Microsoft®

Windows NT® Server

Server Operating System

Routing and Remote Access Service for Windows NT Server: *New Opportunities Today and Looking Ahead*

Abstract

Microsoft® Routing and Remote Access Service (RRAS), formerly known by its code name "Steelhead," provides independent software vendors (ISVs), independent hardware vendors (IHVs), system integrators, value-added resellers, and network managers with significant opportunities for deploying effective and affordable internetworking solutions. Routing and Remote Access Service is already available to Windows NT® Server 4.0 operating system customers at no additional charge as a released-to-Web product. Looking ahead, an enhanced version of RRAS will be released as part of Windows NT Server 5.0. Routing and Remote Access Service is especially valuable for branch office deployments, as well as for use in edge routing where a corporate network connects to the Internet or other wide area network (WAN). By unifying routing and remote access service, internetworking deployments are easy to use, flexible, and affordable. Because the service is part of the extensible and open platform of Windows NT Server, there are great opportunities for third-parties to create value-added internetworking solutions. This paper highlights the key features in RRAS today and outlines enhancements planned for the Windows NT Server 5.0 time frame.

Microsoft Corporation • One Microsoft Way • Redmond, WA 98052-6399 • USA

0997

CONTENTS

INTRODUCTION

Microsoft® Routing and Remote Access Service (RRAS) creates a broad range of new opportunities for independent software vendors (ISVs), independent hardware vendors (IHVs), system integrators, value-added resellers (VARs), and network managers involved in creating internetworking solutions, especially for branch office and edge-of-network deployments.

The Windows NT® Server operating system version 4.0 includes “in the box” two important services – Remote Access Service (RAS) and Multi-Protocol Routing. In the Spring of 1997, Microsoft released to Web an enhancement to these services by creating a unified Routing and Remote Access Service (RRAS).This new service, formerly known by its code name “Steelhead,” is now available as a free released-to-Web offering for Windows NT Server 4.0. Looking ahead, Microsoft also plans to include an enhanced version of Routing and Remote Access Service as part of Windows NT Server 5.0.

This is significant for a variety of third-party organizations. These organizations can immediately begin developing and offering solutions for the Windows NT Server 4.0 platform with the new Routing and Remote Access Service, knowing that their products also will be ready for Windows NT Server version 5.0, as well.

The Windows® operating system is emerging as the communications platform of choice, due to the extensive network communications support included across the entire operating system family. Microsoft is making several enhancements to this built-in communications support with Windows NT Server 5.0, including quality of service support, ATM support, and unified Internet and traditional telephony support. Many of these enhancements are outside the scope of this paper and are covered by other materials. Here is a brief list of some of the communications enhancements planned for Windows NT 5.0 that relate to RRAS.

- **Extensible Authentication Protocol (EAP)**,which allows third-party authentication modules, such as secure ID cards, to plug into the Microsoft Windows NT RRAS PPP implementation.
- **Bandwidth Allocation Protocol,** which dynamically adds or drops multi-link connections according to administrator-set load parameters.
- **RRAS User Profiles Support,** which simplifies remote access management by allowing network managers to create group profiles (such as a Marketing Profile, or Maintenance Profile) to set remote access dial-up rights and use parameters.

RRAS arrives at a time in which there is a broad movement toward the Internet Protocol (IP) networking standard, a huge growth in corporate intranets, and a booming demand for the routing, remote access, virtual private networks (VPN) and other internetworking solutions needed to tie everything together.

Flexibility for network managers and opportunities for third-party developers are greatly enhanced by the openness and extensibility of the Windows NT Server platform and its Routing and Remote Access Service. This openness is epitomized by the Network Driver Interface Specification (NDIS), which provides a standard

layer to which all local area network (LAN) and WAN cards can be built to support Windows NT. This allows network managers and system integrators to choose from an array of IHVs providing NDIS-based network cards. Application programming interfaces (APIs) provide great extensibility to allow third-party developers to create custom routing or network management solutions.

Additional third-party value-add opportunities are found in the integration of Routing and Remote Access Service with the Windows NT Server platform. System integrators, VARs, and network managers can provide complete single-box, turn-key solutions for branch office, small business, and edge routing deployments. The same Windows NT Server-based computer that hosts routing, RAS, and VPNs, can also host integrated communications applications or productivity applications such as the Microsoft BackOffice® family and Microsoft Internet Information Server.

Routing and Remote Access Service offers:

- A full complement of protocols for IP and IPX routing (including OSPF and RIP v2 for IP).
- An intuitive graphical user interface and command line interface with scripting capabilities – both of which can be used via a remote PC for centralized management.
- Packet filtering and additional security features.
- An extensible platform with APIs for additional third-party routing protocols, user interface (UI), and management.
- Demand-dial routing support.
- Secure virtual private networking with Point-to-Point Tunneling Protocol (PPTP) support server-to-server.
- RADIUS client support.

RRAS for Windows NT Server works with an organization’s existing router hardware, to fit into an existing network.

All of this is good news for IT managers and network administrators who will benefit from the increased choice and affordability they will have in building and managing their internetworking infrastructures.

CREATING SOLUTIONS WITH ROUTING AND REMOTE ACCESS SERVICE

The widespread migration toward the Internet Protocol creates a golden age for ISVs, IHVs, system integrators, network consultants, and Net managers who are creating and implementing IP-based internetworking solutions.
Organizations around the world are redesigning their networks to be more Internet-centric. Windows NT Server 5.0 with its Routing and Remote Access Service is the ideal platform for hosting internetworking solutions.

The same Windows NT Server-based system that is placed in a branch office for applications, such as the Microsoft BackOffice family, can also host virtual private networks with Point-to-Point Tunneling Protocol (PPTP)-based connections, enabled by RRAS. The built-in routing capabilities interface with a broad array of industry standard network interface cards (NICs) and routing gear. And the IP and IPX packet filtering, especially when combined with Microsoft Proxy Server 2.0, provides great firewall protection. Of course third-party firewalls and management programs can also be deployed because of the open nature of the Windows NT Server and RRAS platform.

A Rich Set of APIs and a Software Development Kit

To enable third-party value-added development, RRAS supports a set of APIs, exposed and documented in an associated Software Development Kit (SDK), which makes the service an extensible platform. The APIs allow routing protocols to be added, the user interface to be completely customizable, and the manageability to be directed by a variety of third-party hardware and software companies and system integrators.

Using RRAS to Create Great Products

The powerful combination of Windows NT Server and Routing and Remote Access Service creates a wealth of opportunities for a broad range of third-party vendors, including:

- Server OEM Vendors
- ISVs writing routing protocols
- ISVs writing monitoring and management programs
- IHVs providing WAN and LAN cards
- Internet Service Providers (ISPs)
- System Integrators and Network Consultants

Server OEM Vendors

Hardware vendors can package network access solutions using RRAS and Windows NT Server. Because Windows NT Server is a true network operating system, hardware vendors can provide full functional internetworking products on the platform. This is a great example of applying the PC industry business model to the internetworking business.

ISVs Writing Routing Protocols

Many legacy installations will still need implementations of unique protocols running

on standard PC hardware. In addition, the set of routing and internetworking protocols continues to evolve. These specialized routing protocols can be built on or ported to the routing APIs of Routing and Remote Access Service. This is expected to create opportunities for software vendors to sell these protocols to customers through system integrators or via OEMs.

ISVs Writing Monitoring and Management Programs

Independent software vendors can use the extensive set of APIs to create custom monitoring, management, auditing, and accounting packages. Routing and Remote Access Service also supports a standard set of management information bases (MIBs). Microsoft provides a set of management tools with the service, but there are great opportunities for ISVs to build upon this foundation to create their own packages to meet specialized, and general, business needs.

IHVs Providing WAN and LAN Cards

Network interface card (NIC) vendors can benefit from Routing and Remote Access Service by participating in the rapidly growing routing and internetworking market. Single-port LAN or WAN cards that support Windows NT Server can be used to support routing and internetworking. In addition, multi-port LAN and WAN cards can also be used with the service.

Internet Service Providers

Internet service providers (ISPs) can either sell or lease to their customers complete turn-key packages for remote client or branch office networking. Various estimates indicate that about 25% of all routers are sold to customers by ISPs in conjunction with the deployment of Internet access. ISPs can also offer out-sourced service functions such as using the Internet as a Virtual Private Network (VPN). Internet VPNs offer some compelling pricing and flexibility advantages over traditional long distance or leased line arrangements. In addition, Internet VPNs represent another way for an ISP to add value and differentiate its offerings.

System Integrators and Network Consultants

System integrators and network consultants, like OEMs, can assemble edge routing, remote access, VPN and other internetworking solutions based on RRAS and Microsoft Windows NT Server. This is the ideal platform for delivering turnkey, best-of-breed, customized solutions for customers.

PROVIDING A POWERFUL INTERNETWORKING PLATFORM TODAY

Windows NT Server is a great networking and communications platform and Routing and Remote Access Service provides some very compelling elements of this platform. RRAS includes a powerful set of routing protocols and other features including:

- RIP version 2 (and version 1) for IP
- OSPF
- DHCP Relay Agent for IP
- RIP and SAP for IPX
- Static routing
- Routing APIs
- Compatibility with Industry Standard LAN and WAN Cards

RIP version 2 (and version 1) for IP

Routing Information Protocol, the frequently used routing protocol for small to mid-sized networks, is relatively easy to use and provides very good performance. RRAS supports both version 1 and version 2 of RIP.

A RIP router maintains a routing table and periodically sends announcements to inform other RIP routers on the network of the networks it can reach. RIP also announces when it can no longer reach networks. RIP version 1 uses IP *broadcast* packets for its announcements. A later enhancement, RIP version 2, uses IP *multicast* packets for its announcements.

Each entry in a RIP routing table provides information about the entry, including the ultimate destination address, the next hop on the way to the destination, and a metric which indicates the distance in number of hops to the destination, its "cost" to the router. Other information can also be present in the routing table, including various timers associated with the route.

Initially, each router's table includes only the links to which it is physically connected. A router depends on periodic updates from other routers to keep current information on what routes are reachable through them. RIP maintains only the best route to a destination through broadcast messages at 30-second intervals, or *triggered updates*. Triggered updates occur when the network topology changes and routing update messages are sent which reflect those changes. For example, when a router detects a link failure or a router failure, it recalculates its routes and sends routing update messages (triggered updates). Each router receiving a routing update message that includes a change updates its tables and propagates the change.

The biggest advantage of RIP is that it is extremely simple to configure and deploy. The biggest disadvantage of RIP is that as networks grow larger in size, the periodic announcements by each RIP router cause excessive traffic on the network. RIP is widely deployed in networks with up to 50 servers or so, but most larger organizations use other routing protocols.

OSPF

Open Shortest Path First is an Internet Engineering Task Force (IETF) standard link-state routing protocol used for routing IP. OSPF is a more sophisticated routing protocol than RIP, offering faster routing algorithm convergence. The service's OSPF implementation is a result of collaborative effort between Microsoft and Bay Networks, a leading provider of internetworking systems.

Developed in response to the inability of RIP to serve large, heterogeneous internetworks, OSPF is a link-state protocol based on the Shortest Path First (SPF) algorithm. This algorithm computes the shortest path between one source node and the other nodes in the network. Various industry sources indicate that about 35% to 40% of the routed networks in place today make use of OSPF and this number is growing.

Instead of exchanging distances to destinations like RIP routers do, OSPF routers maintain a "map" of the network that is updated after any change in the network topology. This map, called the link-state database, is used to compute the network routes, which must be computed again after any change in the topology. From this computation, the router derives the next hop for the destination, that is, the next router to which the data should be sent and the link that should be used for reaching this next router. Network changes are propagated or *flooded* across the entire network to ensure that each copy of the database is accurate at all times.

Because OSPF routers keep an overview of the network from the perspective of any router, some of the problems that are inherent in RIP (such as loops) are eliminated.

The new service's router OSPF implementation supports the following features:

- Route filters for controlling interaction with other routing protocols
- Dynamic reconfiguration of all OSPF parameters
- Coexistence with RIP
- Dynamic addition and deletion of interfaces

DHCP Relay Agent for IP

Dynamic Host Configuration Protocol (DHCP) provides lower cost of ownership for IP networks because it dynamically assigns IP addresses to PCs or other resources connected to an IP network. This is a dramatic improvement in time and dollar savings compared to manually assigning useable IP addresses. Routing and Remote Access Service provides a relay agent function for DHCP servers so that DHCP assignments can be made across routed networks regardless of whether the connection is made via LAN or WAN links.

Additionally, Windows Internet Name Service provides a distributed, dynamically updated database of host names mapped to IP addresses. This allows users to use friendly host names instead of IP address to locate network resources. Microsoft Domain Naming System (DNS) server running under Windows NT Server 4.0 is a Request For Comment (RFC)-compliant DNS name server that is used to manage

and administer DNS services on a TCP/IP network. Microsoft DNS server supports RFC's 1033, 1034, 1035, 1101, 1123, 1183, and 1536 and is also compatible with the Berkeley Internet Name Domain (BIND) DNS implementation.

Integration of DNS and Windows Internet Name Service services is an important feature that allows inter-operability between non-Microsoft and Windows-based TCP/IP network clients. DNS and Windows Internet Name Service integration provides a method to reliably resolve name queries for Windows-based computers that use dynamic (DHCP-based) IP addressing and NetBIOS computer names. Windows NT Server 4.0 allows ease-of-administration with the graphical DNS Manager that allows one to manage local and remote Microsoft DNS servers and database files.

RIP and SAP for IPX

Routing Information Protocol and Service Advertising Protocol (SAP) are two routing protocols commonly used in Novell NetWare Internetwork Packet Exchange (IPX) small- to mid-size network environments. RRAS supports these routing protocols to enable interoperability in mixed network environments.

RIP for IPX is a simple broadcast protocol used to exchange IPX network routes across a network. This protocol announces routes over each network segment. It is configured periodically so that the routing information kept in the routers is current. Various industry sources indicate that about 15% of the routed networks in place today make use of RIP and SAP for IPX and this number is growing.

RRAS supports network route filters, which enable selective announcements and reception of network routes. RRAS also enables configuration of the timers used for route announcements (for example, the periodic announcement timer).

The Service Advertising Protocol allows nodes that provide services, such as file servers and print servers, to advertise their addresses and the services they provide.

IPX routers send periodic SAP broadcasts to keep all routers on the internetwork synchronized. By default, this is set to every 60 seconds. Routers also send SAP update broadcasts whenever they detect a change in the internetwork configuration.

The implementation of IPX by Windows NT Server (NWLink IPX/SPX Compatible Protocol [NWLink]) conforms to the Novell IPX Router Specification.

Static Routing

Routing and Remote Access Server continues to support use of static, or fixed, routing assignments.

Routing APIs

As noted earlier, Microsoft offers a Software Developer Kit (SDK) that describes for developers how to use RRAS APIs. This is a unique feature enabling Windows NT

Server with RRAS to be a platform for value-added development in routing and networking. It also provides customers great flexibility and investment protection.

Works with Industry Standard LAN and WAN Cards

Because RRAS runs on Windows NT Server 4.0, it can enable internetworking using any of the 2,000+ LAN and WAN cards that have earned the Windows NT Compatible logo. This provides great customer choice.

ENHANCING REMOTE ACCESS

Routing and Remote Access Server brings new enhancements to what was already a powerful remote access platform. New features such as Extensible Authentication Protocol, Bandwidth Allocation Protocol, and RRAS User Profiles bring new power and flexibility to the platform in the Windows NT 5.0 time frame. The remote access component of offers an array of connectivity options including analog, ISDN, frame relay, T1, X.25, and even the Internet. The RAS APIs make it easy for third-parties to create value-added solutions. Here is a brief summary of the remote access features included with RRAS:

- Auto-dial and Auto Logon Dial
- Demand Dial Routing
- Authentication with PAP, CHAP, and MS-CHAP
- Extensible Authentication Protocol (EAP) – new in Windows NT 5.0
- RAS User Profiles
- Encryption
- Point-to-Point Tunneling for Client-to-Server
- Point-to-Point Tunneling for Server-to-Server
- Restartable File Copy
- PPP Multi-Link
- Bandwidth Allocation Protocol (BAP) – new in Windows NT 5.0
- RAS Idle Disconnect

Auto-dial and Auto Logon Dial

The Windows operating system can map and maintain an association between a Dial-Up Networking entry and a network address to seamlessly integrate Dial-Up Networking with files and applications. This means if a user double-clicks on an icon to open a file that is only accessible over the dial-up connection, Dial-Up Networking will automatically initiate the call. This is a Windows NT 4.0 RAS feature that is retained in RRAS.

Demand Dial Routing

Routing and Remote Access Service supports on-demand dialing over any variety of WAN links, including via the Internet with Point-to-Point Tunneling, eliminating the need for continuous, “nailed-up” connections. As a result, demand dial provides significant cost-savings.

Since a PPTP or a Layer 2 Tunneling Protocol (L2TP) tunnel is just another connection, a Windows NT-based server can route packets over a demand-dial tunnel connection that it initiates as a client to a remote tunnel server. Once the connection is established, traffic from one network is routed over a tunnel connection through a tunnel server onto another network.

Authentication – PAP, CHAP, and MS-CHAP

Routing and Remote Access Service supports Password Authentication Protocol (PAP), Shiva-PAP, Challenge Handshake Authentication Protocol (CHAP), MS-

CHAP, as well as support for RADIUS authentication servers.

Extensible Authentication Protocol

The Extensible Authentication Protocol allows new authentication methods to be used with RAS, something that is especially important for the deployment of token card security mechanisms. EAP is the interface that allows third-party authentication modules to plug into the Microsoft Windows NT RAS PPP implementation. Microsoft is adding support for EAP to RRAS in the Windows NT 5.0 time frame.

EAP was proposed to the IETF as a PPP authentication protocol to allow for the authenticator to request more information about the peer before determining the specific authentication mechanism. This is accomplished by postponing this decision from the Link Control Protocol (LCP) phase to the Authentication phase.

RRAS User Profiles

Routing and Remote Access Service will work with the Windows NT Server 5.0 Active Directory to store remote access attributes and profiles for each user. Network managers will be able to assign users to either predefined or customized profiles with system use parameters. Administration will be simplified with user object profiles edited from the Microsoft Management Console (MMC) of Windows NT Server 5.0. In addition to general profile categorizations, such as by workgroup, the system stores information specific to each user, with a pointer to the profile.

Encryption

Routing and Remote Access Service supports 40-bit RSA RC4 encryption. North American customers can also use 128-bit encryption for RAS, which has been made available with Windows NT Server 4.0 Service Pack 2 and later Service Pack releases.

Point-to-Point Tunneling for Client-to-Server

Routing and Remote Access Service continues to support Point-to-Point Tunneling support offered initially in Windows NT 4.0 by enabling remote –client computers to connect to an enterprise network using a secure, encrypted tunnel via the Internet. RRAS with Windows NT Server 5.0, will also support Layer 2 Tunneling Protocol for such client-to-server remote connections.

Point-to-Point Tunneling for Server-to-Server

Routing and Remote Access Service extends the Point-to-Point Tunneling support offered initially in Windows NT 4.0 by enabling remote networks - not just remote clients—to connect using a secure, encrypted tunnel. And as earlier noted, RRAS with Windows NT Server 5.0, will also support Layer 2 Tunneling Protocol. Tunneling enables branch offices to be connected to a corporate network via the Internet rather than via more expensive leased line arrangements. This new use of

the Internet as a Virtual Private Network (VPN) can provide big cost savings compared to traditional WAN link alternatives.

Restartable File Copy

Restartable File Copy automatically begins re-transferring a file upon re-connection whenever the RAS connection has been lost. This removes the frustration of losing a connection during a file transfer. Restartable File Copy addresses these problems by remembering the status of the file transmission and continuing the transfer from that point upon reconnection.

Multi-Link PPP

RRAS retains a compelling communications features first offered with RAS in Windows NT Server 4.0 – Multi-Link PPP. Multi-Link PPP allows the bandwidth of two or more modems and/or ISDN lines to be combined to create a single virtual information pipeline. Multi-link PPP supports the simultaneous transfer of data across parallel connections which effectively delivers scaleable bandwidth for maximum efficiency. This feature can be used for both remote client-to-server connections as well as for remote server-to-server connections. In addition, tunneled connections with PPTP or L2TP can be run over Multi-Link PPP connections so the feature provides a great deal of flexibility.

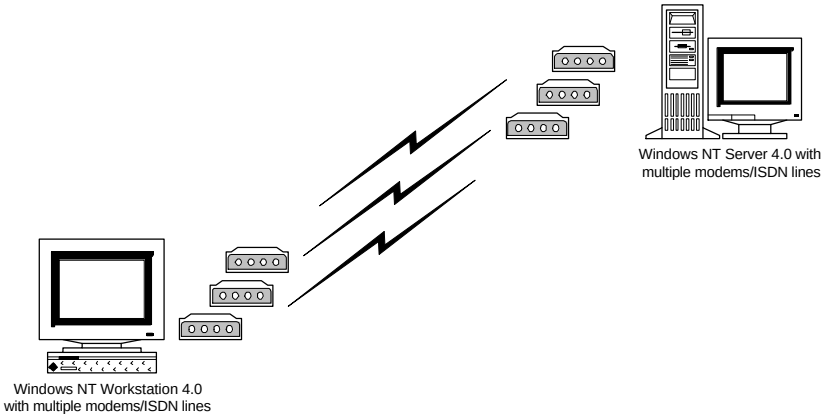

Figure 1. Multi-Link PPP – delivering the bandwidth of two or more analog or digital links.

The Multi-Link PPP support provided by RRAS is based on the IETF standard RFC 1717.

Bandwidth Allocation Protocol

Routing and Remote Access Service will introduce the Bandwidth Allocation

Protocol (BAP) in the Windows NT 5.0 timeframe. BAP brings additional efficiencies to Multi-link PPP by dynamically adding or dropping additional links to accommodate traffic flow.

BAP is especially valuable to operations that have carrier charges based on bandwidth utilization. The network manager uses a simple graphical user interface to set the parameters at which multi-link lines are dropped or added. For example, a manager could set the system so that an extra line was dropped if link utilization dropped below 50 percent for more than 10 seconds. Likewise, the system can be set to add a line if bandwidth utilization goes above 50 percent (or whatever value the network manager chooses) for more than perhaps 20 seconds. Because ISDN lines can be added nearly instantaneously BAP provides a very efficient mechanism for controlling connection costs while dynamically providing optimum bandwidth.

RAS Idle Disconnect

This feature automatically terminates your connection to a remote client or to a remote server after a certain period of time if there has been no activity over the remote dial-up communications link. network administrator can specify the amount of time before this feature is activated. This is a Windows NT 4.0 feature that is retained in RRAS.

MANAGING ROUTING AND REMOTE ACCESS SERVICE

Routing and Remote Access Service and Windows NT Server provide a platform rich in management features which can be used to create great value-added third-party products. Management features include:

- Management and User Interface APIs
- Graphical User Interface
- Wizard for Demand Dial Routing Set-Up
- Scriptable, Command line User Interface
- Remote Manageability

Management and User Interface APIs

Routing and Remote Access Service provides for ease of administration with both an intuitive graphical user interface and a command-line user interface. A full set of APIs make RRAS management extensible, a great example of the potential for third-party development.

The built-in management features and APIs make it easy to deploy RRAS in existing or new network environments. RRAS supports Simple Network Protocol (SNMP) MIB II so RRAS can be managed from an SNMP console. RRAS running on a Windows NT Server platform can appear, act, and be managed like many other routers in an organization. This allows RRAS to interoperate with existing networking systems. SNMP standards allow devices from different companies to be administered from a central point, such as from an HP OpenView console.

Graphical User Interface

RRAS includes a comprehensive, intuitive graphical user interface that provides a wide range of monitoring and administrative functions for all routes, LAN or WAN interfaces, packet filtering features, and more.

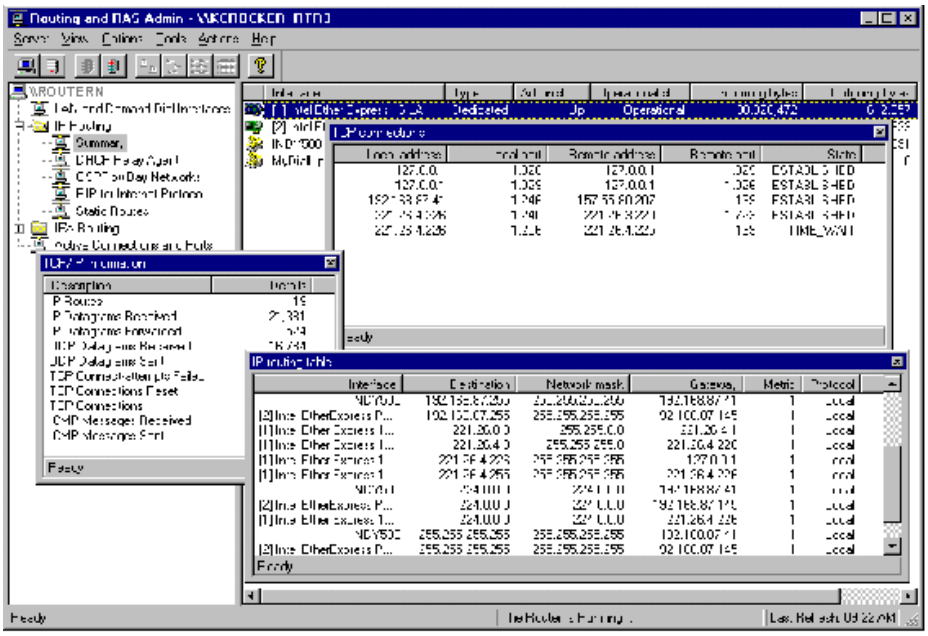

Figure 2. The graphical user interface enhances administration.

RRAS supports administrative screens that are consistent with other standard Windows GUI approaches, including support for right clicking on the mouse for additional control and a setup wizard.

Common administrative tasks that can be performed through the simple graphical user interface include:

- Adding a demand-dial interface
- Granting RAS clients dial-in permissions
- Adding a routing protocol
- Adding interfaces to a protocol
- Deleting interfaces from a protocol
- Managing remote access servers

Wizard for Demand Dial Routing Set-Up

The most challenging set-up and configuration task that emerged from the initial "Steelhead" technical beta program involved the process of setting up a demand dial interface. In fact, this particular task generated the highest number of support calls in that stage of the beta program.

Microsoft addressed the issue by developing a Demand Dial Interface Wizard.

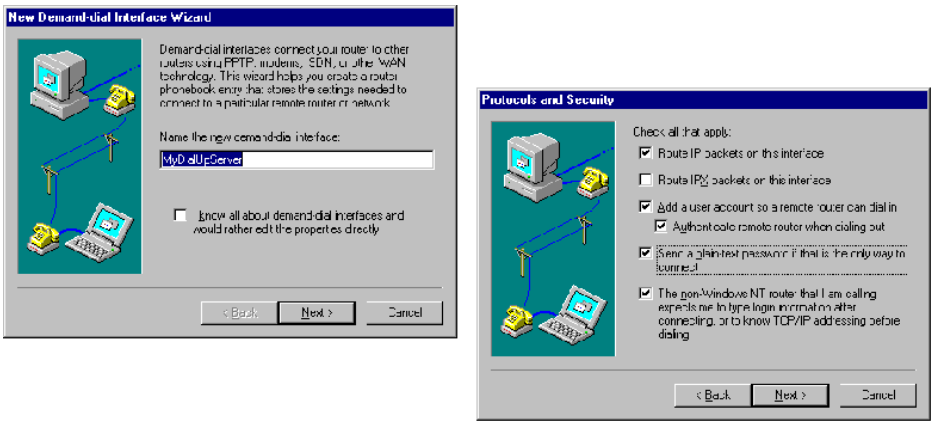

Figure 3. The new Routing Demand Dial Interface Wizard makes set-up a snap.

This wizard makes setting up a demand dial interface quick and easy with RRAS. The wizard prompts the user to type in or check off relevant information then uses that information to configure the service.

Scriptable, Command line User Interface

Many network managers are more comfortable using a command-line interface to manage their network infrastructure, especially in multi-site situations. RRAS supports command-line interface control, including support for scripting.

RRAS provides the **routemon** scripting utility, which network administrators can use to configure interfaces, routing protocols, filters, and routes for routers running the service. Routemon also displays the configuration of a currently running router service on any computer. The utility also has a scripting feature that can be used to run a collection of commands in batch mode against a specified router.

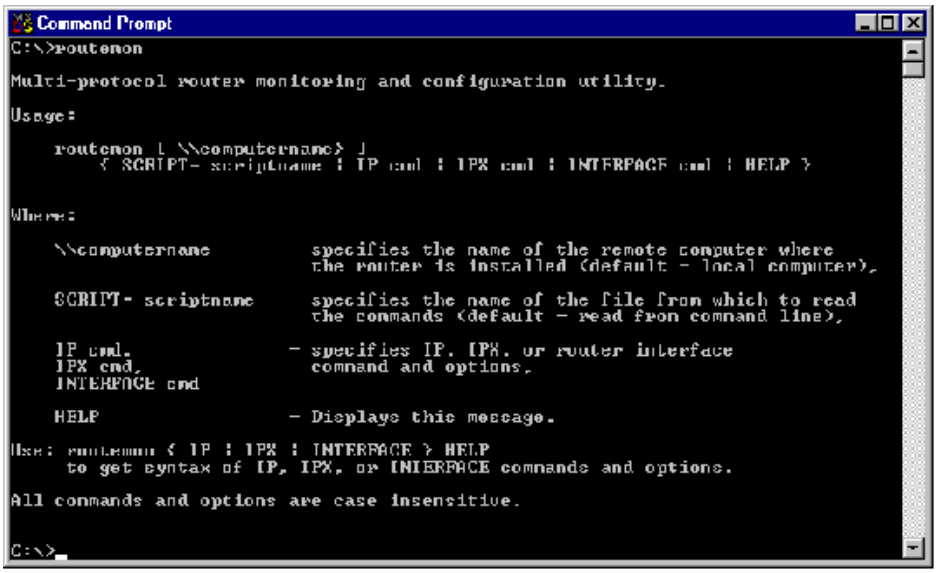

Figure 4. Routemon allows command-line management and scripting.

Remote Manageability

RRAS's GUI controls and command-line controls can be used to enable enterprise network management from a central location, remote site, or from mobile workstations. The service's GUI controls are remotely enabled via Remote Procedure Calls. Command line admin support is remoteable via Telnet.

SECURING NETWORK COMMUNICATION

Network security is a top priority item for any network administrator. Many organizations rely on routers to provide an important measure of security at the point where their internal networks come in contact with the outside world. This security can also be used within an organization's network to maintain a higher degree of security for certain portions of a network -- for example, a human resources or legal. Routing and Remote Access Service provides a range of security features including:

- IP Packet Filtering
- IPX Packet Filtering
- RADIUS Client RFC 2058 Compliant
- Works with Microsoft Proxy Service
- Robust Windows NT Server Security

IP Packet Filtering

- Routing and Remote Access Server supports a variety of inbound and outbound packet filtering features, which provide an important measure of network security.

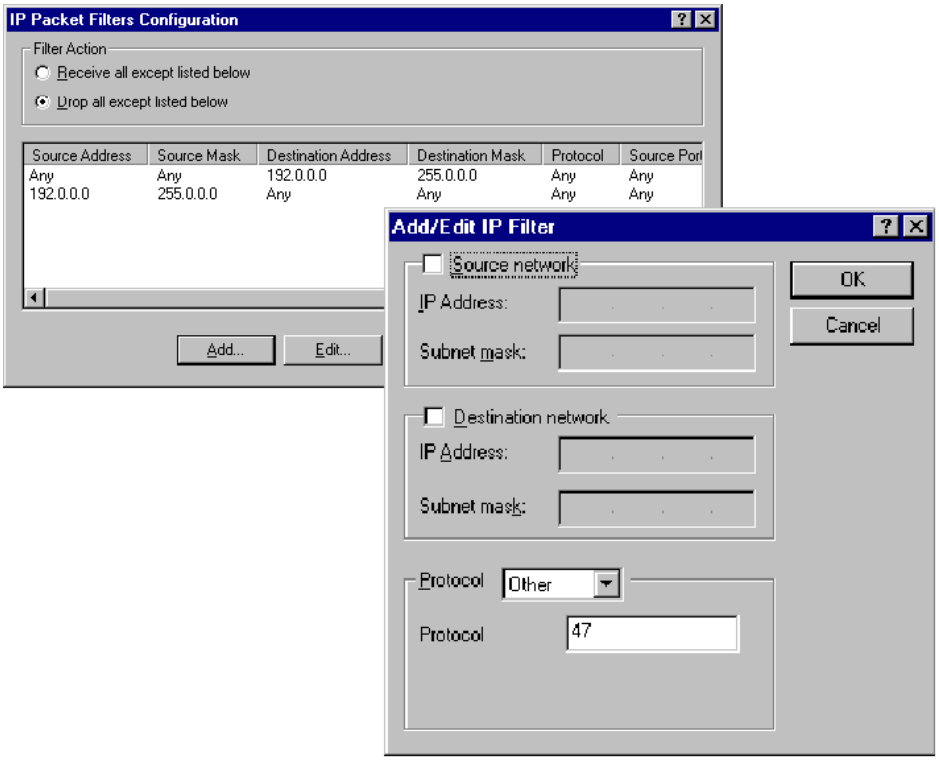

Figure 5. Setting up packet filtering is quick and easy with RRAS.

Filtering options include:

- TCP Port
- UDP Port

- IP protocol ID
- ICMP Type
- ICMP Code
- Source Address
- Destination Address
- TCP Established

RRAS packet Filters are configured on an exception basis. Filters can be configured to pass only packets from routes specified by the network manager or configured to pass everything except packets from specified routes. Managing the packet filtering is made easy with GUI-based tools.

IPX Packet Filtering

RRAS supports a similar level of packet filtering for IPX packets. IPX filtering options include:

- Source Address
- Source Node
- Source Socket
- Destination Address
- Destination Node
- Destination Socket
- Packet Type.

RADIUS Client RFC 2058 compliant

RRAS allows a server PC running Windows NT Server to act as a Remote Authentication Dial-In User Service (RADIUS) client to a RADIUS server, providing expanded choice for authentication. RADIUS, a dialup authentication and accounting protocol commonly used by Internet Service Providers, offers another security option that complies with IETF RFC 2058. With this new RADIUS client support, an ISP administrator can elect to use Windows NT Server domain-based database for user authentication or can instead elect to use some other RADIUS server database to perform the authentication.

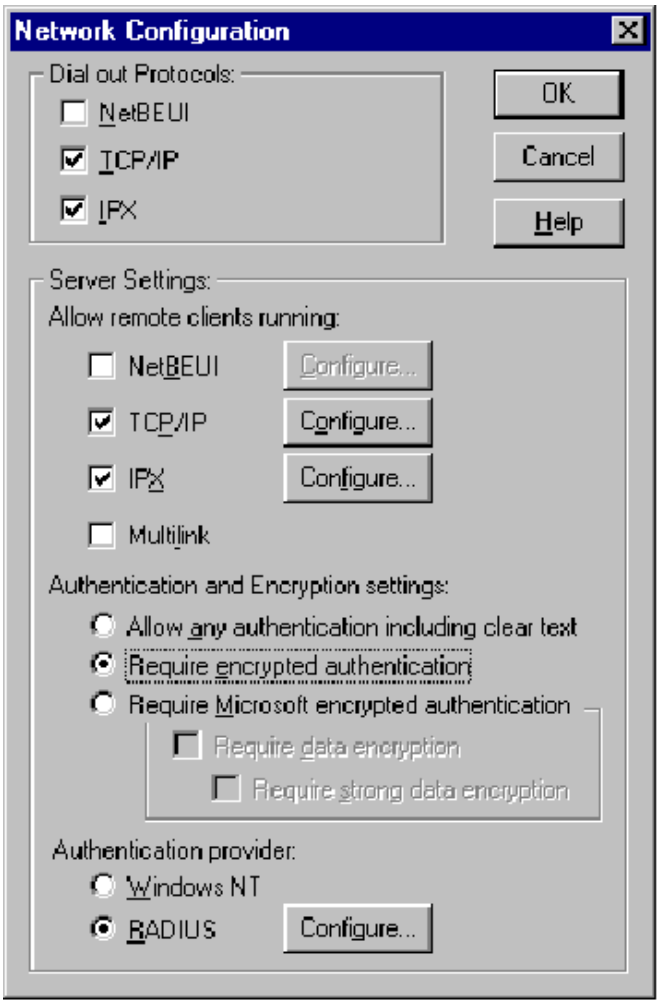

Figure 6. RADIUS Authentication or Windows NT domain authentication can be used.

Integration with Microsoft Proxy Server

The packet-layer security of Routing and Remote Access Service can be combined with the multi-layered security and Web caching performance of Microsoft Proxy Server to provide an even higher level of network security and performance.

Microsoft Proxy Server 2.0 is a unique product combining the security of a firewall with the high performance and cost savings of a Web cache server, in one easy-to-use, affordable package. Microsoft Proxy Server is a great solution for easy and secure Internet access as well as for Intranet support.

Because the Routing and Remote Access Service runs on an industry standard PC platform running Windows NT Server 4.0, an organization can install and use Microsoft Proxy Server on the same server running RRAS. This combination of server-based routing and Microsoft Proxy Server provides a full spectrum of security and performance for organizations of virtually any size.

Robust Windows NT Server Security

Routing and Remote Access Service and Microsoft Proxy Server inherit all the built-in security features that make Windows NT Server such a secure, scalable platform. RRAS supports the authentication and encryption provided in Windows NT Server 4.0, extending these resources for use with routing.

As noted earlier, RRAS supports bulk data encryption using RSA RC4 and a 40-bit or 128-bit session key. The key is negotiated at PPP connect time between the RAS client or Windows NT Server PC running RRAS on one end and the Windows NT Server-based PC on the other end. The service also supports Password Authentication Protocol (PAP), Shiva PAP, Challenge Handshake Authentication Protocol (CHAP), and the Microsoft Challenge Handshake Authentication Protocol (MS-CHAP)algorithms.

SUMMARY

Routing and Remote Access Service makes Windows NT Server a better than ever platform for deploying a broad array of internetworking solutions. And the huge movement toward the IP standard means the release of RRAS comes at an extraordinarily opportune time for ISVs, IHVs, system integrators, VARs, and network managers involved in creating internetworking solutions

With older networks being re-engineered and with an unprecedented demand for branch office communications, edge routing, VPNs, remote access, firewalls, and other internetworking deployments, third parties can use the flexibility, robustness and scalability of RRAS to meet booming customer needs.

System integrators and network managers can combine the power of RRAS with other Windows NT Server products such as Microsoft Proxy Server, Internet Information Server, and the BackOffice family of applications to create turn-key, single-box solutions for branch offices.

RRAS capabilities are enhanced by the addition of Extensible Authentication Protocol, Bandwidth Allocation Protocol, and RRAS User Profiles in the Windows NT Server 5.0 time frame, along with other core communications enhancements in the operating system.

Companies offering solutions based on today's RRAS platform will also be able to capitalize on RRAS and related enhancements in the Windows NT 5.0 time frame to continue offering innovative, value-added internetworking solutions for a wide range of customers.

FOR MORE INFORMATION

For more information on or to download the Routing and Remote Access Service Update, please see: http://www.microsoft.com/ntserver/nts/downloads/winfeatures/RouteRASNT.asp.

For information on Microsoft's communications and telephony offerings, please see: http://www.microsoft.com/ntserver/commserv/default.asp.

For more information regarding Microsoft Proxy Server 2.0, please see http://www.microsoft.com/proxy.

To see a list of the wide variety of LAN and WAN cards that have earned the Windows Compatible logo and, thus, will work with RRAS, please see the Windows Hardware Compatibility List for Windows NT Server 4.0 here: http://www.microsoft.com/hwtest.