Windows 2000 Server

Chapter 2 - Routing and Remote Access Service

Microsoft® Windows® 2000 includes the Routing and Remote Access service, a component originally supplied for Microsoft® Windows NT® version 4.0, which provides integrated multiprotocol routing and remote access, and virtual private network server services for Microsoft® Windows® 2000 Server-based computers.

In This Chapter

Related Information in the Resource Kit

- For more information about unicast IP routing support, see "Unicast IP Routing" in this book.
- For more information about IP multicast support, see "IP Multicast Support" in this book.
- For more information about IPX routing support, see "IPX Routing" in this book.
- For more information about demand-dial support, see "Demand-Dial Routing" in this book.
- For more information about remote access, see "Remote Access Server" in this book.
- For more information about virtual private networking support, see "Virtual Private Networking" in this book.

Introduction to the Routing and Remote Access Service

Multiprotocol routing support for the Windows NT family of operating systems began with Microsoft® Windows NT® 3.51 Service Pack 2, which included components for the Routing Information Protocol (RIP) for IP, RIP for IPX, and the Service Advertising (SAP) for IPX. Windows NT 4.0 also included these components. In June 1996, Microsoft released the Routing and Remote Access Service (RRAS) for Windows NT 4.0, a component that replaced the Windows NT 4.0 Remote Access Service, RIP for IP, RIP for IPX, and SAP for IPX services with a single integrated service providing both remote access and multiprotocol routing.

RRAS for Windows NT 4.0 added support for:

- RIP version 2 routing protocol for IP.
- Open Shortest Path First (OSPF) routing protocol for IP.
- Demand-dial routing, the routing over on-demand or persistent WAN links such as analog phone, ISDN, or using the Point-to-Point Tunneling Protocol (PPTP).
- ICMP Router Discovery.
- Remote Authentication Dial-In User Service (RADIUS) client.
- IP and IPX packet filtering.
- Point-to-Point Tunneling Protocol (PPTP) support for router-to-router VPN connections.
- A graphical user interface administrative program called Routing and RAS Admin and a command-line utility called Routemon.

Windows 2000 Routing and Remote Access Service

The Routing and Remote Access service for Windows 2000 Server continues the evolution of multiprotocol routing and remote access services for the Microsoft Windows platform. New features of the Routing and Remote Access service for Windows 2000 include:

- Internet Group Management Protocol (IGMP) and support for multicast boundaries.
- Network address translation with addressing and name resolution components that simplify the connection of a small office/home office (SOHO) network to the Internet.
- Integrated AppleTalk routing.
- Layer Two Tunneling Protocol (L2TP) over IP Security (IPSec) support for router-to-router VPN connections.
- Improved administration and management tools. The graphical user interface program is the Routing and Remote Access administrative utility, a Microsoft Management Console (MMC) snap-in. The command-line utility is Netsh.

All of the combined features of the Windows 2000 Routing and Remote Access service make a Windows 2000 Server-based computer function as the following:

- Multiprotocol router

  A Routing and Remote Access service computer can route IP, IPX, and AppleTalk simultaneously. All routable protocols and routing protocols are configured from the same administrative utility.
- Demand-dial router

  A Routing and Remote Access service computer can route IP and IPX over on-demand or persistent WAN links, such as analog phone lines or ISDN, or over VPN connections using either PPTP or L2TP over IPSec.
- Remote access server

  A Routing and Remote Access service computer can act as a remote access server providing remote access connectivity to dial-up or VPN remote access clients using IP, IPX, AppleTalk, or NetBEUI.

The combination of routing and remote access services on the same computer create a Windows 2000 remote access router.

An advantage of the Routing and Remote Access service is its integration with the Windows 2000 Server operating system. The Routing and Remote Access service works with a wide variety of hardware platforms and hundreds of network adapters; the result is a lower cost solution than many mid-range dedicated router or remote access server products.

The Routing and Remote Access service is extensible with application programming interfaces (APIs) that third-party developers can use to create custom networking solutions and that new vendors can use to participate in the growing business of open internetworking.

Combining Routing and Remote Access

One question that is commonly asked about the Routing and Remote Access service is: Why combine both routing and remote access into a single service? Both services worked fine separately in the original version of Windows NT 4.0.

The reason for combining the two services lies in the Point-to-Point Protocol *(PPP)*, which is the protocol suite that is commonly used to negotiate point-to-point connections for remote access clients. PPP provides link parameter negotiation, the exchange of authentication credentials, and network layer protocol negotiation. For example, when you dial an Internet service provider (ISP) using PPP, you agree to the size of the packets you are sending and how they are framed (link negotiation), you log on using a user name and password (authentication), and you obtain an IP address (network layer negotiation).

Demand-dial routing connections also use PPP to provide the same kinds of services as remote access connections (link negotiation, authentication, and network layer negotiation). Therefore, the integration of routing (which includes demand-dial routing) and remote access was done to leverage the existing PPP client/server infrastructure that existed for the remote access components.

The PPP infrastructure of Windows 2000 Server includes support for:

- Dial-up remote access (remote access over dial-up equipment such as analog phone lines and ISDN) as either the client or server.
- VPN remote access (remote access over VPN connections using either PPTP or L2TP over IPSec) as either the client or server.
- On-demand or persistent dial-up demand-dial routing (demand-dial routing over dial-up equipment such as analog phone lines and ISDN) as either the calling router or the answering router.
- On-demand or persistent VPN demand-dial routing (demand-dial routing over VPN connections using either PPTP or L2TP over IPSec) as either the calling router or the answering router.

Authentication and Authorization

The distinction between authentication and authorization is important for understanding how connection attempts are either accepted or denied.

- *Authentication* is the verification of the credentials of the connection attempt. This process consists of sending the credentials from the remote access client to the remote access server in either a cleartext or encrypted form using an authentication protocol.
- *Authorization* is the verification that the connection attempt is allowed. Authorization occurs after successful authentication.

For a connection attempt to be accepted, the connection attempt must be both authenticated and authorized. It is possible for the connection attempt to be authenticated using valid credentials, but not authorized. In this case, the connection attempt is denied.

If the remote access server is configured for Windows authentication, Windows 2000 security verifies the credentials for authentication and the dial-up properties of the user account, and locally stored remote access policies authorize the connection. If the connection attempt is both authenticated and authorized, the connection attempt is accepted.

If the remote access server is configured for RADIUS authentication, the credentials of the connection attempt are passed to the RADIUS server for authentication and authorization. If the connection attempt is both authenticated and authorized, the RADIUS server sends an accept message back to the remote access server and the connection attempt is accepted. If the connection attempt is either not authenticated or not authorized, the RADIUS server sends a reject message back to the remote access server and the connection process is denied.

If the RADIUS server is a Windows 2000 server-based computer running the Internet Authentication Service (IAS), the IAS server performs authentication through Windows 2000 security and authorization through the dial-up properties of the user account and the remote access policies stored on the IAS server.

The configuration of the Routing and Remote Access service authentication provider is done from the **Security** tab from the properties of a remote access router in the Routing and Remote Access snap-in or by using the **netsh ras aaaa set authentication** and **netsh ras aaaa set authserver** commands.

Accounting

The Routing and Remote Access service can be configured to log accounting information in the following locations:

- Locally stored log files when configured for Windows accounting. The information logged and where it is stored are configured from the properties of the Remote Access Logging folder in the Routing and Remote Access snap-in.
- At a RADIUS server when configured for RADIUS accounting. If the RADIUS server is an IAS server, the log files are stored on the IAS server. The information logged and where it is stored are configured from the properties of the Remote Access Logging folder in the Internet Authentication Service snap-in.

The configuration of the Routing and Remote Access service accounting provider is done from the **Security** tab from the properties of a remote access router in the Routing and Remote Access snap-in or by using the **netsh ras aaaa set accounting** and **netsh ras aaaa set acctserver** commands.

Installation and Configuration

Unlike with RRAS for Windows NT 4.0 and most network services of Windows 2000, you cannot elect to install or uninstall the Routing and Remote Access service through **Add/Remove Programs** in Control Panel. The Windows 2000 Routing and Remote Access service is automatically installed in a disabled state.

To enable and configure the Routing and Remote Access service

1. Run **Routing and Remote Access** from the Administrative Tools folder.
2. For the local computer, right-click the server icon and select **Configure and Enable Routing and Remote Access**.

   For a remote computer, right-click the **Server Status** icon and click **Add Server**. In the **Add Server** dialog boxes, select the server you want to add.
3. To configure your remote access router, in the Routing and Remote Access Server Setup Wizard, select the appropriate options.

Once the wizard has finished, the remote access router is enabled and configured based on your selections in the wizard. To do further configuration, use the Routing and Remote Access snap-in.

Refreshing the Configuration

You cannot remove the Routing and Remote Access service using **Add/Remove Programs** in **Control Panel**; however, you can refresh the configuration by disabling the Routing and Remote Access service and then reconfiguring it. Disabling the service removes all Routing and Remote Access registry settings.

To refresh the configuration of the Routing and Remote Access service

1. Run **Routing and Remote Access** from the Administrative Tools folder.
2. For the appropriate computer, right-click the server icon and select **Disable Routing and Remote Access**.
3. When prompted with the warning dialog box, select **Yes**.
4. To configure the Routing and Remote Access service configuration, use the enable and configure procedure.

Note If you disable the Routing and Remote Access service, all current configuration for the service, including routing protocol configuration and demand-dial interfaces, is removed and all currently connected clients are disconnected.

Features of the Routing and Remote Access Service

The Routing and Remote Access service for Windows 2000 includes a wide variety of features for unicast and multicast IP routing, IPX routing, AppleTalk routing, remote access, and VPN support.

Unicast IP Support

Unicast IP support consists of the following:

- Static IP routing

  With this inherent function of the TCP/IP protocol for Windows 2000, you can manage static routes using the Routing and Remote Access snap-in rather than the Route tool.

- Routing Information Protocol (RIP) versions 1 and 2

  A distance vector-based routing protocol commonly used in small and medium IP internetworks.

- Open Shortest Path First (OSPF)

  A link state-based routing protocol commonly used in medium to large IP internetworks.

- DHCP Relay Agent

  An agent that relays Dynamic Host Configuration Protocol (DHCP) messages between DHCP clients and DHCP servers on different network segments.

- Network address translation

  A network address translator component that creates a translated connection between privately addressed networks and the Internet.

- IP packet filtering

  The ability to define what traffic is allowed into and out of each interface based on filters defined by the values of source and destination IP addresses, TCP and UDP port numbers, ICMP types and codes, and IP protocol numbers.

- ICMP router discovery

  The ability to periodically advertise and respond to host router solicitations to support ICMP router discovery by hosts on a network segment.

For more information, see "Unicast IP Support" in this book.

IP Multicast Support

IP multicast support consists of the following:

- Multicast forwarding

  With this inherent function of the TCP/IP protocol for Windows 2000, you can view the multicast forwarding table using the Routing and Remote Access snap-in.

- Internet Group Management Protocol (IGMP) versions 1 and 2

  The TCP/IP protocol to track multicast group membership on attached network segments.

- Ability to support limited multicast forwarding and routing

  When you use the IGMP routing protocol and configure interfaces for IGMP router mode and IGMP proxy mode, the Windows 2000 router can support multicast forwarding and routing for specific configurations.

- Multicast boundaries

  Multicast boundaries (barriers to the forwarding of IP multicast traffic) can be based on the IP multicast group address, the Time-To-Live (TTL) in the IP header, or on the maximum amount of multicast traffic in kilobytes per second.

For more information, see "IP Multicast Support" in this book.

IPX Support

IPX support consists of the following:

- IPX packet filtering

  The ability to define what traffic is allowed into and out of each interface based on filters defined by the values of source and destination IPX network, node, socket numbers, and packet type.

- RIP for IPX

  A distance-vector-based routing protocol commonly used on IPX internetworks. The Routing and Remote Access service also provides the ability to configure static IPX routes and RIP route filters.

- SAP for IPX

  Service Advertising Protocol (SAP) is a distance-vector-based advertising protocol commonly used on IPX internetworks to advertise services and their locations. The Routing and Remote Access service also provides the ability to configure static SAP services and SAP service filters.

- NetBIOS over IPX

  NetBIOS over IPX is used by Microsoft networking components to support file and printer sharing components. The Routing and Remote Access service can also forward NetBIOS over IPX broadcasts and configure static NetBIOS names.

For more information, see "IPX Routing" in this book.

AppleTalk

AppleTalk consists of supporting the forwarding of AppleTalk packets as an AppleTalk router and the use of the Routing Table Maintenance Protocol (RTMP). For more information about AppleTalk routing, see "Services for Macintosh" in this book.

Demand-Dial Routing

IP and IPX traffic can be forwarded over demand-dial interfaces over persistent or over on-demand WAN links. For on-demand connections, the Routing and Remote Access service automatically creates a PPP-based connection to the configured endpoint when traffic matching a static route is received.

For more information, see "Demand-Dial Routing" in this book.

Remote Access

The Routing and Remote Access service enables a computer to be a remote access server, accepting remote access connections from remote access clients using traditional dial-up technologies such as analog phone lines and ISDN.

For more information, see "Remote Access Server" in this book.

VPN Server

The Routing and Remote Access service enables a computer to be a virtual private network (VPN) server, supporting both PPTP and L2TP over IPSec and accepting both remote access and router-to-router (demand-dial) VPN connections from remote access clients and calling routers.

For more information, see "Virtual Private Networking" in this book.

RADIUS Client

The Routing and Remote Access service can be configured as a Remote Authentication Dial-In User Service (RADIUS) client for authentication, authorization, and accounting. Parameters of all PPP-based connection attempts are sent to the configured RADIUS server for authentication and authorization. Information about connections is sent to the configured RADIUS server for accounting.

Windows 2000 also includes the Internet Authentication Service (IAS), an implementation of a RADIUS server. For more information, see "Internet Authentication Service" in this book.

SNMP MIB Support

Windows 2000 and the Routing and Remote Access service provide Simple Network Management Protocol (SNMP) version 1 agent functionality with support for Internet MIB II as documented in RFC 1213. SNMP management stations can be used to manage a Windows 2000 remote access router. Beyond Internet MIB II support, the Routing and Remote Access service also provides MIB dynamic-link libraries (DLLs) for the following:

- IP Forwarding Table MIB

  Objects in the IP Forwarding Table MIB are documented in RFC 1354, "IP Forwarding Table MIB."
- Microsoft RIP version 2 for Internet Protocol MIB
- Wellfleet-Series7-MIB for OSPF
- Microsoft BOOTP for Internet Protocol MIB
- Microsoft IPX MIB
- Microsoft RIP and SAP for IPX MIB
- Internet Group Management Protocol MIB

  Objects in the Internet Group Management Protocol MIB are documented in the Internet draft titled "Internet Group Management Protocol MIB."
- IP Multicast Routing MIB

  Objects in the IP Multicast Routing MIB are documented in the Internet draft titled "IP Multicast Routing MIB."

Extensive LAN and WAN Support

The Routing and Remote Access service can run over any of the network adapters supported by Windows 2000 Server, including WAN cards from Eicon, Cisco, SysKonnect, Allied and US Robotics. For more information about supported network adapters, see the Windows 2000 Hardware Compatibility link at http://windows.microsoft.com/windows2000/reskit/webresources .

Graphical and Command-Line Management Utilities

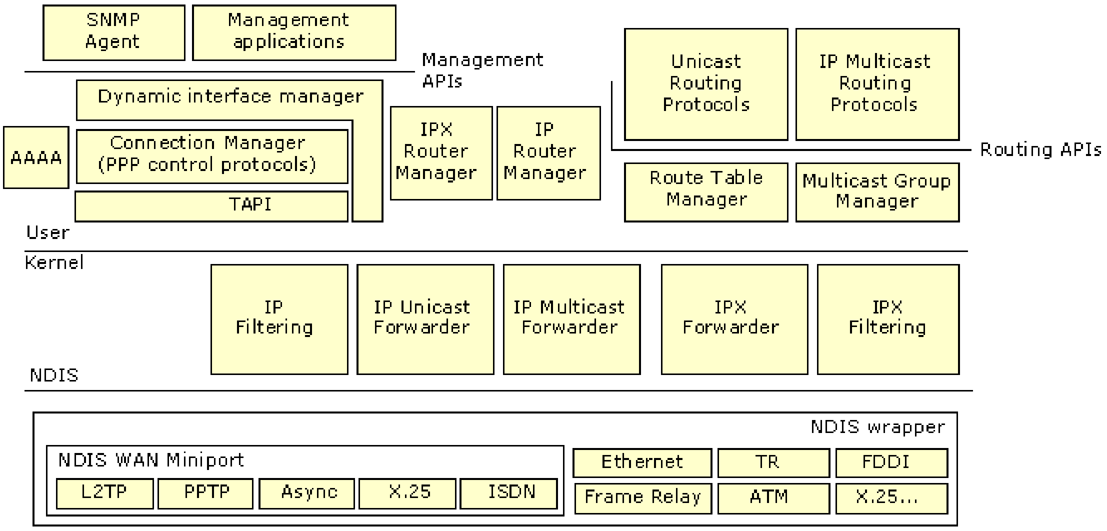
The Routing and Remote Access service includes the Routing and Remote Access snap-in, a Windows 2000 administrative utility that provides easy viewing and configuration of local or remote Windows 2000 remote access routers, and Netsh.exe, a command-line utility that can also run scripts for local automated configuration. For more information, see "Routing and Remote Access Service Tools and Facilities" later in this chapter.

API Support for Third-Party Components

The Routing and Remote Access service has fully published API sets for unicast and multicast routing protocol and administration utility support. Routing protocol developers can write additional routing protocols and interface directly into the Routing and Remote Access service architecture. Other software vendors can also use Routing and Remote Access service administration APIs to provide their own management utilities.

Architecture of the Routing and Remote Access Service

The architecture of the Routing and Remote Access service is shown in Figure 2.1.



If your browser does not support inline frames, click here to view on a separate page.

Figure 2.1 Architecture of the Routing and Remote Access Service

Note The Network Address Translation (NAT) component of the Routing and Remote Access service is not shown in Figure 2.1. NAT is not a routing protocol. For more information about how the NAT component interacts with Routing and Remote Access components and the TCP/IP protocol, see "Unicast IP Routing" in this book.

SNMP Agent

The Windows 2000 Routing and Remote Access service supports the Simple Network Management Protocol (SNMP) management information bases (MIBs) previously described in the "Features of the Routing and Remote Access Service" section earlier in this chapter.

Management Applications

Management applications for the Routing and Remote Access service include the Routing and Remote Access snap-in, available from the Administrative Tools folder and the Netsh command-line utility.

AAAA

A set of components that provides authentication, authorization, auditing, and accounting (AAAA) for the Routing and Remote Access service when it is configured for Windows authentication and Windows accounting. When the Routing and Remote Access service is configured for RADIUS authentication and accounting, the local AAAA components are not used.

The AAAA components are also used by the Internet Authentication Service (IAS).

DIM (Mprdim.dll)

The dynamic interface manager (DIM) is a component that:

- Supports a remote procedure call (RPC) interface for SNMP-based management functions used by management utilities such as the Routing and Remote Access snap-in.
- Loads configuration information from the Windows 2000 registry.
- Communicates with the Connection Manager for demand-dial connections.
- Communicates configuration information to the router managers (such as the IP Router Manager and IPX Router Manager).
- Manages all routing interfaces including LAN, persistent demand-dial, and IP-in-IP interfaces.

Connection Manager

A set of components that:

- Manages WAN devices.
- Establishes connections using TAPI.
- Negotiates PPP control protocols, including Extensible Authentication Protocol (EAP).
- Implements Multilink and Bandwidth Allocation Protocol (BAP).

TAPI

The Telephony Application Programming Interface, also known as Telephony API(TAPI), provides services to create, monitor, and terminate connections in a hardware-independent manner. Connection Manager uses TAPI to create or receive demand-dial connections. For more information about TAPI, see "Telephony Integration and Conferencing" in this book.

IP Router Manager (Iprtmgr.dll)

A component that:

- Obtains configuration information from the DIM.
- Communicates IP packet filtering configuration to the IP filtering driver.
- Communicates IP routing configuration information to the IP forwarder in the TCP/IP protocol.
- Maintains an interface database of all IP routing interfaces.
- Loads and communicates configuration information to IP routing protocols (such as RIP for IP and OSPF supplied with Windows 2000).
- Initiates demand-dial connections on behalf of routing protocols by communicating with the DIM.

IPX Router Manager (Ipxrtmgr.dll)

A component that:

- Obtains configuration information from the DIM.
- Communicates IPX packet filtering configuration to the IPX filtering driver.
- Communicates IPX routing configuration information to the IPX forwarder driver.
- Maintains an interface database of all IPX routing interfaces.
- Loads and communicates configuration information to IPX routing protocols (RIP for IPX, SAP for IPX).
- Initiates demand-dial connections on behalf of routing protocols by communicating with the DIM.

Unicast Routing Protocols

The Routing and Remote Access service provides the following unicast routing protocols.

RIP for IP (Iprip2.dll)

A component that:

- Communicates RIP for IP learned routes with the Route Table Manager.
- Uses Windows Sockets to send and receive RIP for IP traffic.
- Exports management APIs to support MIBs and management applications through the IP Router Manager.

OSPF Routing Protocol (Ospf.dll)

A component that:

- Communicates OSPF learned routes with the Route Table Manager.
- Uses Windows Sockets to send and receive OSPF traffic.
- Exports management APIs to support MIBs and management applications through the IP Router Manager.

RIP for IPX (Ipxrip.dll)

A component that:

- Communicates RIP for IPX learned routes with the Route Table Manager.
- Uses Windows Sockets to send and receive RIP for IPX traffic.
- Exports management APIs to support MIBs and management applications through the IPX Router Manager.

SAP for IPX (Ipxsap.dll)

A component that:

- Communicates SAP for IPX learned services with the Route Table Manager.
- Uses Windows Sockets to send and receive SAP for IPX traffic.
- Exports management APIs to support MIBs and management applications through the IPX Router Manager.

IP Multicast Protocols

The Routing and Remote Access service provides the following IP multicast protocol.

IGMP Version 1 and 2

A component that:

- Communicates multicast group membership information to the Multicast Group Manager.
- Uses Windows Sockets to send and receive IGMP traffic.
- Exports management APIs to support MIBs and management applications through the Multicast Group Manager.

Route Table Manager (Rtm.dll)

A component that:

- Maintains a user mode route table for all routes for those protocols being routed (IP and IPX). The route table includes all routes from all possible route sources.
- Exposes APIs for adding, deleting, and enumerating routes that are used by the routing protocols.
- Ages learned routes.
- Communicates only the best routes to the appropriate forwarder driver. The best routes are the routes with the lowest preference level (for IP routes) and lowest metrics. The best routes become the routes in the IP forwarding table and the IPX forwarding table.

Multicast Group Manager

A component that:

- Maintains all multicast group memberships.
- Communicates multicast forwarding entries (MFEs) in the IP multicast forwarder.
- Reflects group membership between IP multicast routing protocols.

IP Filtering Driver (Ipfltdrv.sys)

A component that:

- Obtains configuration information from the IP Router Manager.
- Applies IP filters after the IP forwarder has found a route.

IP Unicast Forwarder

A component of the TCP/IP protocol (Tcpip.sys) that:

- Obtains configuration information from the IP Router Manager.
- Stores the IP forwarding table, a table of the best routes obtained from the route table manager.
- Can initiate a demand-dial connection.
- Forwards unicast IP traffic.

IP Multicast Forwarder

A component of the TCP/IP protocol (Tcpip.sys) that:

- Stores multicast forward entries (MFEs) obtained from IP multicast routing protocols through the Multicast Group Manager.
- Based on multicast traffic received, communicates new [source, group] information to the Multicast Group Manager.
- Forwards IP multicast packets.

IPX Filtering Driver (Nwlnkflt.sys)

A component that:

- Obtains configuration information from the IPX Router Manager.
- Applies IPX filters after the IPX forwarder driver has found a route.

IPX Forwarder Driver (Nwlnkfwd.sys)

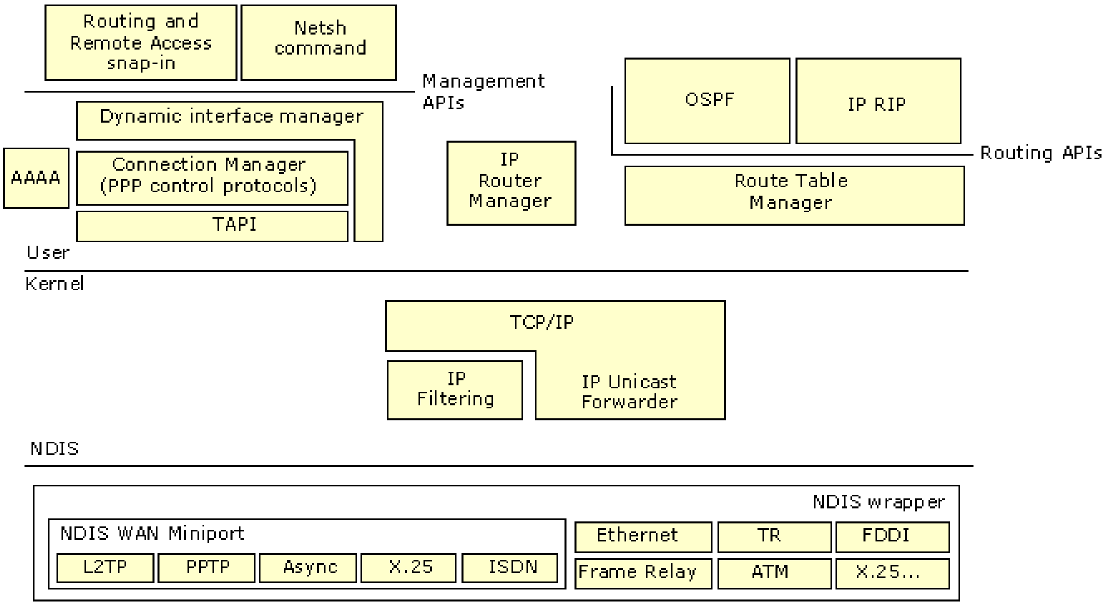
A component that:

- Obtains configuration information from the IPX Router Manager.
- Stores the IPX forwarding table, a table of the best routes obtained from the route table manager.

- Can initiate a demand-dial connection.
- Forwards IPX traffic.

Unicast IP Components and Processes

The unicast IP components of the Routing and Remote Access service are shown in Figure 2.2.



If your browser does not support inline frames, click here to view on a separate page.

Figure 2.2 Unicast IP and the Routing and Remote Access Service

The following sections describe typical unicast IP routing processes in terms of the Routing and Remote Access service unicast IP routing components.

Incoming and Outgoing Packet (Transit Traffic)

An incoming packet is handed first to the IP forwarder, which finds a route and then hands it to the IP filtering driver to check for input filters and output filters. If approved for acceptance by the input filters and for forwarding by the output filters, the packet is handed back to the IP forwarder driver, which forwards the packet over the appropriate interface using Network Driver Interface Specification (NDIS). If the input or output filters do not permit the packet to be forwarded, the packet is silently discarded. If a route is not found, an ICMP Destination Unreachable-Host Unreachable message is sent back to the source of the packet.

Incoming Packet (Local Host Traffic)

An incoming packet is handed first to the IP forwarder, which notes that the packet is not to be routed (destination IP address is the router or a broadcast address). The IP forwarder then hands it to the IP filtering driver to check for input filters. If accepted by the input filters, the packet is handed up to the TCP/IP driver, which processes the packet. If the packet is not accepted by the input filters, the packet is silently discarded.

Outgoing Packet (Local Host Traffic)

An outgoing TCP/IP packet is handed by the TCP/IP driver to the IP filtering driver, which checks for output filters. If approved for sending by the output filters, the packet is handed to the IP forwarder, which sends the packet using the best route over the appropriate interface using NDIS. If the packet is not approved by the output filters, the packet is silently discarded. If a route is not found, an IP routing error is indicated to the source application of the packet.

Routing Protocol Network Communication

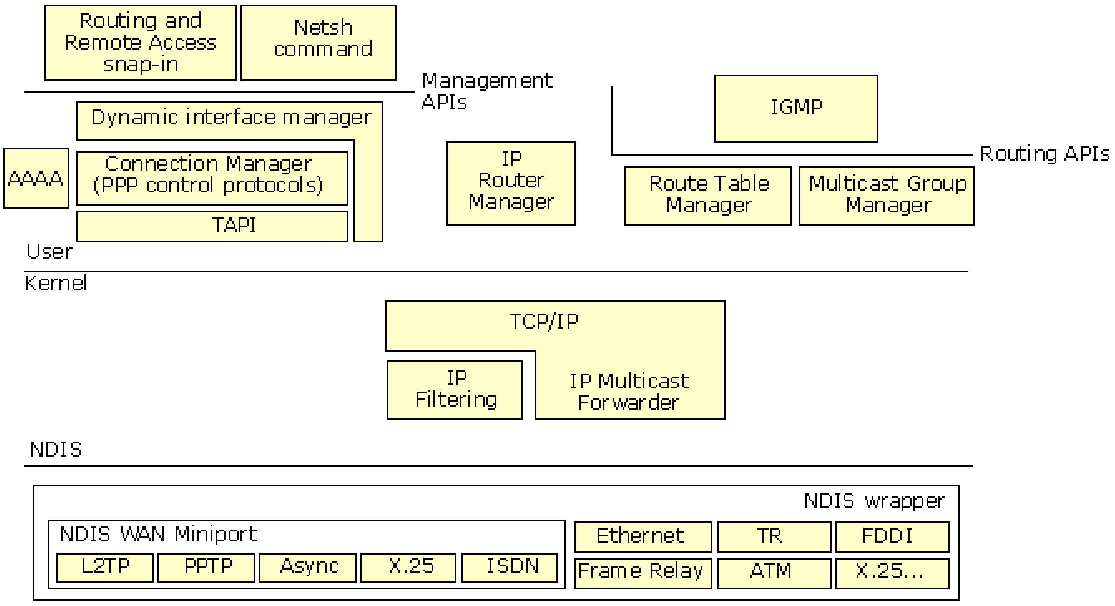
The RIP for IP and OSPF routing protocols operate like any other Windows Sockets application sending and receiving IP packets.

Routing Table Updates

RIP for IP and OSPF update routes in the Route Table Manager. Based on the best route and route source ranking, the table of best routes is updated in the IP forwarder.

IP Multicast Components and Processes

The IP multicast components of the Routing and Remote Access service are shown in Figure 2.3.



If your browser does not support inline frames, click here to view on a separate page.

Figure 2.3 IP Multicast and the Routing and Remote Access Service

The following sections describe typical IP multicast forwarding processes in terms of the Routing and Remote Access service IP multicast components.

Incoming Multicast Packet (MFE Not Present)

An incoming IP multicast packet's source address and group address are compared to the MFEs to the IP multicast forwarding table. If an entry for the [source, group] is not found, an inactive MFE for the [source, group] is added to the multicast forwarding table and communicated to the Multicast Group Manager. The packet is placed in a buffer awaiting the change from an inactive MFE to an active MFE.

Incoming Multicast Packet (Active MFE Present)

An incoming IP multicast packet's source address and group address are compared to the MFEs in the IP multicast forwarding table. If an active entry for the [source, group] is found, the multicast traffic is forwarded out the appropriate interface(s).

Multicast Routing Protocol Network Communication

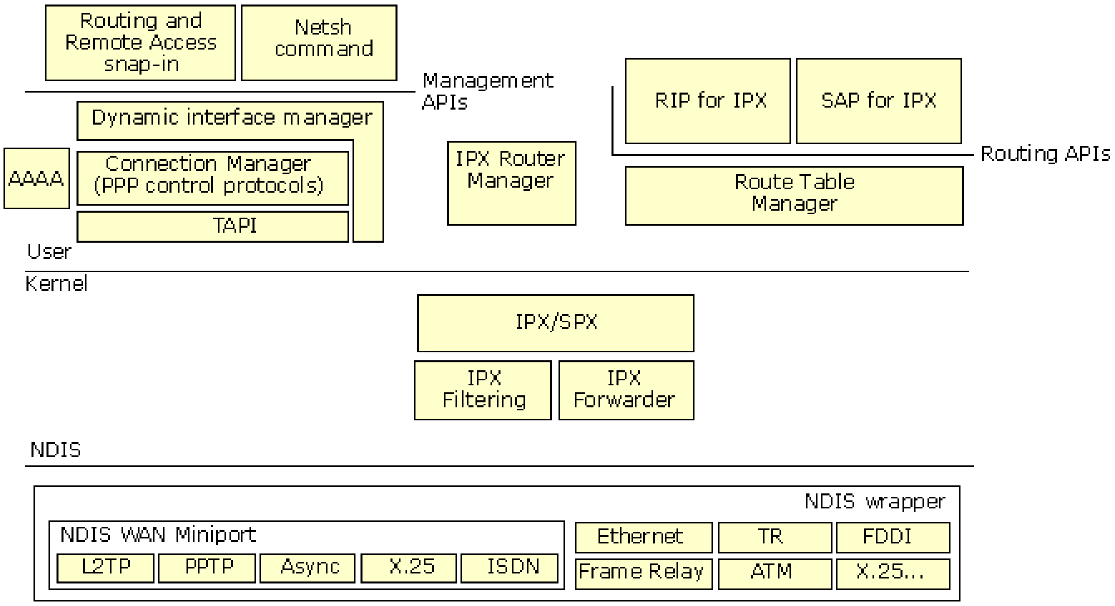
The IGMP v2 IP multicast routing protocol operates like any other Windows Sockets application sending and receiving IP packets.

Multicast Forwarding Table Updates

Based on the ongoing IGMP traffic on interfaces on which IGMP router mode is enabled, the IGMP v2 multicast routing protocol updates [source, group] entries in the Multicast Group Manager. The Multicast Group Manager then updates the IP multicast forwarding table.

IPX Components and Processes

The IPX components of the Routing and Remote Access service are shown in Figure 2.4.



If your browser does not support inline frames, click here to view on a separate page.

Figure 2.4 IP Multicast and the Routing and Remote Access Service

The following sections describe typical IPX routing processes in terms of the Routing and Remote Access service IPX routing components.

Incoming and Outgoing Packet (Transit Traffic)

An incoming packet is handed first to the IPX forwarder driver, which finds a route and then hands it to the IPX filtering driver to check for input filters and output filters. If approved for acceptance by the input filters and for forwarding by the output filters, the packet is handed back to the IPX forwarder driver, which forwards the packet over the appropriate interface using NDIS. If the input or output filters do not permit the packet to be forwarded or if a route is not found, the packet is silently discarded.

Incoming Packet (Local Host Traffic)

An incoming packet is handed first to the IPX forwarder driver, which notes that the packet is not to be routed (the destination IPX internetwork address is the router or a broadcast address) and then hands it to the IPX filtering driver to check for input filters. If accepted by the input filters, the packet is handed up to IPX/SPX, which processes the packet normally. If the packet is not accepted by the input filters, the packet is silently discarded.

Outgoing Packet (Local Host Traffic)

An outgoing IPX packet is handed by the IPX/SPX driver to the IPX filtering driver, which checks for output filters. If approved for sending by the output filters, the packet is handed to the IPX forwarder driver, which sends the packet using the best route over the appropriate interface using NDIS. If the packet is not approved by the output filters, the packet is silently discarded. If a route is not found, a RIP GetLocalTarget message is sent. For more information about IPX routing processes, see "IPX Routing" in this book.

Routing Protocol Network Communication

The RIP for IPX and SAP routing protocols operate like any other Windows Sockets application sending and receiving IPX packets.

Routing Table Updates

Based on information received by the routing protocol, the routing protocol updates routes in the Route Table Manager and, based on the best route, the table of best routes is updated in the IPX forwarder driver.

Registry Settings

When the Routing and Remote Access service is enabled, it creates and maintains its settings in the Windows 2000 registry. For performance reasons, most of the Routing and Remote Access service configuration information is stored in binary in large configuration blocks, not as separate registry entries that can easily be viewed and changed. All configuration of the Routing and Remote Access service should be done through the Routing and Remote Access snap-in or through the Netsh command-line utility described later in this chapter.

Routing and Remote Access service and router interface configuration information is stored in HKEY_LOCAL_MACHINE \System \CurrentControlSet \Services \RemoteAccess.

Router component configuration information is stored in HKEY_LOCAL_MACHINE \Software \Microsoft \Router.

Router phone book settings are stored in HKEY_LOCAL_MACHINE \Software \Microsoft \RouterPhonebook.

Routing and Remote Access Service Tools and Facilities

The following utilities and facilities are provided with the Routing and Remote Access service to aid in configuration and amassing information for accounting, auditing, or troubleshooting:

- Routing and Remote Access snap-in
- Netsh command-line tool
- Authentication and accounting logging
- Event logging
- Tracing

Routing and Remote Access Snap-In

The Routing and Remote Access snap-in is available from the Administrative Tools folder and is the primary management utility for configuring Windows 2000 local and remote access servers and routers.

Routing and Remote Access Floating Windows

Within the Routing and Remote Access snap-in is a series of floating windows that display table entries or statistics. Once displayed, a floating window can be moved anywhere on the display and remains on top of the Routing and Remote Access snap-in when the snap-in is the foreground application. Table 2.1 lists the floating windows in the Routing and Remote Access snap-in, and their location.

Table 2.1 Routing and Remote Access Floating Windows

Floating window	Location	Description
TCP/IP information	IP Routing/General IP Routing/General/Interface	Global TCP/IP statistics, such as the number of routes, packets received, and packets forwarded.
Multicast forwarding table	IP Routing/General	The contents of the TCP/IP multicast forwarding table.
Multicast statistics	IP Routing/General	Statistics per group, such as the number of multicast packets received.
Address translations	IP Routing/General/Interface	The contents of the Address Resolution Protocol (ARP) cache.
IP addresses	IP Routing/General/Interface	The IP addresses assigned to routing interfaces.
IP routing table	IP Routing/General/Interface IP Routing/Static Routes	The contents of the IP routing table.
TCP connections	IP Routing/General/Interface	The list of TCP connections, including local and remote addresses and TCP ports.
UDP listener ports	IP Routing/General/Interface	The list of UDP ports on which the router is listening.
Areas	IP Routing/OSPF	The list of configured OSPF areas.

Link state database	IP Routing/OSPF	The contents of the OSPF link state database.
Neighbors (OSPF)	IP Routing/OSPF	The list of neighboring OSPF routers and their state.
Virtual interfaces	IP Routing/OSPF	The list of configured virtual interfaces and their state.
Neighbors (RIP)	IP Routing/RIP	The list of neighboring RIP routers.
DHCP Allocator information	IP Routing/Network Address Translation	Statistics on the number of types of DHCP messages sent and received.
DNS Proxy information	IP Routing/Network Address Translation	Statistics on the number of types of DNS messages sent and received.
Mappings	IP Routing/Network Address Translation/Interface	Contents of the network address translation mapping table.
Group table	IP Routing/IGMP	Global list of groups detected using IGMP routing protocol.
Interface group table	IP Routing/IGMP/Interface	Interface list of groups detected using IGMP routing protocol.
IPX parameters	IPX Routing/General	Global IPX statistics such as the number of routes and services, packets received, and packets forwarded.
IPX routing table	IPX Routing/General IPX Routing/Static Routes	The contents of the IPX routing table.
IPX service table	IPX Routing/General IPX Routing/Static Services	The contents of the SAP service table.
RIP parameters	IPX Routing/RIP for IPX	Global statistics on the RIP for IPX protocol.
SAP parameters	IPX Routing/SAP for IPX	Global statistics on the SAP for IPX protocol.

Netsh Command-Line Tool

Netsh is a command-line and scripting tool for Windows 2000 networking components for local or remote computers. Netsh is supplied with Windows 2000. Netsh also provides the ability to save a configuration script in a text file for archival purposes or for configuring other servers.

Netsh is a shell that can support multiple Windows 2000 components through the addition of Netsh helper DLLs. A Netsh helper DLL extends Netsh functionality by providing additional commands to monitor or configure a specific Windows 2000 networking component. Each Netsh helper DLL provides a context (a group of commands for a specific networking component). Within each context, subcontexts can exist. For example, within the **routing** context, the subcontexts **ip** and **ipx** exist to group IP routing and IPX routing commands together.

Netsh command-line options include the following:

-a AliasFile Specifies that an alias file be used. An alias file contains a list of Netsh commands and an aliased version so that the aliased command line can be used in place of the Netsh command. Alias files can be used to map commands to the appropriate Netsh command that might be more familiar in other platforms.

-c Context Specifies the context of the command corresponding to an installed helper DLL.

Command Specifies the Netsh command to carry out.

-f ScriptFile Specifies that all of the Netsh commands in the file ScriptFile be run.

-r Remote Computer Name or IP Address Specifies that Netsh commands are run on the remote computer specified by its name or IP address.

Commands can be abbreviated to the shortest unambiguous string. For example, issuing the command **ro ip sh int** is equivalent to issuing **routing ip show interface**. Netsh commands can be either global or context specific. Global commands can be issued in any context and are used for general Netsh functions. Context-specific commands vary according to the context.

Table 2.2 lists the netsh global commands.

Table 2.2 Global Netsh Commands

Command	**Description**
..	Moves up one context level.
? or help	Displays command-line Help.
add helper	Add a Netsh helper DLL.
delete helper	Removes a Netsh helper DLL.
show helper	Displays the installed Netsh helper DLLs.
online	Sets the current mode to online.
offline	Sets the current mode to offline.
set mode	Sets the current mode to online or offline.
show mode	Displays the current mode.
flush	Discards any changes in offline mode.
commit	Commits changes made in offline mode.
show machine	Displays the computer on which the Netsh commands are carried out.
exec	Executes a script file containing Netsh commands.
quit or **bye** or **exit**	Exits Netsh.
add alias	Adds an alias to an existing command.
delete alias	Deletes an alias from an existing command.

show alias	Displays all defined aliases.
dump	Writes configuration.
popd	A scripting command that pops a context from the stack.
pushd	A scripting command that pushes the current context on the stack.

Netsh has the following command modes:

- Online

  In online mode, commands issued at a Netsh command prompt are carried out immediately.
- Offline

  In offline mode, commands issued at a Netsh command prompt are accumulated and carried out as a batch by issuing the **commit** global command. Accumulated commands can be discarded by issuing the **flush** global command.

You can also run a script (a text file with a list of Netsh commands) by using either the -**f** command-line option or by issuing the **exec** global command at a Netsh command prompt.

To create a script of the current configuration, use the global **dump** command. The **dump** command generates

the current running configuration in terms of Netsh commands. You can then use the script created by this command to configure a new server or to reconfigure the existing server. If you are making extensive changes to the configuration of a component, it is recommended to begin the configuration session with the **dump** command, in case you need to restore the configuration prior to changes being made.

For the Routing and Remote Access service, Netsh has the following contexts:

- **ras**

  Use commands in the **ras** context to configure remote access configuration.
- **aaaa**

  Use commands in the **aaaa** context to configure the AAAA component used by both Routing and Remote Access and Internet Authentication Service.
- **routing**

  Use commands in the **routing** context to configure IP and IPX routing.
- **interface**

  Use commands in the **interface** context to configure demand-dial interfaces.

For more information about context-specific commands, see Windows 2000 Server Help and the help provided by the Netsh tool.

Authentication and Accounting Logging

The Routing and Remote Access service supports the logging of authentication and accounting information for PPP-based connection attempts when Windows authentication or accounting is enabled. This logging is separate from the events recorded in the system event log. You can use the information that is logged to track remote access usage and authentication attempts. Authentication and accounting logging is especially useful for troubleshooting remote access policy issues. For each authentication attempt, the name of the remote access policy that either accepted or rejected the connection attempt is recorded.

The authentication and accounting information is stored in a configurable log file or files stored in the %*SystemRoot*%\System32 \LogFiles folder. The log files are saved in Internet Authentication Service (IAS) 1.0 or database format, meaning that any database program can read the log file directly for analysis.

You can configure the type of activity to log (accounting or authentication activity) and log file settings from the properties of the Remote Access Logging folder in the Routing and Remote Access snap-in.

If the remote access router is configured for RADIUS authentication or accounting and the RADIUS server is a computer running Windows 2000 and the Internet Authentication Service (IAS), the same information is recorded on the IAS server computer.

Event Logging

The Windows 2000 Router performs extensive error logging in the system event log. You can use information in the event logs to troubleshoot routing or remote access processes.

Four levels of logging are available:

1. Log errors only (the default)
2. Log errors and warnings
3. Log the maximum amount of information
4. Disable event logging

For example, if an OSPF router is unable to establish an adjacency on an interface, you can:

1. Disable OSPF on the interface.
2. Change the level of logging for OSPF to log the maximum amount of information.
3. Enable OSPF on the interface.
4. Examine the system event log for information about the OSPF adjacency process.
5. Change the level of logging for OSPF to log errors only.

You can then troubleshoot the adjacency problem by analyzing the OSPF entries in the system event log.

Setting the level of event logging is available from the **General** tab of the following dialog boxes:

- **IP Routing Properties** and **General Properties**
- **IP Routing Properties** and **Network Address Translation Properties**
- **IP Routing Properties** and **RIP Properties**
- **IP Routing Properties** and **OSPF Properties**
- **IP Routing Properties** and **IGMP Properties**
- **IPX Routing Properties** and **General Properties**
- **IPX Routing Properties** and **RIP for IPX Properties**
- **IPX Routing Properties** and **SAP for IPX Properties**

Logging consumes system resources and should be used sparingly to help identify network problems. After the event has been logged or the problem is identified, you should immediately reset logging to its default value (log errors only).

When logging the maximum amount of information, the logging information can be complex and very detailed. Some of this information is useful only to Microsoft support engineers or to network administrators who are very experienced with the Windows 2000 Routing and Remote Access service.

Tracing

The Windows 2000 Routing and Remote Access service has an extensive tracing capability that you can use to troubleshoot complex network problems. Tracing records internal component variables, function calls, and interactions. Separate routing and remote access components can be independently enabled to log tracing information to files (file tracing). You must enable the tracing function by changing settings in the Windows 2000 registry.

Caution Do not use a registry editor to edit the registry directly unless you have no alternative. The registry editors bypass the standard safeguards provided by administrative tools. These safeguards prevent you from entering conflicting settings or settings that are likely to degrade performance or damage your system. Editing the registry directly can have serious, unexpected consequences that can prevent the system from starting and require that you reinstall Windows 2000. To configure or customize Windows 2000, use the programs in Control Panel or Microsoft Management Console (MMC) whenever possible.

You enable tracing for each routing protocol by setting the registry values described later in this section. You can enable and disable tracing for routing protocols while the router is running. Each installed routing protocol or component is capable of tracing and appears as a key (such as OSPF and RIPV2).

Tracing consumes system resources and should be used sparingly to help identify network problems. After the trace is captured or the problem is identified, you should immediately disable tracing. Do not leave tracing enabled on multiprocessor computers.

The tracing information can be complex and very detailed. Most of the time this information is useful only to Microsoft support engineers or to network administrators who are very experienced with the Windows 2000 Routing and Remote Access service.

File Tracing

To enable file tracing for each component (represented as *Component* below), you must set the value of the **EnableFileTracing** registry entry in HKEY_LOCAL_MACHINE \SYSTEM \SOFTWARE \Microsoft \Tracing*Component* to **1**. The default value is **0**.

To set the location of the trace file for each component, you must set the value of the **FileDirectory** registry entry in HKEY_LOCAL_MACHINE \SYSTEM \SOFTWARE \Microsoft\Tracing\Component. The location of the log file is entered as a path. The file name for the log file is the name of the component for which tracing is enabled. By default, log files are placed in the *systemroot*\Tracing directory.

To set the level of file tracing for each component, you must set the value of the **FileTracingMask** registry entry in HKEY_LOCAL_MACHINE \SYSTEM \SOFTWARE \Microsoft \Tracing*Component*. The tracing level can be from **0** to **0xFFFF0000**. By default, the level of file tracing is set to **0xFFFF0000**, the maximum level of tracing.

To set the maximum size of a log file, you must set the value of the **MaxFileSize** registry entry in HKEY_LOCAL_MACHINE \SYSTEM \SOFTWARE \Microsoft \Tracing *Component*. You can change the size of the log file by setting different values for **MaxFileSize**. The default value is **10000** (64 KB).

Send feedback to Microsoft