5 Using Routing and Remote Access

Exam Objectives in this Chapter:

- Plan a routing strategy.
  - Identify routing protocols to use in a specified environment.
  - Plan routing for IP multicast traffic.
- Plan security for remote access users.
  - Plan remote access policies.
  - Analyze protocol security requirements.
  - Plan authentication methods for remote access clients.
- Troubleshoot TCP/IP routing. Tools might include the route, tracert, ping, pathping, and netsh commands, and Network Monitor.

Why This Chapter Matters

Modern network installations frequently consist of local area networks (LANs) connected by routers. The LANs might be located at a single site or some distance apart. As a network designer or administrator, you are likely to be responsible for ensuring that the networks can communicate. Routers are complex devices that require a great deal of study, and the Routing and Remote Access (RRAS) service in the Microsoft Windows Server 2003 family includes many of the standard functions and protocols used on routed networks today. Even if you work on an installation that uses hardware routers or software routers with a different operating system from Windows Server 2003, the experience you gain by working with RRAS can benefit you on other platforms.

Lessons in this Chapter:

- Lesson 1: Planning a Routing and Remote Access Strategy ..................... 5-3
- Lesson 2: Static and Dynamic Routing ............................................. 5-12
- Lesson 3: Securing Remote Access .................................................. 5-25
- Lesson 4: Troubleshooting TCP/IP Routing ...................................... 5-43
Before You Begin

Before you begin this chapter, you should have a basic understanding of TCP/IP communications and IP routing principles, as provided in Chapter 2, “Planning a TCP/IP Network Infrastructure.” Reading Chapter 3, “Planning Internet Connectivity,” is also useful, since it contains applications of some of the concepts discussed in this chapter.

Before performing the practice exercises in this chapter, you must install Windows Server 2003 on a computer, using the Setup instructions in “About This Book.”
Lesson 1: Planning a Routing and Remote Access Strategy

The common need to connect networks at different locations compounds the challenges that network designers and administrators face in planning, implementing, and maintaining an internal network. As you learned in Chapter 3, “Planning Internet Connectivity,” a connection between networks at remote locations requires a wide area network (WAN) connection of some type and a router at each site. The WAN is essentially a two-node network that serves only to carry traffic between the two sites, and the routers determine what traffic is permitted to enter and leave each site. Computers running Windows Server 2003 can function as the routers in this arrangement, using RRAS to provide dynamic routing, traffic management, and security features.

After this lesson, you will be able to
■ Describe the characteristics of the WAN technologies most commonly used for remote network connections
■ Decide whether to use static routing or dynamic routing on your network
■ Select the dynamic routing protocol most suitable for your network
■ List the components needed to route IP multicast traffic to an internetwork

Estimated lesson time: 15 minutes

Choosing a WAN Topology

When an enterprise consists of multiple networks at remote locations, connecting them into a single large internetwork is nearly always desirable, but not always economically practical. When deciding whether to connect the network sites, an important part of the process is considering what topologies you can use for the internetwork. Just as with LAN design, in which there are a variety of wiring topologies you can use to connect the computers, internetwork design lets you connect your sites in several different ways.

When you have only two network sites, there is obviously only one topology available. You install a router at each site and connect the routers using a WAN link, as shown in Figure 5-1. In this case, you decide which WAN technology to use based primarily on the bandwidth you need and the cost of the link.
When you have more than two sites to connect, you have more topology choices. The most efficient, and usually the most expensive, remote networking solution is to have a separate WAN link connecting each pair of sites, forming a *mesh topology*, as shown in Figure 5-2. Because each pair of sites has its own dedicated link, the arrangement is highly fault tolerant. Failure of a single link affects only the communications between the two sites connected by that link, and the other connections can compensate by relaying information to the disconnected sites.
The problem with the mesh topology becomes obvious when your enterprise has more than three or four sites. Because each connection requires a router at each site and a separate WAN connection, the amount of time and money required to install and maintain them can quickly become astronomical. A network with three sites requires only three WAN connections to create the mesh, but four sites require six WAN connections. By the time you get to an enterprise with eight sites, you must install 28 separate WAN connections and 56 routers to create the mesh.

**Off the Record** You can implement a large mesh topology using relatively inexpensive equipment, such as dial-up modems and telephone lines, but the performance of an internetwork using slow connections like these is usually not worth the effort.

Another method for connecting sites is to create a *ring topology*. In this topology, the network designer connects each site to its two closest neighbors, as shown in Figure 5-3. This topology requires only two routers and two WAN connections at each site, so it is much easier to install and maintain, as well as being more affordable. However, the ring topology is less efficient than the mesh, because it is not possible for the network at each site to communicate directly with every other site. Unless two sites are adjacent in the ring, traffic has to pass through one or more intermediate sites to get to its destination. This means more traffic on each WAN link, possibly requiring a faster connection than is needed with a mesh topology.

![Figure 5-3 Five network sites connected by WAN links in a ring topology](image)
5-6 Chapter 5 Using Routing and Remote Access

Planning You must determine whether a large number of relatively slow connections is more manageable and affordable than a smaller number of fast connections.

A ring topology is reasonably fault tolerant. Because every site connects to two other sites, the internetwork can compensate for the failure of any single router or WAN connection by sending traffic around the ring in the other direction. This increases the traffic on the other links, but data can still get through to any destination.

For an enterprise that consists of a corporate headquarters and a number of branch offices, the star topology can be a viable compromise between a mesh and a ring. In this topology, one site functions as the hub of the star by having a connection to each of the other sites, as shown in Figure 5-4. A star topology with a single hub site requires as many WAN connections as there are branch offices, substantially fewer than a mesh topology, but more than a ring. However, the star is more efficient than the ring topology, because traffic running between any two sites never has to pass through more than one intermediate network (the hub). The star topology is not as fault tolerant as the ring and mesh topologies. The failure of a single WAN connection affects only the branch office involved, but that office is completely isolated as a result of the failure.

![Figure 5-4 Five network sites connected by WAN links in a star topology](image)

The selection of a WAN topology for your enterprise often depends on the type of WAN connection you elect to use. In addition to varying amounts of bandwidth, WAN technologies also provide varying connection capabilities, which can have a significant effect on the overall cost and efficiency of your internetwork connections.
Selecting a WAN Technology

In Chapter 3, “Planning Internet Connectivity,” you learned about some of the WAN technologies for connecting a private network to the Internet. You can use these same technologies to connect private networks (except for cable television networks, which provide Internet connections only). Leased telephone lines, Digital Subscriber Line (DSL), Integrated Services Digital Network (ISDN), and dial-up modem connections provide varying amounts of bandwidth at various costs, but it would be a mistake to select a WAN technology for your remote network connections based solely on these two criteria. You should also consider the nature of the connections and whether their capabilities suit your needs.

Using Leased Lines

Leased telephone lines are a common type of WAN link used to connect remote networks. A T-1 connection runs at 1.544 megabits/second (Mbps), which is a good deal of bandwidth for internetwork traffic, and fractional T-1 services provide less bandwidth at lower prices. Leased lines can be expensive to install and maintain. After purchasing or leasing the necessary hardware and paying for installation (remembering that hardware and installation costs apply at both ends of the connection), you pay a monthly fee based on the distance between the two sites. DSL connections have many of the same characteristics as traditional leased lines, and are available in a range of speeds and prices.

In addition to bandwidth and cost, two characteristics of leased lines are important to consider: leased lines are persistent connections, and they are permanent. A persistent connection remains open at all times. With a leased line, you pay for the allotted bandwidth around the clock whether you use it or not. For organizations that do not use the connection during off hours, this can waste money. However, it is often possible to use the WAN link even when the offices are closed. You can perform automated tasks such as remote backups and database replications during off hours. A permanent connection is one that is fixed between two sites. After you install a leased line between two locations, moving one of the offices is a lengthy and expensive proposition.

Using Dial-on-Demand Connections

The WAN connections provided by standard asynchronous modems and ISDN are generally slower than leased lines—sometimes much slower—but they have one great advantage. Because these are dial-up services, you can disconnect them at will, and use them to connect to different destinations. The ability to disconnect means that you are paying for only the bandwidth you are using. Both standard telephone lines and ISDN connections typically have a per-minute charge in addition to a monthly fee, so disconnecting during off hours can result in substantial savings.
The ability to connect to different destinations by dialing alternative numbers can have a profound effect on your internetwork design, particularly when you use the dial-on-demand feature incorporated into Windows Server 2003 Routing and Remote Access and into many other routers. *Dial-on-demand* enables a router to connect to a remote network only when a computer sends traffic to a destination on that network.

**Real World  Dial-on-Demand**

You can install a Windows Server 2003 router with an ISDN line at a branch office and configure it to remain idle until someone in the office requires access to a resource at the corporate headquarters. When a user attempts to access a remote resource, the router dials the appropriate number, connects to the headquarters network, and begins routing data. After the transmissions are completed and the ISDN connection has been idle for a specified interval, the router drops the connection until someone needs it again. For WAN technologies that charge by the minute, dial-on-demand prevents you from paying for bandwidth your network is not using, without requiring manual intervention from administrators.

The other advantage of dial-on-demand is that you can use a single dial-up connection to access multiple remote sites. For an organization with ten locations, a mesh topology of WAN connections might be completely impractical using leased lines, but by using a single ISDN line with dial-on-demand at each office, any network can connect to any other network, as needed, simply by dialing the appropriate number. There are drawbacks to this arrangement; for example, each network can connect to only one other network at a time, but for situations where networks need only occasional remote access, dial-on-demand can be an effective and economical solution.

**Exam Tip**  Be sure to understand the ramifications of using persistent WAN connections as opposed to dial-on-demand connections.

**Using Frame Relay**

Frame relay is a popular WAN technology because it provides both flexibility and economy. A frame relay connection consists of a standard leased line linking the network site to the frame relay provider’s nearest point of presence (POP). The provider then furnishes the connection to the frame relay cloud. When you use a frame relay provider for a private network-to-network connection, you must install a leased line at each site that connects the network to the provider’s nearest POP. The provider then connects both lines to the same cloud so that the networks can establish a link.
A private frame relay connection provides the same benefits as a frame relay Internet connection, such as the ability to pay for only the bandwidth you use, and the ability to exceed your contracted bandwidth during heavy traffic periods. In addition, if you select the right provider, frame relay enables you to connect each of your sites to a local POP, reducing the cost of the leased lines. Another major benefit is the ability to connect to multiple sites using a single frame relay connection. You can actually create a mesh topology among all the networks in your enterprise by using a single leased line at each site to connect to a common cloud. Because connections in a frame relay cloud are ephemeral, a single network can simultaneously establish multiple links to different destinations (see Figure 5-5).

**Figure 5-5** Five network sites connected to a single frame relay cloud

**Using VPNs**

All the WAN technologies discussed so far use private carriers to make the connections between networks. However, you can also use virtual private networks (VPNs) to connect networks at remote sites. VPNs are generally practical only for connections
between distant locations, because you still must install a standard WAN connection from each network site to a local Internet service provider (ISP). The benefits of VPN connections are evident when you compare them to leased lines and other technologies that charge based on the distance between the connected sites.

Planning  A company with two offices thousands of miles apart might find it cheaper to install two short-distance leased lines connecting the offices to nearby ISPs instead of one long-distance line connecting the offices directly.

Lesson Review

The following questions are intended to reinforce key information presented in this lesson. If you are unable to answer a question, review the lesson materials and try the question again. You can find answers to the questions in the “Questions and Answers” section at the end of this chapter.

1. Which of the following WAN technologies would be practical to use to create a mesh remote networking topology? (Choose all answers that apply.)
   
   - a. ISDN
   - b. Dial-up modems
   - c. T-1
   - d. Frame relay
   - e. VPNs

2. What term do frame relay providers use to describe the network to which they connect their subscribers’ leased lines?

   ____________________________________________

3. In which of the following WAN topologies can a single cable break totally disconnect one site from the other sites?

   - a. Mesh
   - b. Ring
   - c. Star
   - d. None of the above
Lesson Summary

- A WAN topology is the pattern of connections among your network's various sites. When selecting a topology, be sure to consider the characteristics of the WAN technology you plan to use.

- The WAN technologies you can use to connect remote networks use either persistent connections or dial-on-demand connections.

- Persistent connections provide consistent amounts of bandwidth, usually for a flat monthly fee.

- Dial-on-demand connections enable you to pay for only the bandwidth you use.

- Dial-up services, frame relay, and VPNs all make it possible to create a mesh topology without having to install a separate WAN link for every pair of sites.
Lesson 2: Static and Dynamic Routing

In addition to WAN connections, you also need routers to connect remote networks. Because many of today’s networks use switches internally, many router products are designed primarily to connect remote networks using WAN links. When you are selecting routers for this purpose, one of your first decisions is whether to use hardware or software routers. The Routing and Remote Access service in Windows Server 2003 provides the same routing services as most dedicated hardware routers.

After this lesson, you will be able to

- Describe the characteristics of the WAN technologies most commonly used for remote network connections
- Decide whether to use static or dynamic routing on your network
- Select the dynamic routing protocol most suitable for your network
- List the components needed to route IP multicast traffic to an internetwork

Estimated lesson time: 30 minutes

Selecting Routers

Compared to switches and bridges, which operate at the data-link layer of the Open Systems Interconnection (OSI) reference model, routers are relatively slow devices because they perform more extensive processing on each packet. Hardware-based router products are optimized to perform this type of processing and are therefore generally faster and more efficient than a computer running a software-based router. However, hardware routers also tend to be more expensive and less versatile than software routers. A computer running Windows Server 2003, for example, can handle routing chores as well as performing other server functions as needed.

Planning  The rule of thumb is that when you have a high-speed WAN connection, such as a T-1, that carries heavy traffic, hardware routers are preferable. When the WAN connection is a relatively slow one, such as an ISDN link, or does not carry heavy traffic, a software router can function adequately, usually with far less expense.

Using Static Routing

Another important element of your routing strategy is your decision to use static or dynamic routing on your network. To forward network traffic to the proper locations, the routers on your network must have the correct entries in their routing tables. With static routing, network administrators must manually create and modify the routing table entries. Dynamic routing uses a specialized routing protocol to build and update
the table entries automatically. Static and dynamic routing both provide the same level of router performance. The drawbacks of static routing are the amount of manual maintenance the process requires and the routers’ inability to compensate for changes in the network configuration. Dynamic routing enables routers to compensate for a failed router or WAN link, but it can generate a considerable amount of additional network traffic.

The decision to use static or dynamic routing depends on your routing strategy for the entire enterprise, not just the routers connecting remote networks. If you are using routers to connect multiple LANs at each site, these routers’ tables must have entries that direct traffic destined for other networks to the WAN routers in addition to their internal routing entries. The WAN router tables must have entries that enable them to forward traffic to the appropriate remote site.

Planning When you consider the number of networks, routers, and sites that make up your enterprise, you can decide whether the amount of time and effort needed to maintain static routes is worth the savings in network traffic.

Real World Modifying Routing Tables

The traditional tool for modifying routing tables on a TCP/IP computer, dating back to the earliest UNIX incarnations, is a command line program called route. Most operating systems include a version of this tool; in Windows Server 2003 (and all other versions of the Microsoft Windows operating system), the program is called Route.exe. Using Route.exe’s four subcommands (PRINT, ADD, DELETE, and CHANGE), you can create new routing table entries and modify or delete existing ones.

The ROUTE PRINT command displays the contents of the routing table on a computer running a Windows operating system, as in the following example:

<table>
<thead>
<tr>
<th>Network Destination</th>
<th>Netmask</th>
<th>Gateway</th>
<th>Interface</th>
<th>Metric</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>192.168.2.99</td>
<td>192.168.2.2</td>
<td>1</td>
</tr>
<tr>
<td>127.0.0.0</td>
<td>255.0.0.0</td>
<td>127.0.0.1</td>
<td>127.0.0.1</td>
<td>1</td>
</tr>
<tr>
<td>192.168.87.0</td>
<td>255.255.255.0</td>
<td>192.168.2.21</td>
<td>192.168.2.2</td>
<td>2</td>
</tr>
<tr>
<td>192.168.2.0</td>
<td>255.255.255.0</td>
<td>192.168.2.2</td>
<td>192.168.2.2</td>
<td>1</td>
</tr>
<tr>
<td>192.168.2.2</td>
<td>255.255.255.255</td>
<td>127.0.0.1</td>
<td>127.0.0.1</td>
<td>1</td>
</tr>
<tr>
<td>192.168.2.255</td>
<td>255.255.255.255</td>
<td>192.168.2.2</td>
<td>192.168.2.2</td>
<td>1</td>
</tr>
<tr>
<td>224.0.0.0</td>
<td>224.0.0.0</td>
<td>192.168.2.2</td>
<td>192.168.2.2</td>
<td>1</td>
</tr>
<tr>
<td>255.255.255.255</td>
<td>255.255.255.255</td>
<td>192.168.2.2</td>
<td>192.168.2.2</td>
<td>1</td>
</tr>
</tbody>
</table>
For each routing table entry, the Network Destination and Netmask columns identify a destination network (or host). The Gateway column specifies the IP address of the router the computer should use to transmit packets to the destination. The Interface column specifies which of its network interfaces the computer should use when transmitting data to the Gateway router. The Metric column indicates the relative distance to the destination. For example, the third entry in the sample routing table specifies that to send traffic to any system on the network 192.168.87.0, the computer should transmit the packets to a router with the IP address 192.168.2.21, using its 192.168.2.2 interface.

To create a new entry in the routing table, you use the ROUTE ADD command with parameters that specify the values for the various columns. For example, the command to add the third entry in the sample routing table might appear as follows:

```
route ADD 192.168.87.0 MASK 255.255.255.0 192.168.2.21 METRIC 2 IF 1
```

The address following the ADD parameter is the Network Destination column value. The subnet mask for the destination network address follows the MASK parameter. The IP address following the subnet mask is the Gateway column value. The Metric column value follows the METRIC parameter, and the number following the IF parameter identifies one of the computer's network interfaces. By substituting the DELETE or CHANGE parameter for ADD, you can create commands that remove entries from the routing table or modify existing entries.

When you use the Routing and Remote Access service to configure a computer running Windows Server 2003 as a router, you can view the system's routing table and create new static routes using a graphical interface provided by the Routing And Remote Access snap-in for Microsoft Management Console (MMC), as shown in the following illustration.
Using Dynamic Routing

Dynamic routing uses specialized protocols that enable routers to communicate with each other and share their routing table information. Routers have direct knowledge of only the networks to which they are connected. For a router to efficiently forward traffic to a distant network, it must have information in the form of routing table entries it has obtained from a router connected to that network. When you configure a router to use dynamic routing, it transmits the contents of its routing table to other routers at various intervals.

Dynamic routing eliminates the need for network administrators to manually create static routes on each router. More importantly, dynamic routing enables routers to compensate for changes in the network. For example, network designers often create redundant routes between networks, so that if a router or a connection fails, traffic can still reach any destination. For this type of failover system to work, routing table entries must be changed when a failure occurs. It is possible for administrators to make the changes, if they are on duty when the failure occurs and if they are aware of the failure. However, dynamic routing enables the routers to make these changes automatically.

When a router fails to transmit its routing table entries on schedule, the other routers detect the absence of incoming messages and remove the failed router from their routing tables. This prevents the routers from forwarding traffic to the failed router; instead, they use other paths through the network. When the failed router is back in operation, it resumes transmitting its dynamic routing messages and the other routers on the network begin to use it again by modifying their routing tables accordingly.

Off the Record  On a complex enterprise network, it would be extremely difficult for administrators to monitor all the routers on the network and keep their routing tables updated using manual programs such as Route.exe. Dynamic routing provides a more efficient, automatic solution.

Selecting a Routing Protocol

After you decide to use dynamic routing on your network, the next step is to select the routing protocol. The IP routing that occurs on even the largest private network is relatively simple when compared with the massive routing problems found on the Internet. The TCP/IP standards define many routing protocols, of which private networks only use a few.
Chapter 5 Using Routing and Remote Access

Planning  

The routing protocols most commonly used on private networks are the two supported by the Routing and Remote Access service in Windows Server 2003: Routing Information Protocol (RIP) and Open Shortest Path First (OSPF). In most cases, the designer of a routing strategy selects one of these two protocols.

The following sections compare the characteristics and capabilities of RIP and OSPF, providing the information you need to select the appropriate one for your network.

Understanding Routing Metrics

One of the most important functions of dynamic routing protocols is to evaluate the relative efficiency of routes to a specific destination. On a network with redundant routers, there might be several paths that packets can take from a particular source to a particular destination. When this is the case, a router might have multiple entries for the same destination in its routing table, and it is up to the router to forward packets using the most efficient route available. Routing table entries all include a numeric qualifier called a metric, which the router uses to evaluate routes to the same destination. The lower the metric value, the more efficient the route.

Although IP routers all use the metric the same way, there is no standardized definition for what the metric actually represents, if anything. On a network that uses static routing, network administrators can arbitrarily assign metrics to the routing table entries they create. As long as the routes the administrators want the traffic to take have lower metric values, the routers will choose them instead of routes with higher values. Keeping track of the relative metric values for all the routing tables on the network is another chore that falls to the network administrator who opts to use static routing on a large network.

In dynamic routing, the metric values must represent a specific attribute for routing protocols to compute them. However, different routing protocols use different algorithms to compute the metric for each routing table entry; this is one of the main characteristics that differentiates between routing protocols.

Distance Vector Routing  

RIP uses one of the simplest and most obvious methods for computing routing table metrics. The metric value for each entry in a computer’s routing table represents the number of hops between that computer and the destination. A hop is defined as a passage through a router from one network to another. Therefore,
to reach a destination that is three hops away, packets must pass through three routers. This method is called distance vector routing.

When an enterprise network consists of nothing but LANs all running at the same speed, distance vector routing is an effective method for measuring the relative speeds of different routes through the internetwork. On a network running at one speed, the time it takes for a router to process a packet (called the router's latency period) is the single largest source of delay between the packet's transmission and its arrival at the destination. Therefore, a packet traveling to a destination three hops away is almost certainly going to take longer to arrive than a packet traveling two hops, no matter how long the relative cable segments are.

The distance vector routing that RIP uses is an excellent solution on a network located at a single site, with LANs running at the same speed. However, for an enterprise network that consists of LANs running at different speeds, or that includes slow WAN links to remote sites, distance vector routing is not as effective.

**Real World  Distance Vector Routing**

RIP makes no distinction between different types of networks. A hop is a hop, whether the packets are passing over a 1,000 Mbps Gigabit Ethernet network or a 33 Kbps dial-up modem connection. When you use a distance vector routing protocol like RIP on a mixed-speed network, it is possible for packets using a route with a metric value of 2 to take far longer to reach their destinations than those using a route with a metric value of 3. RIP metrics are therefore not reliable indicators of a route’s efficiency on this kind of a network.

**Exam Tip** Be sure to understand that the metrics in distance vector routing protocols represent the number of hops to the destination, regardless of the type or speed of the network connecting the routers at each hop. RIP is a distance vector routing protocol.

**Link State Routing** The primary difference between RIP and OSPF is the method each protocol uses to compute the metric values for routing table entries. OSPF is called a link state routing protocol because it calculates metrics in a way that provides a much more realistic estimate of each route’s relative efficiency. Instead of relying solely on the number of hops, OSPF uses a method called the Dijkstra algorithm, which uses multiple criteria to evaluate the efficiency of a route. In addition to counting the number of hops, these criteria include the link’s transmission speed and delays caused by network traffic congestion.
Network administrators can also supply a route cost value, which OSPF factors into the equation. This enables administrators to skew the metric values in favor of certain links that they want the routers to use by default. For example, an organization might use a 128 Kbps fractional T-1 connection to link two office networks, while also maintaining an ISDN connection between the two offices as a fallback. The two links run at the same speed, but the administrators want the routers to use the T-1 by default, because they are paying a flat monthly fee for it, while the ISDN connection has a per minute charge. Ordinarily, OSPF would probably assign the same metric to both routes, because they run at the same speed; OSPF might even give the ISDN route a lower metric when the T-1 is experiencing traffic delays. By assigning a lower route cost value to the T-1 route, administrators can ensure that traffic uses the T-1 connection by default, only falling back to the ISDN link when the T-1 fails.

Link state routing is more processor intensive than distance vector routing, but it is also more precise and more capable of compensating for changes in the network infrastructure.

Understanding Routing Protocol Communications

Link state routing is one of the main reasons that administrators choose OSPF over RIP, but there are other considerations when choosing a routing protocol. One of the biggest criticisms leveled at RIP has always been the amount of network traffic it generates. When a RIP router starts, it generates a RIP request message and transmits it as a broadcast over all its network interfaces. The other RIP routers on the connected networks, on receiving the request, generate reply messages containing all the entries in their routing tables. On receiving the reply, the router assimilates the information about the other networks in the enterprise into its own routing table. By exchanging routing table information with all the other routers on their connected networks, RIP routers eventually develop a picture of the entire internetwork, enabling them to forward traffic to any destination.

When a RIP router receives routing table entries from another router, it increments the metric value for each entry before adding it to the table. This enables the routers to keep track of the number of hops needed to reach each destination.

After the initial exchange of messages, the RIP routers all transmit periodic updates at regular intervals. These updates are broadcast messages containing the entire contents of the system’s routing table. An essential part of the RIP communications process, these updates enable RIP routers to determine when another router on the network has
stopped functioning. When a RIP router fails to receive update messages from another router for a specified amount of time, the router recognizing the absence removes the failed router’s entries from its routing table. When the failed router starts transmitting updates again, the other routers add its routing table entries back to their tables.

With every RIP router on the network broadcasting its entire routing table over and over, the amount of network traffic generated by the routers can be enormous. RIP version 2 (included with Windows Server 2003) addresses this problem by adding support for multicast transmissions. A multicast is a transmission addressed to a group of computers with a common attribute or trait. In this case, RIP version 2 routers can transmit their messages to a RIP multicast address so that only the other RIP routers on the network process the messages. This is an improvement over broadcast transmissions because non-routers don’t have to process the RIP messages. However, RIP routers still generate a lot of traffic that can add a significant burden to a busy network.

Planning In addition to its multicasting ability, RIP version 2 can share more routing information than version 1. A RIP version 1 message can carry only a Network Destination and Metric value for each routing table entry. The router receiving the message uses the transmitting router’s IP address for the Gateway value. Most importantly, RIP version 1 messages do not include Netmask values, which is a serious shortcoming if you have subnetted your network. RIP version 2 addresses these problems by including Gateway and Netmask values for each routing table entry. In most cases, if you plan to use RIP on your network, you should make sure that all the RIP routers on your network support RIP version 2.

Off the Record To prevent the OSPF link state replication process from dominating a large network, it is possible to split the network into discrete areas. Each area is a group of adjacent networks, connected to a backbone area. The OSPF routers in each area are responsible only for maintaining a link state database for the networks in that area. Other routers, called area border routers, are responsible for sharing routing information between areas.
Chapter 5 Using Routing and Remote Access

Administering Routing Protocols

OSPF's link state routing capabilities and its ability to form areas make it more efficient and scaleable than RIP, but it does have drawbacks. Deploying RIP on a network is usually simplicity itself. In Windows Server 2003, all you have to do is install the RIP protocol in the Routing and Remote Access service, and RIP immediately begins transmitting its messages. In most cases, RIP requires no additional configuration and no maintenance. OSPF is a different story, however. Deploying OSPF in a large network requires planning so that you can properly create areas and the backbone area. OSPF also requires more configuration and administration than RIP.

Exam Tip When preparing for the exam, no time spent familiarizing yourself with the RIP and OSPF configuration parameters in the Routing And Remote Access console will be wasted. Use the online help to learn the functions of the routing protocol parameters.

Planning RIP is usually the preferable routing protocol on any network that can tolerate its drawbacks. If your network can tolerate the amount of traffic RIP generates, and the network provides a suitably homogeneous environment, you can benefit from the protocol's simplicity and ease of installation. On a large network that uses WAN links to connect remote sites, or that a large amount of broadcast traffic would hamper, you are probably better off expending the time and effort to use OSPF.

Routing IP Multicast Traffic

IP multicasting is a technique that is designed to provide a more efficient method of one-to-many communications than unicast or broadcast transmissions. A unicast transmission, by definition, involves two systems only, a source and a destination. To use unicasts to send the same message to a group of computers, a system must transmit the same message many times. A broadcast message can reach multiple destinations with a single transmission, but broadcasts are indiscriminate. The message reaches every system on the network, whether or not it is an intended recipient. Broadcasts are also limited to the local network, so they can't reach recipients on other networks.

Multicast transmissions use a single destination IP address that identifies a group of systems on the network, called a host group. Multicasts use Class D addresses, as assigned by the Internet Assigned Numbers Authority (IANA), which can range from 224.0.1.0 to 238.255.255.255. Because one Class D address identifies an entire group of systems, the source computer requires only a single transmission to send a message to the entire group.
Members of a multicast group can be located on any LAN in an internetwork and are still accessible with a single transmission. However, for the transmission to reach the entire multicast group, the routers on the network must know which hosts are members of the group in order to forward messages to them.

**Off the Record** Most of the routers on the market today, including the Routing and Remote Access service in Windows Server 2003, support IP multicasting.

Computers that will be members of a multicast host group must register themselves with the routers on the local network, using the Internet Group Management Protocol (IGMP). To support multicasting, all the members of the host group and all the routers providing access to the members of the host group must support IGMP.

**Off the Record** All the Windows operating systems that include a TCP/IP client include support for IGMP.

To receive all the IP multicast traffic on the network, the network interface adapters in a router must support a special mode called *multicast promiscuous mode*. Unlike *promiscuous mode*, in which the network interface adapter processes all incoming packets, multicast promiscuous mode has the network interface adapter process all incoming packets with the multicast bit (that is, the last bit of the first byte of the destination hardware address) set to a value of 1.

**Planning** Most network interface adapters on the market support multicast promiscuous mode, but make sure that the adapters in your routers have this support if you intend to use multicasting on your network.

To support multicasting on a large internetwork, the routers must be able to share their information about host group memberships. To do this, the routers use a multicast routing protocol, such as the Distance Vector Multicast Routing Protocol (DVMRP), the Multicast Open Shortest Path First (MOSPF) protocol, or the Protocol Independent Multicast (PIM) protocol. The Routing and Remote Access service in Windows Server 2003 does not include support for these, or any, multicast routing protocols other than the IGMP routing protocol component, but a Windows Server 2003 router can run a third-party implementation of such a protocol.
Practice: Installing RIP

In this practice, you configure RRAS to function as a LAN router and then install and configure the RIP routing protocol. If you are working on a network, your server will be able to exchange routing table information messages with other RIP routers on the same LAN.

Exercise 1: Configuring Routing and Remote Access as a LAN Router

In this procedure, you configure RRAS to function as a basic LAN router.

1. Log on to Server01 as Administrator.
2. Click Start, point to All Programs, point to Administrative Tools, and then click Routing And Remote Access. The Routing And Remote Access console appears and SERVER01 (local) is listed in the console tree.
3. Click SERVER01 (local) and, on the Action menu, click Configure And Enable Routing And Remote Access. The Routing And Remote Access Server Setup Wizard appears.
4. Click Next. The Configuration page appears.
5. Select the Custom Configuration. Select the Any Combination Of The Features Available In Routing And Remote Access option button and then click Next. The Custom Configuration page appears.
7. Click Finish. A Routing And Remote Access message box appears, asking if you want to start the service.

Exercise 2: Installing RIP

In this procedure, you install the RIP routing protocol on your RRAS router.

1. In the Routing And Remote Access console, expand the IP Routing icon.
3. In the Routing Protocols list, select RIP Version 2 For Internet Protocol and then click OK. A RIP icon appears below the IP Routing icon.
Lesson 2  Static and Dynamic Routing  5-23

4. Click the RIP icon and, on the Action menu, click New Interface. The New Interface For RIP Version 2 For Internet Protocol dialog box appears.

5. In the Interfaces list, select the interface that connects your computer to the LAN and then click OK. A RIP Properties dialog box for your selected interface appears.

In the General tab, you can specify whether the RIP outgoing messages your server transmits should use the RIP version 1 or version 2 packet format, broadcasts or multicasts, or no transmissions at all. You can also specify whether the server should process incoming RIP messages that use the version 1 format, version 2, or both.

6. Click the Advanced tab and then change the Periodic Announcement Interval (Seconds) setting to 300 seconds.

The Periodic Announcement Interval (Seconds) setting is the frequency at which the router transmits its RIP messages. In a stable network where configuration changes and communications failures are rare, you can safely increase this setting to reduce the amount of broadcast traffic RIP generates.

7. Change the Time Before Routes Expire (Seconds) setting to 1800 and the Time Before Route Is Removed (Seconds) setting to 1200.

If you increase the Periodic Announcement Interval (Seconds) value on all the RIP servers on your network, you must increase these two settings as well so that the router does not purge the routing table too quickly of information from RIP.

8. Click OK. The interface you selected appears in the details pane, along with statistical indicators displaying the number of RIP messages the server transmits and receives.


Exercise 3: Disabling Routing and Remote Access

In this procedure, you disable RRAS, removing the configuration you just created. This leaves RRAS in its original state, so that you can create different configurations later in this chapter.

1. Click SERVER01 (local) and, on the Action menu, click Disable Routing And Remote Access. A Routing And Remote Access message box appears, warning you that you are disabling the router.

2. Click Yes. The Routing and Remote Access service is stopped, and the subheadings beneath the SERVER01 (local) icon disappear.

Lesson Review

The following questions are intended to reinforce key information presented in this lesson. If you are unable to answer a question, review the lesson materials and try the question again. You can find answers to the questions in the “Questions and Answers” section at the end of this chapter.

1. To support IP multicasting, which of the following components must be installed on a Windows Server 2003 router? (Choose all correct answers.)
   a. The Protocol Independent Multicast (PIM) protocol
   b. A network interface adapter that supports multicast promiscuous mode
   c. The Routing And Remote Access MMC snap-in
   d. Internet Group Management Protocol

2. Specify whether each of the following characteristics describes distance vector routing, link state routing, or both.
   a. Used by OSPF
   b. Uses the number of hops to the destination when calculating metrics
   c. Uses link speed when calculating metrics
   d. Used by RIP
   e. Unsuitable for enterprises with networks running at various speeds

Lesson Summary

- Static routing is the manual creation of routing table entries, and can require extensive maintenance. It is not practical for large networks with frequent infrastructure changes.

- Dynamic routing uses a specialized routing protocol that automatically compensates for changes in the network. Routing protocols enable routers to exchange messages containing information about their networks.

- RIP is a distance vector routing protocol that is suitable for small networks running at a single speed, but it generates a lot of broadcast traffic. OSPF is a link state routing protocol that is scaleable to support networks of almost any size, but requires more planning, configuration, and maintenance than RIP.

- To support IP multicasting, a router must support IGMP and have network interface adapters that support multicast promiscuous mode.
Lesson 3: Securing Remote Access

The Routing and Remote Access service in Windows Server 2003 provides routing capabilities that enable the computer to forward traffic between LANs, whether they are at the same or distant locations. However, RRAS can also give individual computers at remote locations access to a network, enabling users on the road or working at home to connect to network resources. While remote access can be a tremendous convenience, both to users and to network administrators, it can also be a serious security hazard. Unless you protect your network from unauthorized access, any user with a modem and a telephone line can gain access to your data.

After this lesson, you will be able to

■ Determine the security requirements of your remote access installation
■ Control remote access with user account properties
■ Create remote access policies

Estimated lesson time: 30 minutes

Determining Security Requirements

Before you implement a remote access solution, you should consider what security measures are necessary to grant users the access they need while preventing them from accessing resources for which they lack authorization. To determine what security measures you should use, you must ask questions like the following:

■ Which users require remote access? In most organizations, not every user needs remote access, and you should take steps to limit that access to users who need it. You can specify users who are permitted remote access by authenticating them as they log on and by using remote access policies to dictate conditions that users must meet.

■ Do users require different levels of remote access? Depending on users’ standing in the organization and the resources they need, you can use permissions to assign different levels of remote access.

■ Do users need access to the network? In the case of users whose needs can be met by access to the remote access server, you can prevent them from accessing the entire network.

■ What applications must users run? You can limit users to specific applications by creating packet filters that permit only traffic using specific protocols and port numbers onto the network.
Controlling Access Using Dial-In Properties

The most basic method for securing remote access to your network through a Routing and Remote Access server is to use the properties of the individual accounts that clients use to connect to the network. When you display the Properties dialog box for a user account in the Active Directory Users And Computers console and click the Dial-In tab, you see the interface shown in Figure 5-6.

![Figure 5-6 The Dial-In tab in a user account's Properties dialog box](image)

The security-related options in this tab are as follows:

- **Remote Access Permission (Dial-in Or VPN)**  In this group box, you can specify whether the individual user is allowed or denied remote access, or you can specify that remote access be controlled by using group memberships, as specified in remote access policies.

- **Verify Caller ID**  This check box option enables you to specify the user's telephone number, which the system will verify during the connection process using caller ID. If the number the user calls from does not match the number supplied, the system denies the connection.

- **Callback Options**  This group box enables you to specify that the user cannot use callback, that the user sets the callback options, or that the user must use callback. The callback options cause the Routing and Remote Access server to break the connection after it authenticates a user and then dial the user to reconnect. You can use this mechanism to save on long distance charges by having the remote access calls originate at the server's location, but it can also function...
as a security mechanism if you select the Always Callback To option and then furnish a specific callback number in this option’s text box. If you select the Always Callback To option, the user must be dialing in from the location you specify to connect to the server.

Planning Authentication

Authentication is the most basic form of remote access security. Without it, anyone can connect to your remote access server and gain access to the network. In addition, many of the other remote access security measures that Windows Server 2003 provides are keyed off the user’s identity, which is confirmed by the authentication process.

When you display the Properties dialog box of a Routing and Remote Access server and select the Security tab, you can select the authentication protocol you want to use by clicking Authentication Methods, as shown in Figure 5-7. You should base your selection of an authentication protocol on the amount of security your network needs and the capabilities of your remote access clients, which must be able to support the same protocol.

![Figure 5-7](image)

Figure 5-7 The Security tab in a Routing and Remote Access server's Properties dialog box
Real World Authentication

Most forms of authentication are based on an exchange of user names and passwords. However, passwords are subject to compromise by a variety of methods. Intruders might capture network data packets containing passwords and other account information, and users might write their passwords down and then store them in an insecure place, share them with other users, or even disclose them to social engineers who specialize in providing convincing reasons for needing a person’s private information. The Routing And Remote Access service in Windows Server 2003 includes support for several authentication protocols, which provide varying degrees of protection, primarily by controlling how the systems transmit their passwords to each other. These protocols can’t prevent users from giving away their passwords, but they can stop intruders from intercepted them.

Using RADIUS

In addition to supporting multiple authentication protocols, RRAS enables you to use the Remote Authentication Dial-In User Service (RADIUS), a standard defining a service that provides authentication, authorization, and accounting for remote access installations. RADIUS proxy and server support is a new feature in Windows Server 2003. You can install and use the Microsoft Internet Authentication Service (IAS) server for both RADIUS servers and RADIUS proxies. (You install IAS using Network Services in the Add/Remove Windows Components tool.)

Connection request processing determines how the IAS processes a RADIUS request. When you use an IAS server as a RADIUS server, the server attempts to authenticate and authorize the connection request. If it determines that the request’s credentials are authentic, the RADIUS server authorizes the user’s connection attempt and access, and then logs the remote access connection as an accounting event. When you use IAS as a RADIUS proxy, the proxy forwards the connection request to a member of a remote RADIUS server group for authentication and authorization.

Changing the Authentication Provider setting in the Security tab in the Routing and Remote Access server’s Properties dialog box to RADIUS Authentication activates the Configure button, which enables you to specify the RADIUS server you want to use for remote access authentication.
After you have configured a Routing and Remote Access server to use RADIUS, RRAS transmits all authentication traffic to the RADIUS server for confirmation. The RADIUS server stores all the user accounts and passwords, as well as other account information. The real advantage of RADIUS is that you can run multiple remote access servers and configure them all to use a single RADIUS server for authentication. This way, remote users can access any remote access server, and you have to maintain only a single set of user accounts on the RADIUS server. Organizations that use RADIUS typically have large remote access installations, for example, ISPs.

The Authentication Methods dialog box, shown in Figure 5-8, lists the authentication protocols that Windows Server 2003 RRAS supports. The characteristics of the authentication protocols are as follows:

**Extensible Authentication Protocol (EAP)** An open-ended system that allows RRAS to use third-party authentication protocols as well as those supplied with Windows Server 2003. To use EAP, you select the Extensible Authentication Protocol (EAP) check box in the Authentication Methods dialog box and then click EAP Methods to display the EAP Methods dialog box. This dialog box contains a list of the EAP methods currently installed on the system. EAP is the only authentication protocol supported by Windows Server 2003 RRAS that enables you to use mechanisms other than passwords (such as digital certificates stored on smart cards) to verify a user's identity. In addition to providing the infrastructure to support third-party authentication mechanisms, Windows Server 2003 RRAS supports the following EAP types:
Extensible Authentication Protocol–Message Digest 5 Challenge Handshake Authentication Protocol (EAP–MD5 CHAP)—Uses the same authentication mechanism as CHAP (explained later in this list), but packages the authentication messages in EAP packets.

Extensible Authentication Protocol–Transport Level Security (EAP–TLS)—Required to authenticate remote access users with smart cards or other security mechanisms based on certificates.

Protected EAP (PEAP)—A password-based EAP type designed for wireless networks.

EAP–RADIUS—Not a true EAP type, but a mechanism that enables the Routing and Remote Access server to encapsulate EAP authentication messages in the RADIUS message formation and send them to a RADIUS server.

Microsoft Encrypted Authentication Version 2 (MS-CHAP v2) A password-based authentication protocol that enables the client and the server to mutually authenticate each other using encrypted passwords. This makes it all but impossible for potential intruders to compromise passwords by capturing packets. Microsoft Challenge Handshake Authentication Protocol Version 2 (MS-CHAP v2) is the simplest and most secure option to use when your clients are running Microsoft Windows 98 or later.

Microsoft Encrypted Authentication (MS-CHAP) An earlier version of the Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) that uses one-way authentication and a single encryption key for transmitted and received messages. The security that MS-CHAP v1 provides is inferior to that of version 2, but RRAS includes it as well to support remote access clients running Windows 95 and Windows NT 3.51, which cannot use MS-CHAP v2.

Encrypted Authentication (CHAP) A standard authentication protocol included in RRAS to support non-Microsoft remote access clients that cannot use MS-CHAP or EAP. Less secure than either version of MS-CHAP, Challenge Handshake Authentication Protocol (CHAP) requires access to users' passwords, and by default, Windows Server 2003 does not store the passwords in a form that CHAP can use. To authenticate users with CHAP, you must open the group policy governing users and enable the Store Passwords Using Reversible Encryption password policy. Then you must have every user's password reset or changed so that it is stored in the reversible form that CHAP can use.

Shiva Password Authentication Protocol (SPAP) A relatively insecure authentication protocol designed for use with Shiva remote access products.

Unencrypted Password (PAP) A password-based authentication protocol that transmits passwords in clear text, leaving them open to interception by packet captures. Some RRAS administrators use Password Authentication Protocol (PAP)
as a fallback authentication mechanism for clients that support none of the more secure authentication protocols. Using PAP is better than no authentication at all, but you should be careful not to use it for accounts that have administrative access to servers or other resources, as it can compromise the passwords for these accounts.

■ Allow Remote Systems To Connect Without Authentication Enables remote access clients to connect to the Routing and Remote Access server with no authentication at all, enabling anyone to access the network. The use of this option is strongly discouraged.

Exam Tip You should understand the differences among these authentication protocols and how they provide their respective levels of security.

Using Remote Access Policies

After a Routing and Remote Access server successfully authenticates remote access users and verifies their identities, it attempts to authorize the users. Authorization is the process of determining whether the server should permit the connection to proceed. Even though the server might have successfully authenticated a user, that user must also satisfy a set of conditions before the server can grant the connection. To specify these conditions, you create remote access policies in the Routing And Remote Access console.

Note The use of remote access policies is limited to the Windows Server 2003 family or to Windows 2000 native-mode domains. Mixed-mode and Windows NT domains cannot use them.

Remote access policies are sets of conditions that users must meet before RRAS authorizes them to access the server or the network. You can create policies that limit user access based on group memberships, day and time restrictions, and many other criteria. Remote access policies can also specify what authentication protocol and what type of encryption clients must use. You can also create different policies for different types of connections, such as dial-up, VPN, and wireless.

Remote Access Policy Components

Remote access policies consist of three elements, as follows:

■ Conditions Specific attributes that the policy uses to grant or deny authorization to a user. A policy can have one or more conditions. If there is more than one condition, the user must meet all the conditions before the server can grant access.
Some of the conditions that RRAS remote access policies can require clients to meet are as follows:

- **Authentication type**—Specifies the authentication protocol that the client must use
- **Day and time restrictions**—Specifies the time of day and the day of the week when users must connect
- **Framed protocol**—Specifies the data-link layer protocol that the client must be using
- **Tunnel type**—Specifies the tunneling protocol that a VPN client must be using to connect to the server
- **Windows groups**—Specifies the groups to which the user must belong

**Remote access permission**  Clients receive permission to access the remote network either by satisfying the conditions of the Routing and Remote Access server's remote policies, or by an administrator explicitly granting them the permission in the Dial-in tab in each user's Properties dialog box.

**Remote access profile**  A set of attributes associated with a remote access policy that the Routing and Remote Access server applies to a client once it has authenticated and authorized it. The profile can consist of any of the following elements:

- **Dial-in constraints**—You can use a profile to set limitations to a dial-in connection, such as a time limit for the duration of the connection, an idle time limit before the server terminates the connection, and the hours and days when the client can connect. You can also limit client access to specific server telephone numbers or specific media types.
- **IP**—You can specify whether the clients or the server should supply the IP addresses the clients use, or you can specify a static IP address that the server should assign to the client. You can also create input and output filters that limit the types of traffic exchanged by the clients and the server, based on IP addresses, port numbers, or both.
- **Multilink**—Grants the client permission to use the Windows Multilink feature, which enables the client to combine the bandwidth of multiple modem connections into a single data pipe. You can also limit the number of connections you permit a client to use, and you can specify Bandwidth Allocation Protocol (BAP) settings.
- **Authentication**—Enables you to specify the authentication protocol the client must use to connect to the server, using the same selection of protocols as in the Authentication Methods dialog box, described earlier in this lesson.
Lesson 3  Securing Remote Access  5-33

❑ Encryption—Enables you to specify the types of encryption that clients can use when connecting to the server.

❑ Advanced—Enables you to set values for special attributes that RADIUS servers use when communicating with the Routing and Remote Access server.

Creating Remote Access Policies

To create a remote access policy, you open the Routing And Remote Access console, expand the icon for your Routing and Remote Access server, and click the Remote Access Policies subheading (see Figure 5-9). In the details pane is a list of the policies that already exist on the server. You can modify these policies or add new ones.

![Figure 5-9  The Remote Access Policies node in the Routing And Remote Access console](image)

**Important**  Before RRAS can use remote access policies to regulate access to the server by group membership, you must configure the user's account by selecting the Control Access Through Remote Access Policy option button in the Dial-in tab in the user's Properties dialog box in the Active Directory Users And Computers console.

When you select New Remote Access Policy from the console's Action menu, the New Remote Access Policy Wizard launches and walks you through the steps of creating the new policy by specifying values for the conditions described earlier. After you finish using the wizard, the console adds the new policy to the bottom of the list in the details pane.

**Tip**  Administrators can configure remote access policies to either grant or deny user access based on the specified conditions. In some cases, it is easier to deny access based on a smaller set of conditions than it is to grant them based on a larger set. For example, if nine groups should receive permission to access the network remotely, and one group should be denied permission, it is easier to grant all users permission by default and explicitly deny permission to that one group rather than grant permission to nine different groups.
When multiple policies are listed in the details pane, you can control the order of the list by clicking a policy and choosing Move Up or Move Down from the Action menu. The order of the policies is important, because the RRAS applies them in order to each connection attempt. The logic sequence for the connection process is as follows:

1. RRAS checks the incoming connection against the first remote access policy in the list. If there are no policies in the list, RRAS rejects the connection attempt.

2. If the incoming connection does not satisfy all the conditions in the first policy, RRAS proceeds to check the connection against the next policy in the list.
   If the incoming connection does not satisfy all the conditions in any one of the policies in the list, RRAS rejects the connection attempt.

3. When the incoming connection does satisfy all the conditions of one of the policies in the list, RRAS checks the value of the user's Ignore-User-Dialin-Properties attribute, which you set in the Advanced tab of the profile settings for a remote access policy.

4. If the Ignore-User-Dialin-Properties attribute is set to False, RRAS checks the remote access permission setting for the user account attempting to connect.
   If the Deny Access option is selected, RRAS rejects the connection attempt.
   If the Allow Access option is selected, RRAS applies the user account and profile properties to the connection. If the connection attempt does not match the settings of the user account and profile properties, RRAS rejects the connection attempt. If the connection attempt matches the settings of the user account and profile properties, RRAS accepts the connection attempt.
   If the Control Access Through Remote Access Policy option is selected, RRAS checks the remote access permission setting of the policy. If Deny Access is selected, RRAS rejects the connection attempt. If Allow Access is selected, RRAS applies the user account and profile properties, accepting the connection attempt if it matches the user account and profile properties settings, and rejecting the attempt if it does not.

5. If the Ignore-User-Dialin-Properties attribute is set to True, RRAS checks the remote access permission setting of the policy.
   If Deny Access is selected, RRAS rejects the connection attempt.
   If Allow Access is selected, RRAS applies the profile properties, accepting the connection attempt if it matches the profile properties settings, and rejecting the attempt if it does not.
Using Network Access Quarantine Control

The remote access security measures you have seen so far have all related to authenticating the incoming user. Network Access Quarantine Control, a new feature in Windows Server 2003 with Service Pack 1 (SP1), gives network administrators the ability to validate the configuration of remote client computers before granting access to the entire corporate network.

Typical remote access configurations can only validate the credentials of the remote access user and check that the user has permission to make a remote connection. Therefore, a remote computer can access internal network resources even when the remote computer’s configuration does not comply with organization network policy. Therefore, the remote computer might not have:

- The correct service pack or the latest security patches installed.
- The correct antivirus software and signature files installed.
- Routing disabled. A remote access client computer with routing enabled might pose a security risk, providing an opportunity for a malicious user to access corporate network resources through the client computer, which has an authenticated connection to the private network.
- Firewall software installed and active on the Internet interface.
- A password-protected screensaver with an adequate wait time.

Despite the efforts made within organizations to ensure that computers physically attached to the network comply with network policy, those computers that remote or mobile workers use for remote access connections can present significant risk to the network.

Network Access Quarantine Control delays full access to a private network until the configuration of a connecting remote computer has been examined and validated. When a remote computer initiates a connection to a remote access server, the user is authenticated and the remote access computer is assigned an IP address. However, the computer is placed in quarantine mode with limited network access. The client component of the administrator-provided script is run on the remote access computer. When the script notifies the remote access server that it has successfully run and the remote access computer complies with current network policies, quarantine mode is removed and the remote access computer is granted normal remote access.

The quarantine restrictions placed on individual remote access connections consist of the following:

- A set of quarantine packet filters that restrict the traffic that can be sent to and from a quarantined remote access client.
A quarantine session timer that restricts the amount of time the client can remain connected in quarantine mode before being disconnected.

You can use either restriction, or both, as needed.

**Important** Network Access Quarantine Control is not a security solution. It is designed to help prevent computers with unsafe configurations from connecting to a private network, rather than to protect a private network from malicious users who have obtained a valid set of credentials.

### The Components of Network Access Quarantine Control

The components required for this remote access quarantine solution include the following:

- **Quarantine-compatible remote access clients** Client computers must be configured to run the Remote Access Quarantine Client and the validation script. The supported client operating systems are Windows Server 2003, Windows XP, Windows 2000, Windows Me, and Windows 98 SE. These versions of Windows support Connection Manager (CM) profiles that are created with the Connection Manager Administration Kit (CMAK) provided in Windows Server 2003 with SP1. The CM profile contains the following:
  - A postconnect action that runs a network policy requirements script. This is configured when the CM profile is created with CMAK.
  - A validation script that performs validation checks to verify that the remote access client computer conforms to the minimum security guidelines required to access the corporate network. If the script does not run successfully and the connecting computer does not satisfy all of the network policy requirements, the script should direct the remote access user to a quarantine resource such as an internal Web page, which describes how to install the components that are required for network policy compliance.
  - A notifier component that sends a message that indicates a successful execution of the script to the quarantine-compatible remote access server. You can use your own notifier component or you can use Rqc.exe, which is provided with the Windows Server 2003 Resource Kit Tools for computers running...
Windows Server 2003 with no service packs installed. For computers running Windows Server 2003 with SP1, Rqc.exe is installed with the CMAK component in the Program Files\CMAK\Support folder. The CMAK component is installed through the Add/Remove Windows Components option, accessed through the Add Or Remove Programs Control Panel icon.

- **Quarantine-compatible remote access server**  The Remote Access Quarantine Service (Rqs.exe) or Listener runs on the RRAS server and listens for requests from the remote clients for removal of quarantine restrictions.

- **Quarantine-compatible RADIUS server (optional)**  If RRAS on the remote access server is configured for RADIUS authentication, a quarantine-compatible RADIUS server running Windows Server 2003 and IAS is required.

- **Quarantine resources**  These resources consist of servers that a remote access client in quarantine mode can access to perform name resolution (such as DNS servers), obtain the latest version of the CM profile (file servers with anonymous access allowed), or access instructions and components needed to make the remote access client comply with network policies (Web servers with anonymous access allowed). Anonymous access to file and Web resources are needed because, although the remote access user has the correct credentials to create the remote access connection, he or she might not be using the correct domain credentials to access protected file and Web resources.

- **Accounts database**  For Windows Server 2003 or Windows 2000–based networks, Active Directory is used as the accounts database to store user accounts and their dial-in properties.

- **Quarantine remote access policy**  Configured with the required conditions for remote access connections, and with profile settings that can specify the MS-Quarantine-IPFilter or MS-Quarantine-Session-Timeout attributes. The packet filters configured for the MS-Quarantine-IPFilter attribute provide the quarantine of the remote access client until the notifier component on the remote access client indicates that the computer is in compliance with network policies. You use the MS-Quarantine-Session-Timeout attribute to specify how long the remote access server must wait to receive the notification that the script has run successfully before terminating the connection.

Figure 5-10 shows the components of Network Access Quarantine Control with RADIUS as the authentication provider.
Chapter 5  Using Routing and Remote Access

Practice: Installing a Routing and Remote Access Server

In this practice, you configure the Routing and Remote Access service on Server01 to function as a remote access server. For the purposes of this exercise, the Microsoft Loopback Adapter is assumed to be connected to a WAN device providing a connection to an ISP. Remote access clients can access the server using VPN connections. The other adapter (which is the actual network interface card in the computer) is connected to the local private network. After configuring RRAS, you create separate remote access policies for your domain users and administrators, with different security conditions.

Exercise 1: Configuring Routing and Remote Access as a Remote Access Server

In this procedure, you configure RRAS on Server01 to function as a remote access server, supporting both dial-in and VPN connections.

1. Log on to Server01 as Administrator.

2. Click Start, point to All Programs, point to Administrative Tools, and then click Routing And Remote Access. The Routing And Remote Access console appears and SERVER01 (local) is listed in the console tree.

3. Click SERVER01 (local) and, on the Action menu, click Configure And Enable Routing And Remote Access. The Routing And Remote Access Server Setup Wizard appears.
4. Click Next. The Configuration page appears.

5. Accept the (default) Remote Access (Dial-up Or VPN) option button and then click Next. The Remote Access page appears.

6. Select both the VPN and Dial-up check boxes and then click Next. The VPN Connection page appears.

7. Click the WAN Connection interface in the Network Interfaces box and then click Next. The IP Address Assignment page appears.

8. Accept the (default) Automatically option button and then click Next. The Managing Multiple Remote Access Servers page appears.

9. Accept the (default) No, Use Routing And Remote Access To Authenticate Connection Requests option button and then click Next. The Completing The Routing And Remote Access Server Setup Wizard page appears.

10. Click Finish. A Routing And Remote Access message box appears, warning you to configure the DHCP Relay Agent to service clients on other networks.


Notice that the IP Routing icon contains four subheadings: General, Static Routes, DHCP Relay Agent, and IGMP, and that the SERVER01 (local) icon now has Remote Access Clients, Remote Access Policies, and Remote Access Logging subheadings.

12. Leave the Routing And Remote Access console open for later practices.

Exercise 2: Creating a Remote Access Policy for Domain Users

In this procedure, you create a remote access policy that is designed to grant your domain users remote access to the network using VPN connections only. You do this using one of the common scenarios scripted into the New Remote Access Policy Wizard.


2. Click Next. The Policy Configuration Method page appears.

3. Accept the (default) Use The Wizard To Set Up A Typical Policy For A Common Scenario option button, and in the Policy Name text box, type Domain Users VPN. Click Next. The Access Method page appears.

4. Select the VPN, Use For All VPN Connections, To Create A Policy For A Specific VPN Type, Go Back To The Previous Page, And Select Set Up A Custom Policy option button and then click Next. The User Or Group Access page appears.
5. Accept the (default) Group, Individual User Permissions Override Group Permissions option button and then click Add. A Select Groups dialog box appears.

6. Type **Domain Users** in the Enter The Object Names To Select text box and then click Check Names. Domain Users now appears underlined.

7. Click OK. The Domain Users group is added to Group Name box in the User Or Group Access page. Click Next. The Authentication Methods page appears.

8. Accept the (default) Microsoft Encrypted Authentication Version 2 (MS-CHAPv2) option button and then click Next. The Policy Encryption Level page appears.


10. Click Finish. The Domain Users VPN policy you created now appears in the console's details pane in the Remote Access Policies list.

**Exercise 3: Creating a Remote Access Policy for Domain Administrators**

In this procedure, you create a remote access policy that enables the domain administrators to connect to the remote access server using dial-in connections, but only with specific authentication and encryption protocols. You do this using the custom policy capabilities of the New Remote Access Policy Wizard.


2. Click Next. The Policy Configuration Method page appears.

3. Click the Set Up A Custom Policy option button and then type **Administrators Dial-in** in the Policy Name text box. Click Next. The Policy Conditions page appears.

4. Click Add. The Select Attribute dialog appears.

5. Scroll down the Attribute Types list and click Windows-Groups. Click Add. The Groups dialog box appears.

6. Click Add. A Select Groups dialog box appears.

7. Type **Domain Admins** in the Enter The Object Names To Select text box and then click Check Names. Domain Admins now appears underlined.

8. Click OK. The Domain Admins group is added to the Groups list in the Groups dialog box.

9. Click OK. The Windows-Groups condition you just created is added to the Policy Conditions list. Click Next. The Permissions page appears.
10. Click the Grant Remote Access Permission option button and then click Next. The Profile page appears.

11. Click Edit Profile. The Edit Dial-In Profile dialog box appears.

12. Click the Authentication tab and clear all the check boxes except Microsoft Encrypted Authentication Version 2 (MS-CHAP v2).

13. Click the Encryption tab and clear all the check boxes except Strongest Encryption (MPPE 128 bit).

14. Click OK to return to the Profile page and then click Next. The Completing The New Remote Access Policy Wizard page appears.

15. Click Finish. The Administrators Dial-In policy you just created now appears in the console’s details pane in the Remote Access Policies list.


**Lesson Review**

The following questions are intended to reinforce key information presented in this lesson. If you are unable to answer a question, review the lesson materials and try the question again. You can find answers to the questions in the “Questions and Answers” section at the end of this chapter.

1. Which of the following authentication protocols do you use with smart cards?
   a. MS-CHAP v2
   b. EAP-TLS
   c. PEAP
   d. PAP

2. What is the function of a RADIUS server in a remote access installation?

3. How does the callback option in a user account’s dial-in properties function as a security feature?
4. Which of the following is not a component of a remote access policy?
   a. Authentication protocol
   b. Conditions
   c. Remote access profile
   d. Remote access permission

Lesson Summary

- To determine the security requirements you need for your remote access server, determine which users need remote access to the network, what type of access they need, and whether different users require different degrees of access.
- RRAS supports several authentication protocols, including EAP, MS-CHAP (versions 1 and 2), CHAP, SPAP, and PAP.
- Remote access policies are sets of conditions that remote clients attempting to connect to the Routing and Remote Access server must meet. You can use policies to control remote access based on group membership and other criteria.
- RRAS matches each connection attempt against the list of remote access policies you create on the server. The server grants access only when a connection meets all the conditions in one of the policies.
- Remote access profiles are sets of attributes that RRAS applies to connections after successfully authenticating and authorizing them. You can use profiles to control when clients can connect to the network, what types of IP traffic you permit them to use, and what authentication protocols and encryption algorithms they must use.
Lesson 4: Troubleshooting TCP/IP Routing

The Routing and Remote Access service is one of the more complex components in Windows Server 2003. Because RRAS can perform so many functions, it has a large number of configurable settings. Even a minor misconfiguration can prevent the server from routing traffic properly. The TCP/IP implementation in Windows Server 2003 includes a variety of tools that you can use to troubleshoot RRAS and its various functions.

After this lesson, you will be able to

■ Use TCP/IP tools to isolate a router problem
■ Check an RRAS installation for configuration problems
■ Troubleshoot static and dynamic routing problems

Estimated lesson time: 20 minutes

Isolating Router Problems

In most cases, administrators discover router problems when communications fail between computers on the network. However, once the troubleshooter suspects that there might be a routing problem, the next step is to determine which router is malfunctioning. Some of the TCP/IP tools in the Windows operating system that can help you in this respect are discussed in the following sections.

Using Ping.exe

PING is the standard TCP/IP tool for testing connectivity; virtually every TCP/IP client includes a PING implementation. In the Windows operating systems, PING takes the form of a command line program called Ping.exe. By typing ping followed by an IP address on the command line, you can test any TCP/IP system’s connectivity with any other system.

Note  PING functions by transmitting a series of Echo Request messages containing a sample of random data to the destination you specify, using the Internet Control Message Protocol (ICMP). The system that receives the Echo Request messages is required to generate an Echo Reply message for each request that contains the same data sample and return the messages to the sender.

Compared to other tools, PING has limited utility when you are trying to locate a malfunctioning router. You might be able to ping a router’s IP address successfully even
Chapter 5  Using Routing and Remote Access

when it is not routing traffic properly. However, as part of your initial troubleshooting efforts, you can use PING to test a routed network connection in the following manner:

1. Ping the computer’s loopback address (127.0.0.1) to confirm that the TCP/IP client is installed and functioning.

   If this test fails, there is a problem with the TCP/IP installation on the computer, with the network interface adapter, or with the network adapter driver. The problem is not caused by network cables or other external hardware, because messages addressed to the loopback address never leave the system.

2. Ping the computer’s own IP address to confirm that the routing table contains the appropriate entries.

   A properly configured routing table contains an entry with the computer’s own IP address as the network destination and the loopback address as the gateway the system should use to reach that destination. If this test fails (after you have successfully pinged the loopback address), this entry in the routing table is missing or incorrect. You should check the routing table carefully at this point, because other important entries might also be missing or incorrect.

3. Ping the IP address of another computer on the same LAN.

   This test confirms that the computer is not being prevented from accessing the network by problems with TCP/IP configuration or network hardware. If this test fails, you should check that the computer has a correct IP address and subnet mask, and that the computer’s physical connection to the network is intact.

4. Ping the DNS name of another computer on the same LAN.

   If this test fails, and you are able to successfully ping the IP address of the same computer, there is a name resolution problem. Check the computer’s DNS server address and that the DNS server is functioning properly.

5. Ping the computer’s designated default gateway address.

   Successfully pinging the default gateway does not confirm that the gateway is routing packets as it should, but it does verify that gateway system is up and running, and that its TCP/IP client is properly configured. If this test fails (after you have successfully completed all the previous tests), you should examine the router functioning as the default gateway for TCP/IP configuration or network hardware problems.

6. Ping several computers on another network that are accessible through the default gateway.

   If this test fails (and the previous test succeeded), then you know that although the default gateway is up and running, it might not be routing packets properly. A failure to ping a single computer on another network could indicate that the
destination system is not running, but if you cannot ping several systems on another network, it is likely that there is a routing problem.

**Tip** For best results, you should try to ping systems on a network to which the default gateway is directly connected. This way, you know that if the test fails, the default gateway is the problem. If the packets are passing through two or more routers to get to their destinations, any one of the routers could be at fault, and you must use another tool (such as Tracert.exe or Pathping.exe) to determine which router is malfunctioning.

**Using Tracert.exe**

Tracert.exe is the Windows operating system's implementation of the UNIX traceroute program. TRACERT enables you to view the path that packets take from a computer to a specific destination. When you type `tracert` and an IP address at the Windows command prompt, the program displays a list of the hops to the destination, including the IP address and DNS name (where available) of each router along the way, as follows:

```
Tracing route to www.adatum.co.uk [10.146.1.1]
over a maximum of 30 hops:
  1  <10 ms   <10 ms   192.168.2.99
  2   105 ms  92 ms    98 ms  qrvl-67terminal01.epoch.net [172.24.67.3]
  3   101 ms  110 ms   98 ms  qrvl.epoch.net [172.24.67.1]
  4   123 ms  109 ms  118 ms  svcr03-7b.epoch.net [172.24.103.125]
  5   123 ms  112 ms  114 ms  clsm02-2.epoch.net [172.24.88.26]
  6   136 ms  130 ms  133 ms  s1-0-T3.sprintlink.net [10.228.116.5]
  7   143 ms  126 ms  138 ms  s1-3.sprintlink.net [192.168.5.117]
  8   146 ms  129 ms  133 ms  s1-12-0.sprintlink.net [192.168.5.1]
  9   131 ms  128 ms  139 ms  s1-13-0.sprintlink.net [192.168.18.38]
 10   130 ms  134 ms  134 ms  s1-8-0.sprintlink.net [192.168.7.94]
 11   147 ms  149 ms  152 ms  s1-0.sprintlink.net [192.168.173.10]
 12   154 ms  146 ms  145 ms  ny2-ge021.router.demon.net [172.21.173.121]
 13   230 ms  225 ms  226 ms  tele-ge023.router.demon.net [172.21.173.12]
 14   233 ms  228 ms  226 ms  tele-fxp1.router.demon.net [10.159.252.56]
 15   223 ms  224 ms  224 ms  tele-14.router.demon.net [10.159.254.245]
 16   236 ms  221 ms  226 ms  tele-165.router.demon.net [10.159.36.149]
 17   220 ms  224 ms  210 ms  www.adatum.co.uk [10.146.1.1]
Trace complete.
```

Tracert.exe is an excellent tool for locating a malfunctioning router, because it is able to inform you how far packets have gotten on the way to their destination. When one of the routers on the path is not forwarding packets properly, the TRACERT output stops at the last functioning router. You know then that the next router on the path is the one experiencing the problem.
How Tracert.exe Works

Tracert.exe works by sending ICMP Echo Request messages to the destination, much as PING does, but with a special difference. For the first group of three Echo Request messages, TRACERT assigns a value of 1 to the IP header’s Time to Live (TTL) field. The TTL field is a safety measure designed to prevent packets from circulating endlessly around an internetwork. Normally, computers running Windows operating systems assign a value of 128 to the TTL field. When a router processes a packet, it reduces the TTL value by 1; if the TTL value reaches 0, the router discards the packet and returns an error message to the system that transmitted it.

Because the first three TRACERT packets have a TTL value of 1, when they reach the first router on their path, the router reduces their TTL values to 0 and discards them, sending error messages back to the sender. Then, for each successive group of three Echo Request messages, TRACERT increments the initial TTL value by 1, causing each group of packets to travel one more hop on the way to the destination before the router discards them. The TRACERT program uses the error messages generated by the routers (which contain the routers’ IP addresses) to create the output display.

Tip

It is important to understand that routes through a large internetwork can change frequently, for a variety of reasons, and packets can take different paths to the same destination. Therefore, when you use TRACERT, it is possible (although not probable) for the path through the internetwork taken by successive sets of Echo Request messages to be different. When you are using TRACERT to locate a malfunctioning router, you should run the program at least twice, using the same destination, to ensure that you are seeing an accurate path through the network.

Using Pathping.exe

Pathping.exe is another tool available from the Windows command prompt that is similar to Tracert.exe in that it traces a path through the network to a particular destination and displays the names and addresses of the routers along the path. PATHPING is different, however, because it reports packet loss rates at each of the routers on the path. TRACERT is the preferred tool for locating a router failure that completely interrupts communications, while PATHPING is more useful when you can connect to a destination, but you are experiencing data loss or transmission delays.

After displaying the path to the destination, PATHPING sends 100 packets (by default) to each of the routers on the path and computes the packet loss rate in the form of a percentage. A typical PATHPING output display appears as follows:
Troubleshooting the Routing and Remote Access Configuration

The most common symptom of trouble for an RRAS router is simply that the server is not routing traffic. However, although the symptom might be simple, the cause might not be. To begin troubleshooting, it is best to start with the most obvious possible causes, such as the following:

- **Verify that the Routing and Remote Access service is running**  Display the Services tool on the Administrative Tools menu to verify that the status of the Routing and Remote Access service is Started. In most cases, you should set the Startup Type selector to Automatic. If the service had been running and has now stopped for no apparent reason, check the Event Viewer console for error messages related to the stoppage.

- **Verify that routing is enabled**  In the Routing And Remote Access console, display the Properties dialog box for your server and, in the General tab, make sure that the Router check box and the appropriate routing option for your network (Local Area Network (LAN) Routing Only or LAN And Demand-Dial Routing) are selected. If your router is also functioning as a remote access server, you should select that check box as well. If RRAS is not configured with the correct options, you should check the other configuration parameters or disable the Routing and Remote Access service completely and reconfigure it from scratch.

- **Check the TCP/IP configuration settings**  Just like any other TCP/IP computer, a router must have the proper TCP/IP configuration settings in order to function properly. Make sure that you’ve configured all the router’s interfaces with the correct IP addresses, subnet masks, and other settings.

- **Check the IP addresses of the router interfaces**  When you use the Routing And Remote Access Server Setup Wizard to configure RRAS to function as a router, the wizard creates interfaces in the router configuration using the computer’s current interface settings. If you change the interface settings, such as the IP address...
Chapter 5 Using Routing and Remote Access

or subnet mask, you must change the corresponding setting in the RRAS interface as well. In the Routing And Remote Services console, display the Properties dialog boxes for the interfaces listed in the IP Routing’s General subheading and check to see that their IP addresses and subnet masks match the actual interface addresses, and that the interfaces show Operational status.

Troubleshooting the Routing Table

If you have configured RRAS correctly, and you are still experiencing routing problems, another cause could be that the routing table does not contain the information needed to route network traffic properly. The cause of this problem depends largely on whether you use static routing or dynamic routing. If you use static routing, someone might have deleted, omitted, or mistyped important routing table entries. If you use dynamic routing, your routing protocol might not be functioning properly.

Troubleshooting Static Routing

Because static routing requires human beings to create all the specialized entries in a routing table, the only possible source of problems in the routing table (excluding hardware failures) is human error. If you have created your static routes in the Routing And Remote Access console, you can view and modify them there by selecting the IP Routing’s Static Routes subheading in the console tree (see Figure 5-11). Note, however, that doing this displays only the static routes you have created in the Routing And Remote Access console.

Important If someone has created static routes using the Route.exe command line utility, these routes do not appear in the Routing And Remote Access console’s Static Routes display, nor do the default entries in the routing table appear. The only way to modify or delete routing table entries created with Route.exe is to use Route.exe.

![Figure 5-11 The Static Routes display in the Routing And Remote Access console](image)

To display the entire routing table for the computer using the Routing And Remote Access console, click the Static Routes subheading and, on the Action menu, click
Show IP Routing Table to produce a display like the one in Figure 5-12. You cannot modify the routing table in this display, however, just view it.

<table>
<thead>
<tr>
<th>Destination</th>
<th>Network mask</th>
<th>Gateway</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>192.168.2.59</td>
<td>3COM</td>
</tr>
<tr>
<td>127.0.0.0</td>
<td>255.0.0.0</td>
<td>127.0.0.1</td>
<td>Loopback</td>
</tr>
<tr>
<td>127.0.0.1</td>
<td>255.255.0.0</td>
<td>127.0.0.1</td>
<td>Loopback</td>
</tr>
<tr>
<td>192.168.2.0</td>
<td>255.255.255.0</td>
<td>192.168.2.3</td>
<td>3COM</td>
</tr>
<tr>
<td>192.168.2.1</td>
<td>255.255.255.0</td>
<td>192.168.2.3</td>
<td>3COM</td>
</tr>
<tr>
<td>192.168.2.2</td>
<td>255.255.255.0</td>
<td>192.168.2.3</td>
<td>3COM</td>
</tr>
<tr>
<td>192.168.2.3</td>
<td>255.255.255.0</td>
<td>192.168.2.3</td>
<td>3COM</td>
</tr>
<tr>
<td>192.168.3.0</td>
<td>255.255.255.0</td>
<td>192.168.3.3</td>
<td>NEC2000</td>
</tr>
<tr>
<td>192.168.3.1</td>
<td>255.255.255.0</td>
<td>192.168.3.3</td>
<td>NEC2000</td>
</tr>
<tr>
<td>192.168.3.2</td>
<td>255.255.255.0</td>
<td>192.168.3.3</td>
<td>NEC2000</td>
</tr>
<tr>
<td>192.168.3.3</td>
<td>255.255.255.0</td>
<td>192.168.3.3</td>
<td>NEC2000</td>
</tr>
<tr>
<td>192.168.3.4</td>
<td>255.255.255.0</td>
<td>192.168.3.3</td>
<td>NEC2000</td>
</tr>
<tr>
<td>192.168.4.0</td>
<td>255.255.255.0</td>
<td>192.168.3.3</td>
<td>NEC2000</td>
</tr>
<tr>
<td>192.168.4.1</td>
<td>255.255.255.0</td>
<td>192.168.3.3</td>
<td>NEC2000</td>
</tr>
<tr>
<td>224.0.0.0</td>
<td>240.0.0.0</td>
<td>192.168.2.3</td>
<td>3COM</td>
</tr>
<tr>
<td>224.0.0.1</td>
<td>240.0.0.0</td>
<td>192.168.2.3</td>
<td>3COM</td>
</tr>
<tr>
<td>255.255.255.0</td>
<td>255.255.255.0</td>
<td>192.168.2.3</td>
<td>NEC2000</td>
</tr>
<tr>
<td>255.255.255.0</td>
<td>255.255.255.0</td>
<td>192.168.2.3</td>
<td>NEC2000</td>
</tr>
</tbody>
</table>

Figure 5-12 The RRAS IP Routing Table window

The Route.exe command-line utility enables you to view, add, modify, or delete any entries in the computer’s routing table, regardless of how you created them.

Tip Although it might take you a bit of time to get used to its command line syntax, Route.exe is a much better tool for creating static routes than the Routing And Remote Access console. For example, if you try to create a routing table entry with a gateway address that does not exist on one of the router’s connected networks, Route.exe refuses to create the entry and displays an error message. The Static Route dialog box in the Routing And Remote Access console allows you to create this incorrect table entry without complaining.

Troubleshooting Routing Protocols

If you use dynamic routing, the lack of the proper entries in a router’s routing table is the result of the routing protocol failing to put them there. Assuming that no network communications problem is preventing the routers from exchanging messages, it is likely that the routing protocol on one or more of the routers is not configured properly. To verify the functionality of the routing protocol, use the following procedures:

1. Verify that the routing protocol is installed on all the participating routers.

On an RRAS router, you must install the routing protocol manually after you configure the Routing and Remote Access service. Other operating systems and stand-alone routers might have their own procedures for installing or enabling the routing protocol. Make sure that all the routers on the network are configured to use the same routing protocol, and that the protocol implementations are compatible.
2. Verify that the routing protocol is configured to use the correct interfaces.

After you install RIP or OSPF on an RRAS router, you must specify the interfaces over which you want the protocol to transmit its messages. To do this, you click the routing protocol icon in the console tree and, on the Action menu, click New Interface. In the New Interface dialog box, you select the interface in the computer that provides access to the network where the other routers are located. If other routers are located on both networks to which the Routing and Remote Access server is connected, you should perform this procedure twice, to install both interfaces.

After you have ascertained that RRAS has the routing protocol installed and the interfaces selected, you can begin checking elements specific to the individual routing protocol, as described in the following sections.

**Troubleshooting RIP**

To determine whether RIP is functioning properly, you can select the RIP subheading in the console tree, as shown in Figure 5-13.

![Figure 5-13](image)

The RIP display in the Routing And Remote Access console

The details pane shows the number of RIP packets transmitted and received by the router. If RRAS is not sending or receiving RIP messages (or both), you should check the RIP configuration settings, as described in the following procedures:

1. Verify that all the RIP routers are using the same message types.

   The RIP implementation in Windows Server 2003 supports version 2 of the protocol, but you can configure RIP on each interface to transmit its messages as either version 1 or version 2 broadcasts, or version 2 multicasts. By default, RRAS uses RIP version 2, but you may have to modify these settings so that the router functions with other RIP implementations on your network. Be sure to check every RIP router on your network to see which version of the protocol it uses, and then modify your RRAS configuration accordingly.
Lesson 4  Troubleshooting TCP/IP Routing

When configuring the RIP version properties, remember that you must configure ingoing traffic, outgoing traffic, and each interface separately.

2. Check RIP security properties.

In the Security tab in each RIP interface’s Properties dialog box, you can specify the address ranges of routes that you want RIP to accept from other routers. By default, RRAS RIP accepts all incoming routes, but if new entries are not appearing in the computer’s routing table, check to make sure that no one has changed the security settings inappropriately.

3. Check the RIP timing interval settings.

By default, the RRAS RIP implementation transmits update messages every 30 seconds, and RRAS removes RIP entries from the routing table if they are not refreshed at least every 20 minutes (1200 seconds). If you decide to modify these defaults (as a bandwidth conservation measure), make sure that the Periodic Announcement Interval value is lower than the Time Before Route Is Removed setting. Otherwise, RRAS will remove entries from the table before they have a chance to be refreshed.

If you change the RIP timing interval settings on one router, you should change them on all the other RIP routers in the same way.

Troubleshooting OSPF

As with RIP, when you click the OSPF subheading in the Routing And Remote Access console tree, the details pane shows the number of OSPF packets the router has sent and received, so you can tell if the protocol is functioning. If the router is not sending or receiving OSPF packets, the first thing to check is whether OSPF is enabled on each of the interfaces you installed. Display the Properties dialog box for each interface and check to see that the Enable OSPF For This Address option button is selected.

If OSPF is enabled on the interfaces and your routers are still not communicating, it is time to check whether each router is configured in accordance with your OSPF deployment plan. Unlike RIP, which requires little or no configuration, an OSPF deployment requires you to make decisions such as how many areas you want to create, and which routers will handle the communication between areas by functioning as area border routers. Make sure that you have configured each OSPF router on the network to perform its designated roles.
Lesson Review

The following questions are intended to reinforce key information presented in this lesson. If you are unable to answer a question, review the lesson materials and try the question again. You can find answers to the questions in the “Questions and Answers” section at the end of this chapter.

1. Which of the following TCP/IP tools is best suited to troubleshooting a situation in which a router is dropping packets?
   a. Ping.exe
   b. Tracert.exe
   c. Pathping.exe
   d. Route.exe

2. What would happen if a router on your network supported only RIP version 1, and all your other routers were Routing and Remote Access servers using RIP with its default configuration?

3. If you use static routing on your network, and several administrators are responsible for creating the routing table entries on your routers, what should you do if you open the Routing And Remote Access console on one of your routers, click the Static Routes subheading, and see no entries?

Lesson Summary

- Tracert.exe is a command line tool that can help you locate a non-functioning router on the network. TRACERT uses ICMP Echo Request messages with incrementing TTL values to test the connection to each router on the path to a given destination.

- Pathping.exe is a command line tool that sends large numbers of test messages to each router on the path to a particular destination and compiles statistics regarding dropped packets. Pathping.exe is best suited to locating a router that is malfunctioning but still operational.

- When a routing table lacks the proper entries, the cause depends on whether you use static or dynamic routing on the network.
For an RRAS router to use either RIP or OSPF, you must install the routing protocol and then select the interfaces over which the protocol will transmit messages.

Incorrect routing protocol configurations can prevent the routers on the network from sharing their routing table entries, which in turn prevents the routers from forwarding traffic properly.

Case Scenario Exercise

You are the network infrastructure design specialist for Litware Inc., a manufacturer of specialized scientific software products, and you have already created a network design for their new office building, as described in the Case Scenario Exercise in Chapter 1. The office building is a three-story brick structure built in the late 1940s, which has since been retrofitted with several types of network cabling by various tenants. Your network design for the building calls for the installation of four LANs, each of which is connected to a fifth, backbone network. The backbone is connected to the company’s home office using a T-1 leased line, and a second T-1 connects the backbone to an ISP’s network, for Internet access.

To connect the building's internetwork to the company's home office and to the ISP, you must install two routers, and you have decided to use computers running Windows Server 2003 and the Routing and Remote Access service. The first computer running Windows Server 2003 is called Router01 and two network interface adapters are installed in it. In the Network Connections tool, the adapter connecting the computer to the local network is called LAN Connection and the adapter connected to the T-1 providing access to the home office network is called WAN Connection. The second computer, Router02, also has two network interface adapters, named LAN Connection and ISP Connection, respectively.

The Litware home office network and all the company’s other branch offices use RIP, and you have already configured the routers connecting the building’s LANs to use RIP.

Based on this information, answer the following questions:

1. When you are running the Routing And Remote Access Server Setup Wizard on Router2, which option should you select in the Configuration page?
   a. Network Address Translation (NAT)
   b. Remote Access (Dial-Up Or VPN)
   c. Secure Connection Between Two Private Networks
   d. Virtual Private Network (VPN) Access And NAT
2. When configuring RIP on Router01, which interfaces should you install?
   a. None
   b. LAN Connection only
   c. WAN Connection only
   d. Both LAN Connection and WAN Connection

3. On which of the two routers must you install RIP? Explain why.

4. Which of the following methods can you use to reduce the amount of RIP traffic passing over the T-1 link to the home office?
   a. Set the Outgoing Packet Protocol setting to RIP Version 1 Broadcast
   b. Increase the Periodic Announcement Interval setting
   c. Set the Incoming Packet Protocol setting to RIP Version 1 Only
   d. Decrease the time Before Route Is Removed setting

5. On which of the RRAS configurations should you enable demand-dial routing?
   a. Neither
   b. Router01 only
   c. Router02 Only
   d. Both

Troubleshooting Lab

For each of the following scenarios, specify which of the following tools you would use to troubleshoot the problem: Ping.exe, Tracert.exe, Route.exe, or Pathping.exe.

1. A router on a private internetwork is forwarding traffic to some destination networks properly, but is failing to forward traffic to others. Which tool do you use to repair the problem?
2. On a large corporate internetwork, packets originating on one LAN are not reaching destination systems on another LAN, and both the source and destination computers are functioning properly on their local networks. How do you determine which router on the network is not forwarding packets properly?

3. Traffic levels on your company network have risen precipitously, and you have determined that this is due to a dramatic increase in packet retransmissions. You suspect that one of the routers on the network is dropping packets. How do you determine which one?

Chapter Summary

- A WAN topology is the pattern of connections among your network’s sites. When selecting a topology, be sure to consider the characteristics of the WAN technology you plan to use.
- Dial-up services, frame relay, and VPNs all make it possible to create a mesh topology without having to install a separate WAN link for every pair of sites.
- Static routing is the manual creation of routing table entries, and can require extensive maintenance. It is not practical for large networks with frequent infrastructure changes.
- Dynamic routing uses a specialized routing protocol, such as RIP or OSPF, that enables the routers to exchange messages containing information about their networks.
- RIP is a distance vector routing protocol that is suitable for smaller networks running at a single speed, but it generates a lot of broadcast traffic. OSPF is a link state routing protocol that is scaleable to support networks of almost any size, but requires more planning, configuration, and maintenance than RIP.
- To support IP multicasting, a router must support IGMP and have network interface adapters that support multicast promiscuous mode.
- RRAS supports multiple authentication protocols, including EAP, MS-CHAP (versions 1 and 2), CHAP, SPAP, and PAP. You should configure RRAS to use the strongest protocol that your clients and servers have in common.
Remote access policies are sets of conditions that remote clients attempting to connect to the Routing and Remote Access server must meet. You can use policies to control remote access based on group membership and other criteria.

Tracert.exe is a command line tool that can help you locate a non-functioning router. TRACERT uses ICMP Echo Request messages with incrementing TTL values to test the connection to each router on the path to a given destination.

Pathping.exe is a command line tool that sends large numbers of test messages to each router on the path to a particular destination and compiles statistics regarding dropped packets. Pathping.exe is best suited for locating a router that is malfunctioning but still operational.

Exam Highlights

Before taking the exam, review the key points and terms that are presented below to help you identify topics you need to review. Return to the lessons for additional practice, and review the “Further Reading” sections in Part 2 for pointers to more information about topics covering the exam objectives.

Key Points

- A distance vector routing protocol like RIP is the preferred routing protocol for an internetwork with LANs that all run at the same speed, because the number of hops is a viable measure of a route’s efficiency.

- Link state routing protocols like OSPF are preferable on internetworks with links running at different speeds, such as remote offices connects by WAN links, because their metrics use a more realistic measurement of a route’s efficiency.

- To route IP multicast traffic, you must install IGMP on your routers, so that client computers on the networks can register their memberships in a host group.

- Windows Server 2003 includes a variety of security measures to protect remote access servers against unauthorized access, including multiple authentication protocols and encryption algorithms.

- Tracert.exe is the best tool for locating a non-functioning router, while Pathping.exe is better for locating a router that is dropping some packets.
Key Terms

**Distance vector routing** A dynamic routing method that rates the relative efficiency of specific routes through the network by counting the number of hops between the source and the destination.

**Link state routing** A dynamic routing method that rates the relative efficiency of specific routes through the network using link speed, network congestion delays, and a route cost value assigned by an administrator, in addition to the number of hops.

**Authentication** The process of confirming the identity of a connecting user.

**Authorization** The process of determining whether the server should permit the connection to proceed.
Lesson 1 Review

1. Which of the following WAN technologies would be practical to use to create a mesh remote networking topology? (Choose all answers that apply.)
   - a. ISDN
   - b. Dial-up modems
   - c. T-1
   - d. Frame relay
   - e. VPNs
   a, d, and e

2. What term do frame relay providers use to describe the network to which they connect their subscribers’ leased lines?
   A cloud

3. In which of the following WAN topologies can a single cable break totally disconnect one site from the other sites?
   - a. Mesh
   - b. Ring
   - c. Star
   - d. None of the above
   c

Lesson 2 Review

1. To support IP multicasting, which of the following components must be installed on a Windows Server 2003 router? (Choose all correct answers.)
   - a. The Protocol Independent Multicast (PIM) protocol
   - b. A network interface adapter that supports multicast promiscuous mode
   - c. The Routing And Remote Access MMC snap-in
   - d. Internet Group Management Protocol
   b, c, and d
2. Specify whether each of the following characteristics describes distance vector routing, link state routing, or both.

   a. Used by OSPF
      Link state routing
   b. Uses the number of hops to the destination when calculating metrics
      Both
   c. Uses link speed when calculating metrics
      Link state routing
   d. Used by RIP
      Distance vector routing
   e. Unsuitable for enterprises with networks running at various speeds
      Distance vector routing

Lesson 3 Review

1. Which of the following authentication protocols do you use with smart cards?

   a. MS-CHAP v2
   b. EAP-TLS
   c. PEAP
   d. PAP

b

2. What is the function of a RADIUS server in a remote access installation?

   RADIUS is a service that can provide authentication, authorization, and accounting services for multiple remote access servers.

3. How does the callback option in a user account’s dial-in properties function as a security feature?

   The callback feature can provide additional security when an administrator specifies the telephone number that the Routing and Remote Access server will use to call the user back during the connection process.

4. Which of the following is not a component of a remote access policy?

   a. Authentication protocol
   b. Conditions
   c. Remote access profile
   d. Remote access permission

a
Lesson 4 Review

1. Which of the following TCP/IP tools is best suited to troubleshooting a situation in which a router is dropping packets?
   a. Ping.exe
   b. Tracert.exe
   c. Pathping.exe
   d. Route.exe

2. What would happen if a router on your network supported only RIP version 1, and all your other routers were Routing and Remote Access servers using RIP with its default configuration?

   The RIP version 1 router would not be able to process the incoming packets from the RRAS routers, because they use RIP version 2 messages by default.

3. If you use static routing on your network, and several administrators are responsible for creating the routing table entries on your routers, what should you do if you open the Routing And Remote Access console on one of your routers, click the Static Routes subheading, and see no entries?

   You should use Route.exe to view the computer's routing table, because static routes not created in the Routing And Remote Access console do not appear in the Static Routes display.

Case Scenario Exercise

Based on the information provided in the Case Scenario Exercise, answer the following questions:

1. When you are running the Routing And Remote Access Server Setup Wizard on Router2, which option should you select in the Configuration page?
   a. Network Address Translation (NAT)
   b. Remote Access (Dial-Up Or VPN)
   c. Secure Connection Between Two Private Networks
   d. Virtual Private Network (VPN) Access And NAT

   a
2. When configuring RIP on Router01, which interfaces should you install?
   a. None
   b. LAN Connection only
   c. WAN Connection only
   d. Both LAN Connection and WAN Connection

3. On which of the two routers must you install RIP? Explain why.
   You only have to install RIP on Router01 because this is the router connecting the building network to the home office. Router02 does not need RIP because it only routes traffic to the Internet.

4. Which of the following methods can you use to reduce the amount of RIP traffic passing over the T-1 link to the home office?
   a. Set the Outgoing Packet Protocol setting to RIP Version 1 Broadcast
   b. Increase the Periodic Announcement Interval setting
   c. Set the Incoming Packet Protocol setting to RIP Version 1 Only
   d. Decrease the time Before Route Is Removed setting

5. On which of the RRAS configurations should you enable demand-dial routing?
   a. Neither
   b. Router01 only
   c. Router02 Only
   d. Both

Troubleshooting Lab

For each of the following scenarios, specify which of the following tools you would use to troubleshoot the problem: Ping.exe, Tracert.exe, Route.exe, or Pathping.exe.

1. A router on a private internetwork is forwarding traffic to some destination networks properly, but is failing to forward traffic to others. Which tool do you use to repair the problem?
   Route.exe
2. On a large corporate internetwork, packets originating on one LAN are not reaching destination systems on another LAN, and both the source and destination computers are functioning properly on their local networks. How do you determine which router on the network is not forwarding packets properly?

Tracert.exe

3. Traffic levels on your company network have risen precipitously, and you have determined that this is due to a dramatic increase in packet retransmissions. You suspect that one of the routers on the network is dropping packets. How do you determine which one?

Pathping.exe