing and remote access server setup wizard, the server is now set up as a router. Once you have completed the wizard, the RRAS window should look similar to **Figure 5**.

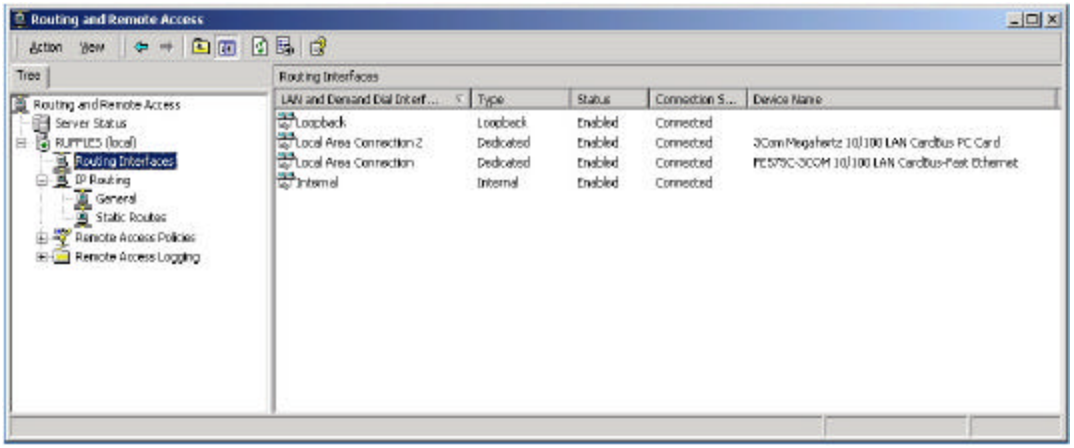

Figure 5 - Routing and Remote Access

At this point, ensure that all the routing interfaces have addresses. The next step is to install and set up routing protocols on each interface, which will be covered in the next section.

Configuration of Router Interfaces for RIP Version 2

Since the Windows 2000 Router is best suited to route small to medium networks, the routing protocol recommended in this guide is RIP. This recommendation is made because RIP is also better suited to support small to medium sized networks with less complexity than the OSPF protocol.

RIP is a dynamic vector-distance routing protocol, meaning that routing decisions are automatically calculated based on the number of intermediate hops to the final destination. By default, the maximum number of hops for RIP is 15, so a hop value of 16 would indicate to RIP that an address is unreachable. A hop value of 1 indicates a directly connected network. Also, the standard for RIP address advertisement is every 30 seconds, with an expiration time of 180 seconds. For example, if a router does not receive an update from another router within 180 seconds, it marks the route from which no update was received as expired or unusable. After the standard default time of 240 seconds, if the router still has no updates, the expired route is then completely removed from the routing table. It is important to make sure all routers in the RIP environment have identical times for each of the three variables, otherwise a loss in connectivity or looping can occur.

Windows 2000 supports the two distinct versions of RIP although they are not compatible with each other. Version 1 of RIP provides basic routing updates by broadcasting updates at specific interval, whereas Version 2 can either broadcast or multicast. RIP Version 2 is recommended for a more efficient configuration and has been used as an example in this guide.

NOTE: Implementation of the OSPF protocol is also supported by Windows 2000, although this guide does not address specific configuration issues. If your network is currently running OSPF, Windows 2000 Router can be configured to integrate into this environment. Before configuring your router with OSPF, solid planning must take place, which should include careful consideration of each level of OSPF design. Design considerations are: Autonomous System Design, Area Design, and Network design. Since OSPF can be quite complex, it is highly recommended to carefully review the OSPF help menus prior

to implementing the protocol. Refer to the NSA "Router Security Guide" for more details on OSPF Configuration.

To configure the Windows 2000 router interfaces for RIP Version 2, perform the following steps:

- From the Routing and Remote Access Window, in the console tree click **General**
- Right click **General**
- Click **New Routing Protocol**
- In the **Select Routing Protocol** dialog box, click **RIP Version 2 for Internet Protocol.** See **Figure 6**.
- Click **OK**.

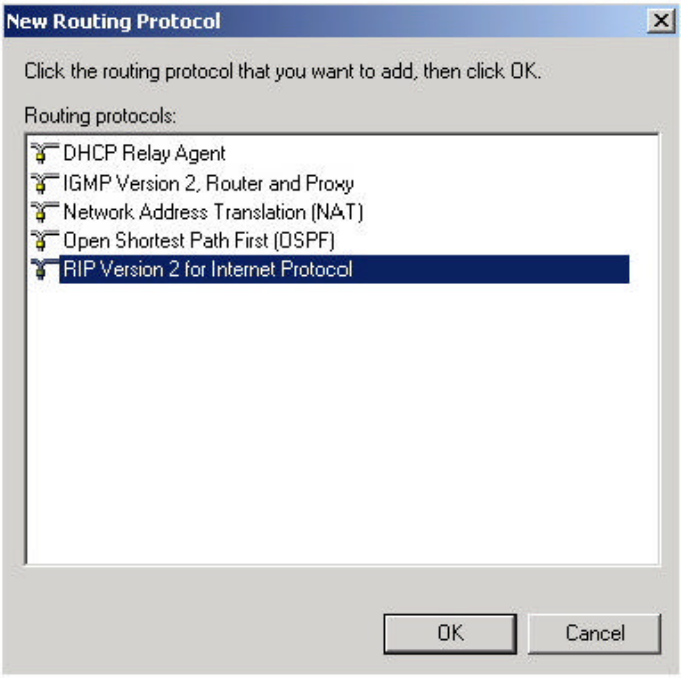

Figure 6 - Select Routing Protocol Dialog Box

Once the Protocol has been added to **Routing and Remote Access**:

- Right-click **RIP**
- Select **New Interface**
- Click the interface, which will be running RIP. You will see the Interface for RIP dialog box as shown in **Figure 7**.

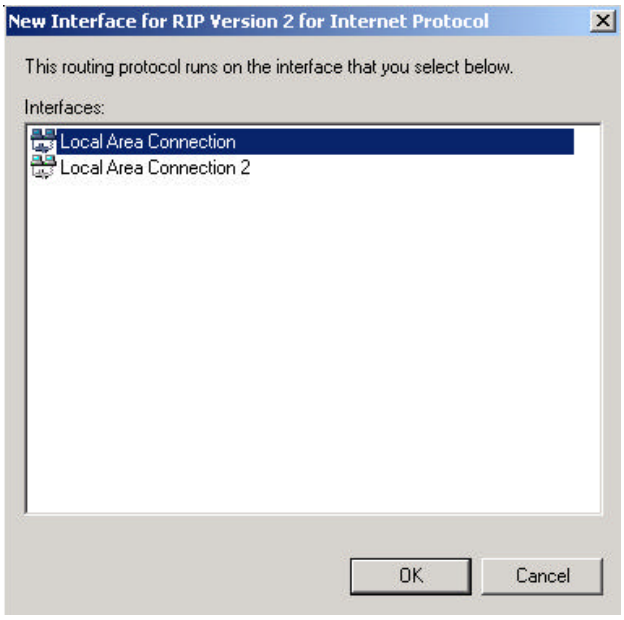

Figure 7 - Interface Protocol Dialog Box

- Select the interface that will be running the RIP v2 protocol.
- After RIP is added to the interface, right click on the interface
- Select **Properties**. This will display the **RIP Properties** dialog box as shown in **Figure 8**.
- At the **General** tab select **Periodic update mode** as the **Operation mode** for the interface. This option allows the networks within the RIP environment to keep in sync as the routing information is being continuously exchanged.

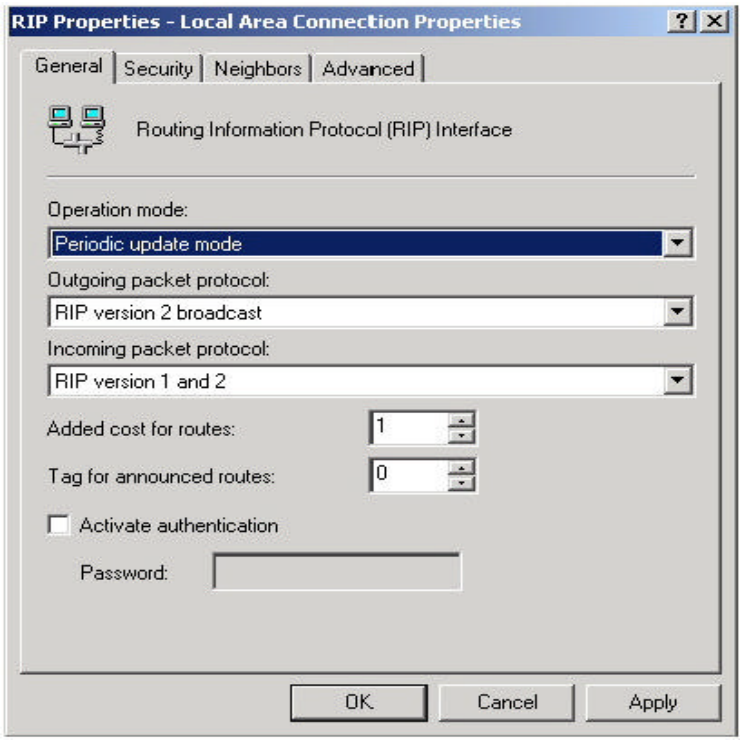

Figure 8 - RIP Interface Properties, General Tab

Although password authentication has not been selected, this option is available to be set at this window. Use password authentication to prevent a denial of service attack by an unauthorized router. When the authentication and password is enabled, when an update is received by the router and contains an incorrect or no password, the router will discard the update. Since Windows 2000 router does not have the option of password encryption, it is possible for a network sniffer to easily capture RIP packets and read the password. **Therefore, use of RIP password authentication for route integrity protection is not recommended at this time.** If route integrity assurance is an important concern for the network, then employ static routes only.

✍✍ Next, click on the Advanced tab as shown in Figure 9.

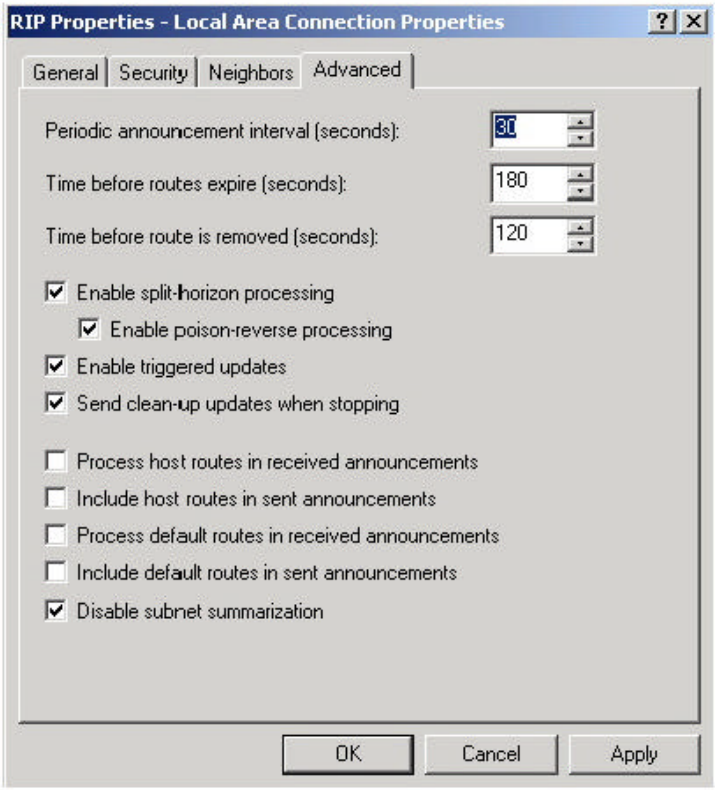

Figure 9 - RIP Interface Properties, Advanced Tab

As mentioned earlier, the values shown in **Figure 9** are the default standard RIP settings. The Windows 2000 RIP feature has several configuration options that can be implemented to counteract common router convergence problems. Two main problems encountered with RIP updates are the possibility of routing traffic through an inefficient path and the possibility of a routing update taking excessive time to converge. Both cases will cause the routing domain to become unstable through link congestion and possible loss of packets.

Split horizon with poison-reverse processing has been enabled to eliminate looping and prevent convergence problems. Enabling triggered updates, clean-up updates and disabling subnet summarization also reduce problems in converging while also decreasing network traffic.

NOTE: After the Windows 2000 Router settings have been configured, it is important to make sure that the neighboring routers are configured with the same settings.

Summary

In summary, the following are recommended when configuring the Windows 2000 Server as a router:

- Domain controllers should not be used as routers.
- In the case where a Windows 2000 server is used as the enclave boundary "external" router, the server should not be a member of any domain, but should be administered as a stand-alone host.
- Windows 2000 Routing is best suited to route small to medium networks. Given this, the recommended routing protocol is the Routing Information Protocol (RIP).
- The use of RIP password authentication is not recommended as the passwords are passed in the clear.
- To help eliminate looping and convergence problems, enable split horizon with poison-reverse processing, triggered updates, clean-up updates, and disable subnet summarization.

Chapter 3

Windows 2000 Router Security Configuration

The following guidelines should be considered in order to enhance the security of the RIP protocol and decrease possible denial of service attacks to the router.

Password Authentication

As mentioned in the previous section, password authentication is an available option as shown in **Figure 8**. However, since the actual password cannot be encrypted, any network sniffer can easily capture the RIP packets and read the password. Again, use of this option is not recommended at this time.

Peer Security

The Windows 2000 router also has a peer security feature, which can be enabled to designate authorized route IP addresses. The addition of peer filters configures peer security. To add peer filters:

- In **Routing and Remote Access**, in the console tree right click **RIP**
- Click **Properties**
- On the **Security** tab, as shown in **Figure 10**, add the IP address of the routers for which update announcements will be accepted. If the broadcast source is an unauthorized router, the update is discarded.

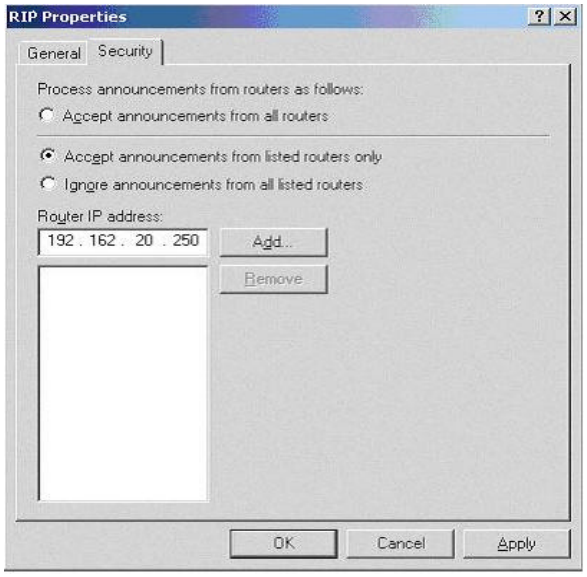

Figure 10 - RIP Peer Security Dialog Box

IPSec

IPSec was developed by the Internet Engineering Task Force (IETF) to provide security for transmission of sensitive information over unprotected networks. IPSec uses encryption to protect the information packets and authenticates the IP packets at the network layer.

The three main technologies IPSec uses are Authentication Header (AH) protocol, Encapsulating Security Payload (ESP) protocol, and Internet Key Exchange (IKE). IPSec used IKE to generate the encryption and authentication keys, which are used to handle the negotiation of the protocols and algorithms.

IKE uses encryption to protect the actual security negotiation. IKE must be able to use at least DES encryption. Therefore, Windows 2000 computers must be able to perform DES in CAPI (Cryptographic API) in order to secure traffic using any type of IPSec packet format.

Unfortunately, Microsoft has confirmed that when using the Windows 2000 router with RIP version 2 or OSPF routing protocols, IPSec or IP-to-IP tunnels cannot be used. This is because both RIP and OSPF routing protocols require a numbered interface to function and neither IPSec nor IP-to-IP tunnels provide a numbered interface. For more information, see Microsoft Knowledge Base Article Q227523 at http://support.microsoft.com/support/kb/articles/Q227/5/23.ASP. This is also why the recommended configuration is with a contained domain environment.

Packet Filtering

One of the main purposes of using the Windows 2000 routing features is to control access to network resources at minimal costs. Controlling access to the network resources can be done by packet filtering.When packet filters are enabled on the router interfaces, detailed rules control what traffic will be accepted or forwarded on that interface. Packet filtering can mitigate the possibility of networks being used as an agent of during a DDOS attack. This section will discuss the configuration of packet filtering.

Before discussing how to configure the Windows 2000 router to filter packets, it is important to understand packet filtering. When a packet arrives at the router interface, the router examines the IP header. The IP Packet header contains the following information, which the router examines:

- Source IP address
- Destination IP address
- IP protocol type (i.e., TCP, UDP or ICMP)

The source IP address is the address of the machine sending the message, the destination IP address is the intended recipient machine address, and the IP protocol type is a higher-level protocol that basically tells IP what the next level of protocol is that will receive the data. The IP protocol types will contain a header, which the router examines. These headers for TCP, UDP or ICMP will include the following information:

- Source TCP or UDP Port number
- Destination TCP or UDP Port number

- ICMP Type number
- ICMP Code number

The Source TCP or UDP port number is the port number from the sending machine. For example, if an HTTP web server machine sends the message, then the source port number will be port 80, because the message was most likely sent out of port 80.

The destination TCP or UDP port number is the port to which the data is being sent. If a message is being sent to an SMTP server, then the destination port number will most likely be port 25.

The ICMP type numbers are used to identify the different types of ICMP messages, for example, Echo Requests, Echo Reply, or Destination Unreachable. The ICMP messages can provide vital information about why a message failed to reach its destination because these messages also include type codes.

Lastly, ICMP Code numbers are codes given to the ICMP Type messages just mentioned. For example, an ICMP Type 3 message of " Destination Unreachable" can be associated with the different code messages such as:

- Destination Unreachable - Network unreachable
- Destination Unreachable - Host unreachable
- Destination Unreachable - Protocol unreachable
- Destination Unreachable - Port unreachable

There are different codes for each of the above Type 3 messages. All of this header information is important to understand when filtering packets. The next section discusses how to configure the router filters.

Configuring Windows 2000 Router Packet Filtering

Packet filtering can only be configured after RRAS has been enabled and the interfaces have been added to the IP Routing General subnode.

To begin the packet filtering option on the Windows 2000 Router at the RRAS window:

- Click **IP Routing** under your router name
- Double-click **General** under **IP Routing**
- Double-click the interface to which you want to add packet filters. This will bring you to the dialog box shown in **Figure 11**.

Packet filtering for Windows 2000 is defined by exception. For example, to define a filter you must decide if you want to allow all packets through except for certain defined packets, or filter all packets and accept only certain ones.

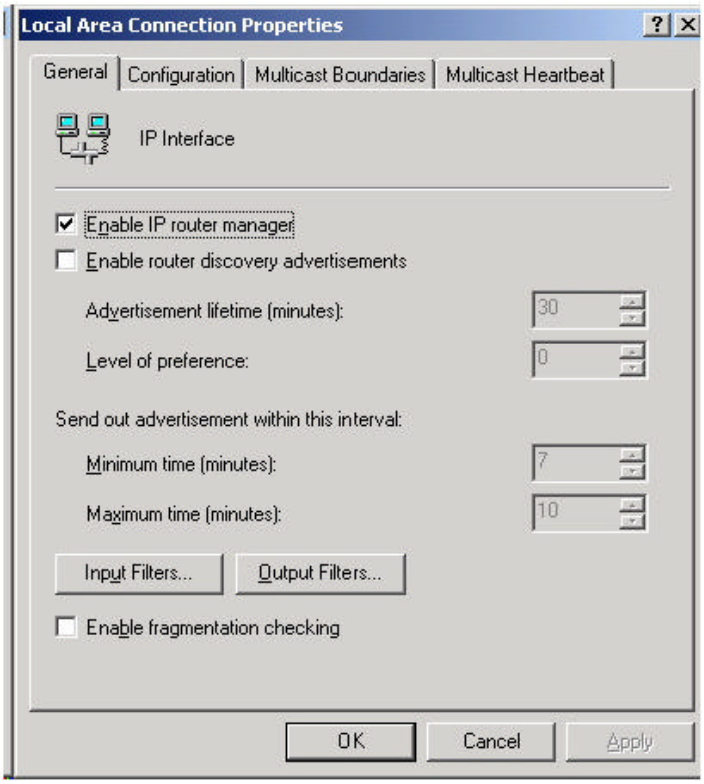

Figure 11 - Local Interface Configuration

Here you will need to decide if you want to configure Input Filters or Output Filters. Input Filters are for filtering packets arriving or coming in to the interface. Output Filters are filters that apply to packets that are being sent out of the interface.

If an Input Filter is defined to drop packets heading for TCP port 80, the filter will drop all incoming packets that have destination TCP port number set to 80, regardless of the destination host IP address. This applies to packets that have a source other than the router itself and must arrive at the interface that has the Input Filter defined.

If an Output Filter is defined for port 21 (FTP) to drop any such requests and a client on the internal network sends a packet to an Internet host with the destination port number of 21, the router interface will not send the packet out.

Select the **Enable fragmentation checking** box to specify whether the router drops all fragmented IP packets it receives on this interface. This option only applies to incoming traffic. If you want to prevent the router from forwarding fragmented IP packets on any interface, select this box on all interfaces on the router.

Refer to the **NSA Router Security Configuration Guide**, section 3.2.2 Packet Filters for TCP/IP for detailed recommendations on applying packet filters. To ensure the optimum security, it is recommended to follow the security principle of "All communications are denied unless expressly permitted". This principle is also recommended in the **NSA Router Security Configuration Guide**, section 3.2.2.

At this point, it also must be determined which services and protocols must cross the router. Once this determination is made, create a set of filtering rules that permit the traffic to cross the router, while prohibiting all other traffic. To accomplish this:

- In the Input Filters Dialog box, click **Add**

- The "Drop all packets except those that meet the criteria below" option should be selected when the specific rules are added at the Add IP Filter Dialog box as shown in Figure 13.

In cases where only certain hosts or networks need access to particular services, add a filter rule that permits that service but only for the specific host address or range of addresses. For example, the network firewall host might be the only address authorized to initiate web connections (TCP port 80) through the router. Each network requirement may be different.

In some cases, the above-mentioned filtering rules may not be practical. If this is the case, then the recommended filtering is to prohibit services that are commonly not needed and if used could potentially open your network to security compromise. Refer to the two tables in the **NSA Router Security Configuration Guide**, section 3.2.2 for detailed instructions on which services to restrict. Also please refer to the **NSA Router Security Configuration Guide,** section 4.3.3. "Filtering Traffic through the Router", which covers IP Address Spoof Protection for Inbound and Outbound traffic. The router should be configured to prohibit traffic on the network that does not have an authorized or valid IP address. An example of this type of filtering is shown below.

In this example an Input Filter is defined by clicking **Input Filter**. See **Figure 12**.

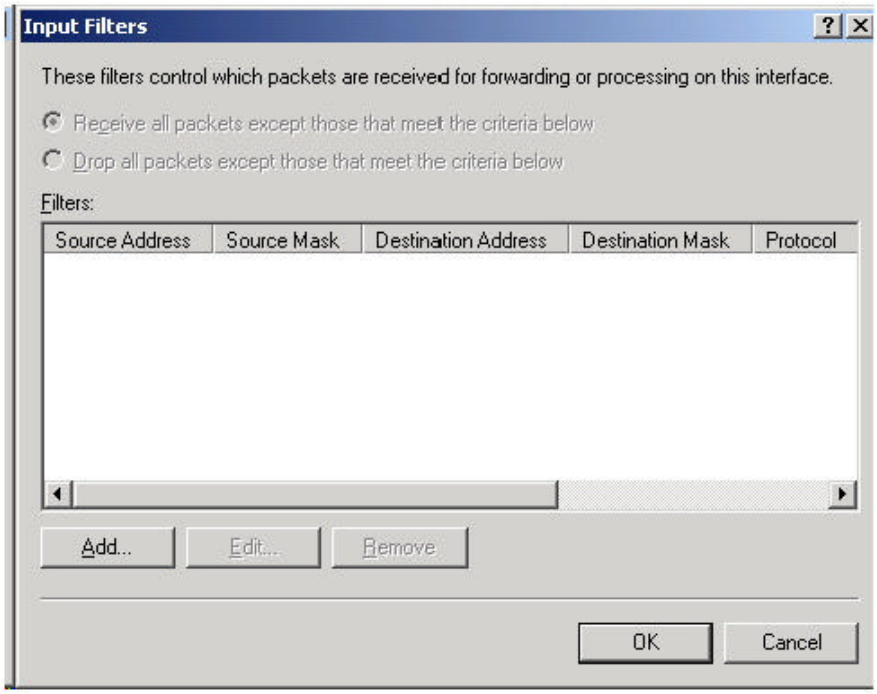

Figure 12 - Input Filters Dialog Box

At the Input Filters dialog, you must first click **Add** before a rule can be defined. See **Figure 13**.

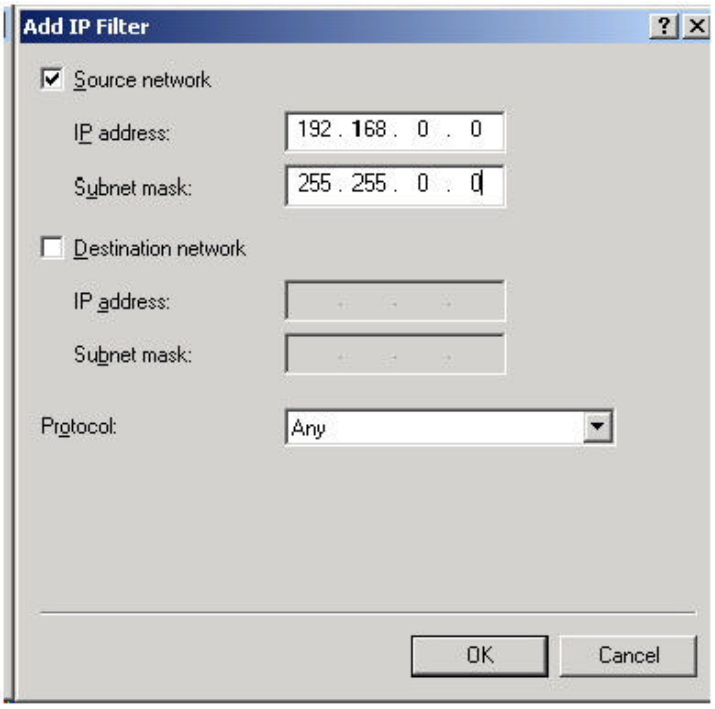

Figure 13 - Add IP Filter Dialog Box

In this example, which illustrates only one portion of an effective router security policy, all packets are allowed through the router except those coming in with a source address from the private network ID 192.168.0.0/16. This is also a good filter to define for any network because many network spoofers often use private network addresses in the source port of their messages.

With the Windows 2000 router, it is best to use general filters that cover a group of computers on a network as shown above. For detailed router security filters, please refer to the **NSA Router Security Configuration Guide** section 4.3.3. "Filtering Traffic through the Router", which covers IP Address Spoof Protection for Inbound and Outbound traffic, Exploits Protection which includes TCP SYN Attack, Land Attack, Smurf Attack, ICMP Message Types & Traceroute, and Distributed Denial of Service Attacks. These instructions can also be applied to the Windows 2000 Router Filters.

Audits and Logging

Please note that when filters are configured on the router interface, the capability to view the actual filter activity is not available although the router will successfully filter or drop designated packets. For example, our filtering example allowed all packets across the local interface except source addresses from the network 192.168.20.0/16. In testing performed by the author, the filter was successful at dropping the appropriate packets as viewed using Network Monitor, but there was no record of actual packets being dropped recorded in any of the Windows 2000 logfiles. This is a significant limitation. If a network is being attacked, it is important for the network administrator to have the capability to view the actual attempted attacks.

Summary

In summary, the following are recommended for enhanced security of the Windows 2000 Server as a router using the RIP protocol:

- Configuration of Peer Security is recommended to enable the designation of authorized routed IP addresses.
- IPSec and IP-to-IP tunnels are designed to enhance secure transmission; however, they cannot be used with PIP viersion2 or OPSP routing protocols.
- Packet filters should also be enabled on the router in order to control what traffic will be accepted and forwarded on the router interfaces. It is best to specify general filters that cover a group of computers on a network rather than specify each individual host. To ensure the optimum security, it is recommended to follow the security principle of "All communications are denied unless expressly permitted."
- In order to help preclude IP address spoofing, the router should be configured to prohibit network traffic that does not have an authorized or valid IP address.

Conclusion

The primary focus of this guide is configuring the Windows 2000 Server Router feature of the Routing and Remote Access application. The Windows 2000 Router platform has numerous other capabilities that have not been discussed in this configuration guide.

The disadvantage of the Windows 2000 routing is the limited security features. If using IPSec, Windows 2000 router does not support the ability to use IPSec with the RIP and OSPF routing protocols. Therefore, the Windows 2000 router does not have the ability to route sensitive information over WANs or the Internet via protected tunneling. Also, although the capability exists to filter specified packets, ports and IP addresses, the router does not provide the capability to record and view the actual denied filter activity. Again, if a network is under attack, even though the router successfully filters, it's important for system administrators to have an awareness that these attempted attacks are occurring. Lastly, the Windows 2000 router does not provide the capability to encrypt the router authentication password. This disadvantage allows any sniffer the ability to collect the packet, read the password in clear text and spoof an authorized router.

Overall, Windows 2000 Server Routing proves to be fairly simple to configure and cost effective. It supports both RIP and OSPF routing protocols, allowing the router the flexibility to be integrated into a variety of routing architectures. The Windows 2000 Router proves to be an acceptable mid range routing solution for small internal network environments. It is not, however, recommend in environments requiring transmission of sensitive information.

This Page Intentionally Left Blank

Appendix

A

References

Black, Ulysses, *IP Routing Protocols*, Prentice Hall, 2000.

NSA System and Network Attack Center, *Router Security Configuration Guide,* May 2000.

NSA Systems and Network Attack Center, *Microsoft Windows 2000 Network Architecture Guide*, October 2000.

Windows 2000 Magazine Website: http://www.winntmag.com