Windows 2000 Server

Chapter 5 - Providing Dial-Up Client Access

Microsoft® Windows® 2000 has extensive support for remote access technology to connect remote clients to corporate networks or the Internet. This chapter describes how to deploy dial-up client access solutions, including how to effectively plan, design, and implement Windows 2000 components (such as Routing and Remote Access, Internet Authentication Service (IAS), and Connection Manager) in an enterprise environment to support dial-up solutions for remote clients.

This chapter is intended for network engineers and support professionals who are already familiar with TCP/IP, IP routing, Internetwork Packet Exchange (IPX) routing, Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS), Windows Internet Name Service (WINS), and wide area network (WAN) technology. It assumes that you have read the section about remote access in Microsoft® Windows® 2000 Server Help.

Overview of Dial-Up Client Access

Implementing secure, reliable, and cost-effective remote access solutions that meet enterprise objectives requires understanding how current technologies can be used and how to efficiently implement the technologies in your environment.

Although virtual private network (VPN) connections are increasingly used to meet high-demand and long-distance connection needs, direct dial-up access is still a viable solution for many remote access requirements, especially when implemented with Remote Authentication Dial-In User Service (RADIUS) authentication.

Microsoft® Windows® 2000 Server has features that facilitate the effective implementation of remote client access solutions. In addition to the remote access support provided in Windows 2000 by the Routing and Remote Access service, Windows 2000 Server includes Internet Authentication Service (IAS), which is the Microsoft implementation of RADIUS-compliant authentication and accounting. It also includes Connection Manager components that support delivery of client software that is self-installing and that provides single-click access to users.

Remote Client Connectivity

Remote clients requiring access to a central network generally use one of the following two methods to connect to the network:

- **Direct access using dial-up networking connections**. Dial-up networking is a direct, physical, non-permanent connection between the remote client and the dial-up networking server. Dial-up networking clients connect through a physical port on a network access server (NAS) by using the service of a telecommunications provider, such as analog phone and Integrated Services Digital Network (ISDN).
- **Virtual private network connections over the Internet**. Virtual private networking is the creation of a logical, indirect, secure, connection across a private network or across a public network, such as the Internet. A virtual private network client uses special TCP/IP-based protocols called tunneling protocols to make a virtual call to a virtual port on a virtual private network server. A remote access VPN connection allows data to travel securely across a network using dial-up media, such as analog modems and ISDN, or advanced persistent connection technologies, such as asymmetric digital subscriber line (ADSL) and cable modems.

Dial-Up Client Access Components

Connecting remote users, such as telecommuters or traveling employees, to a central network using dial-up access requires the following components:

- A NAS that links the remote computer to the enterprise network, with the hardware and software required to connect the server to the intranet and WAN, including an authentication system that validates remote users and manages network access.
- A dial-up client with valid user credentials and a computer with a modem, and client software to support a dial-up connection.

Figure 5.1 shows components of a basic dial-up client access solution, where authentication is managed through NASs.

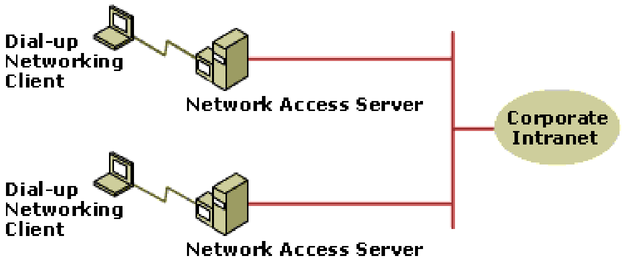


Figure 5.1 Basic dial-up networking components

Some solutions require only one server to handle dial-up connections. Others require more sophisticated solutions, with a complex network of VPN servers, direct-dial network access boxes, centralized RADIUS authentication servers, smart cards, and authentication systems based on public key infrastructure (PKI). This chapter covers basic dial-up networking and RADIUS solutions. For more information about VPNs and expanded security components (such as certificate services) see "Expanding and Securing Remote Client Access."

RADIUS Client-Server

Remote access solutions, especially in large enterprises, can be challenging to manage. RADIUS is an Internet Engineering Task Force (IETF) standard protocol for providing centralized user authorization, authentication, and accounting services for remote access networks based on Point-to-Point Protocol (PPP). RADIUS is supported on a variety of operating systems and hardware platforms and, when integrated with a remote access solution, RADIUS can provide better manageability, interoperability, and security than non-RADIUS remote access solutions.

In addition to the dial-up networking client, RADIUS solutions require the following:

- **A RADIUS client.** This is a NAS that receives access requests from remote access clients and uses the RADIUS protocol to send RADIUS authentication and accounting requests to one or more RADIUS authentication servers.
- **A RADIUS server.** This is a server using the RADIUS protocol to process RADIUS authentication and accounting information from RADIUS clients, including validating the client request and storing the accounting information in log files. The RADIUS server provides support for centralized remote access authentication, authorization, accounting, and auditing. A RADIUS server is independent of the platform or operating system of the RADIUS client.

RADIUS supports both dial-up and VPN connections. Figure 5.2 shows the basic components of a dial-up solution using RADIUS to centrally manage authorization, authentication, and accounting.

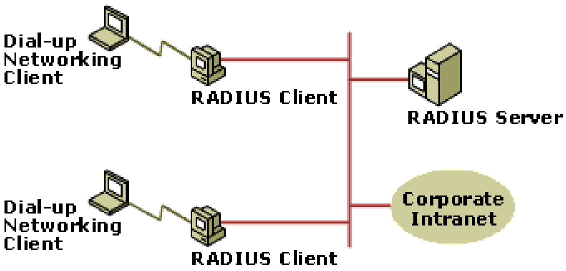


Figure 5.2 Dial-up networking components for a RADIUS solution

Planning Dial-Up Client Access Solutions

Planning is critical to the deployment of any remote access solution. The information in this section covers how to plan effectively for deployment of a dial-up client access solution, including:

- Analyzing your user, business, and IT requirements for dial-up client access.
- Assessing dial-up client access solutions.
- Planning a dial-up deployment project.

Analyzing Dial-Up Client Access Requirements

Dial-up client access can provide secure, cost-effective, and manageable remote access for many types of users. But some remote access requirements can be met more effectively by other remote access solutions, such as VPN connections, so you should analyze all remote access requirements and objectives before selecting any single solution. These business, user, and IT requirements along with your enterprise's objectives are critical for planning, designing, and implementing the right solutions.

After analyzing your requirements and objectives, you should consider deploying dial-up solutions if:

- Users, such as telecommuters and sales personnel, require regular remote connectivity from locations in the local calling area.
- Users have limited mobility requirements (only occasional requirements for access from non-local locations).
- Use of the Internet as a mechanism for accessing intranet-based resources is not possible because it cannot be implemented securely in the existing enterprise environment.
- Variability of the data throughput rate for an Internet connection is insufficient to support client needs.
- Cost of providing phone lines, modems, and multiport communication adapters is not prohibitive.

Although dial-up solutions are still a high-demand solution, they are increasingly being replaced with VPN solutions.

Assessing Windows 2000 Dial-Up Client Access Solutions

Windows 2000 includes extensive features and functionality that can provide integrated, end-to-end remote access solutions for a wide range of users. Solutions using Windows 2000 components can simplify deployment, can preserve investments in existing networking components, and can provide remote access connections that parallel the in-office network experience.

Use the information in this section along with your own analysis of requirements to determine how your objectives can be met using Windows 2000. Many of the Windows 2000 components that support dial-up client access can also be used to provide VPN access and remote site connectivity. These solutions can provide:

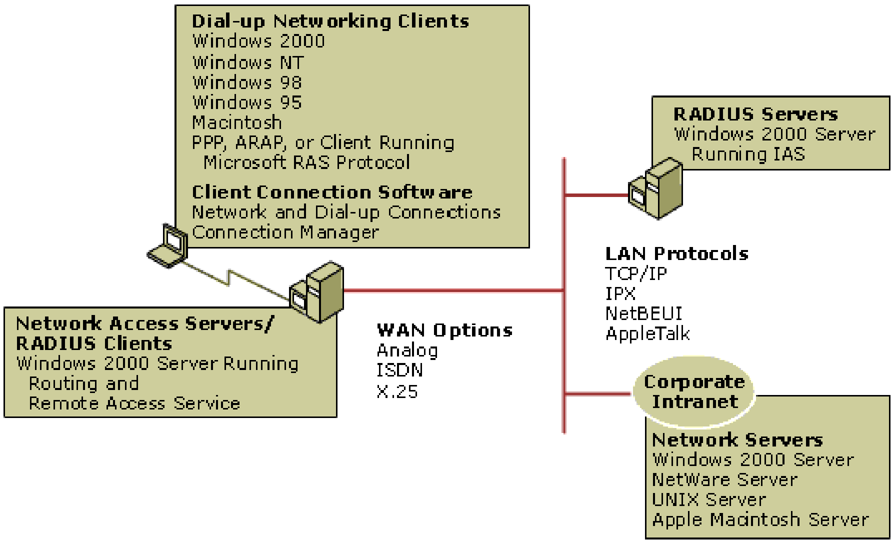
- Backward compatibility and full interoperability with other standards-based remote access solutions.
- Interoperability with an extensive set of third-party networking components.
- Improved scalability of remote access connections.
- Efficient integration of diverse NASs.
- Automated scheduling of routine replications and updates for minimum network activity periods.
- Reductions in total cost of ownership (TCO) by reducing overhead, improving productivity, increasing availability, and centralizing administration.

Windows 2000 Server components work together to provide integrated and seamless support for your dial-up and other remote access needs. Windows 2000 dial-up networking support includes:

- **Dial-up networking servers**. A remote access server that is running Windows 2000 Server can be configured to provide dial-up networking access to an entire network, or to restrict access to the shared resources of the remote access server.
- **Dial-up networking clients**. Remote access clients that are running Windows 2000, Microsoft® Windows NT®, WindowsMe®, Microsoft® Windows® 98, Microsoft® Windows® 95, Microsoft® Windows® for Workgroups, Microsoft® MS-DOS®, Microsoft® LAN Manager (dial-up networking or remote access), and Apple Macintosh can all connect to a remote access server running Windows 2000 Server. You can create custom dial-up software and phone books that simplify the user connection process.
- **Local area network (LAN) and remote access protocols**. Application programs use LAN protocols to transport information. Remote access protocols are used to negotiate connections and provide framing for LAN protocol data that is sent over WAN links. Windows 2000 Server supports LAN protocols such as TCP/IP, IPX, AppleTalk, and NetBEUI, which enable access to the Internet, UNIX, Apple Macintosh, Novell NetWare, and Windows resources. Windows 2000 Server supports remote access protocols such as PPP and the Microsoft RAS Protocol (NetBEUI only).
- **WAN options**. Clients can dial in by using standard analog telephone lines and a modem or modem pool. Faster links are possible by using ISDN or other broadband. You can also connect remote access clients to remote access servers by using X.25 or asynchronous transfer mode (ATM) connections through a direct connection, such as a digital subscriber line (DSL) or cable modem, or through an ATM on-demand connection. The Routing and Remote Access service supports PPP connections over switched virtual circuit (SVC) or permanent virtual circuit (PVC) ATM connections. For more information about ATM connections, see "Connecting Remote Sites."
- **Security options**. Windows 2000 Server logon and domain security, support for security hosts, data encryption, RADIUS, smart cards, remote access policies, and callback provide secure network access for dial-up clients.

Implementing Windows 2000 Server with the Routing and Remote Access, Internet Authentication Service (IAS), and Connection Manager components provides extensive functionality, performance, availability, security, and management support for remote access. Use the information in this section to determine whether these components are appropriate for your remote access needs.

Figure 5.3 provides an overview of the primary support provided by Windows 2000 for dial-up networking solutions.


Dial-up Networking Clients
Windows 2000
Windows NT
Windows 98
Windows 95
Macintosh
PPP, ARAP, or Client Running Microsoft RAS Protocol
Client Connection Software
Network and Dial-up Connections
Connection Manager
RADIUS Servers
Windows 2000 Server Running IAS
LAN Protocols
TCP/IP
IPX
NetBEUI
AppleTalk
Network Access Servers/ RADIUS Clients
Windows 2000 Server Running Routing and Remote Access Service
WAN Options
Analog
ISDN
X.25
Corporate Intranet
Network Servers
Windows 2000 Server
NetWare Server
UNIX Server
Apple Macintosh Server

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

Figure 5.3 Windows 2000 Support for Dial-Up Networking Solutions

The following information describes key components provided by Windows 2000 for providing remote access, especially dial-up client access. Use this information to determine how Windows 2000 can meet your dial-up client access requirements. If you have requirements that are not met by the functions and features described in this chapter, you may want to consider expanding your remote access solution to include virtual private networking and additional security features, such as certificate services and filtering. For more information about the support provided in Windows 2000 for these additional remote access functions and features, see "Expanding and Security Remote Access."

Network Access Servers

The integrated Routing and Remote Access service of Windows 2000 Server acts as a foundation for the NAS. Many enterprises have existing remote access infrastructures that they want to preserve and expand upon. Regardless of the situation, virtually every enterprise will centrally manage remote access policies based on the groups of users defined in their enterprise-wide user directory. The Routing and Remote Access service of Windows 2000 Server lets you accomplish this in several ways, including:

- Supporting the use of password-based authentication methods, including (password authentication protocol) PAP, Challenge Handshake Authentication Protocol (CHAP), or Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) implementations, as well as the standards-based Extensible Authentication Protocol (EAP), which supports the addition of modules that support new authentication methods and emerging technologies, including smart cards and biometric devices.
- Authenticating directly with the Active Directory^{TM} directory service, so it does not require a separate user database and provides centralized authentication support for Windows and RADIUS remote access solutions.
- Using the RADIUS protocol to forward authentication requests to a RADIUS server that can validate users on a user directory that is not part of a Windows operating system (such as a NetWare or UNIX user directory).
- Defining remote access policies specific to individual user groups, based on the characteristics and requirements of each group, including authentication and encryption methods, connection types, security group, and time-and-day restrictions. A remote access policy is a set of conditions and connection settings that, combined with the dial-in properties of the user account, defines remote access permissions and usage for the users to whom the policy applies. Remote access policies provide network administrators flexibility in authorizing connection attempts.

Consider deploying Windows 2000 Server and Routing and Remote Access service to create reliable, secure, and scalable dial-up solutions if your remote access requirements indicate the need for:

- Both IP and IPX protocols.
- Various interface types and integration of dial-up modems, ISDN, ADSL, T1, T3, and/or Synchronous Optical Network (SONET).
- Dial-up and/or VPN connections.
- Multilink connections, logical connections that consist of multiple physical connections, such as ISDN connections (with or without dynamic allocation of bandwidth across the connections).
- Secure authentication and encryption methods.
- Security features such as caller ID verification and callback support.
- Per session route filters that can control which network resources dial-up clients can access.
- Certificate services, supporting the implementation of extremely secure solutions using technology such as smart cards.
- Diverse client support:
  - PPP connections that use TCP/IP, IPX, NetBEUI, or AppleTalk.
  - Microsoft RAS Protocol clients, including Microsoft® Windows NT® version 3.1, Windows for Workgroups, MS-DOS, and LAN Manager clients (to use the remote access NetBIOS gateway to access NetBIOS-based resources by using NetBIOS over TCP/IP, NetBIOS over IPX, or NetBEUI across the remote connection).
  - Integrated Windows 2000 Server networking services (including DHCP, DNS, WINS, RADIUS, and Active Directory) that support dynamic allocation of addresses for remote access connections and central administration of remote access users.
  - NASs that can integrate with an existing third-party authentication infrastructure, such as a token-card authentication system.

    Note A remote access server running Windows 2000 Server does not support Serial Line Internet Protocol (SLIP) clients.

For additional information about Windows 2000 support for dial-up networking clients and incoming connection clients, see Windows 2000 Server Help.

RADIUS Support

Internet Authentication Service (IAS) is a component of Windows 2000 Server that implements RADIUS server. Benefits of deploying

IAS include:

- Centralized remote access authentication, authorization, accounting, and auditing of remote access servers.
- Support for Windows 2000 remote access servers and existing NASs.
- Support for the same protocols and authorization methods as Routing and Remote Access service.

Consider implementing IAS with RADIUS clients to support remote client access connections in any homogenous or heterogeneous networking environments if you need:

- Centralized management of authentication and authorization for multiple NASs in your enterprise (whether homogenous or heterogeneous).
- High availability and performance from your remote access solutions.
- A highly scalable design for your remote access infrastructure.
- Standards-based solutions for security and authentication.
- RADIUS support for existing NASs.

Dial-Up Client Connection Software

Connection Manager components are the optional Windows 2000 Server components for creating and supporting centrally managed client software. These components provide the tools needed to provide turnkey client software to users. These Connection Manager components include:

- **Connection Manager Administration Kit (CMAK)**. CMAK provides a wizard that simplifies the creation of custom service profiles. A service profile provides self-extracting, branded client software that can usually be automatically installed and run by users with nothing required from them except the selection of an access number.
- **Connection Point Services**. The Phone Book Administrator (PBA) and Phone Book Service (PBS) of Connection Point Services (CPS) work with Connection Manager to provide an effective method of creating, maintaining, and automatically updating phone books that contain the access numbers for all remote locations and users.

Connection Manager service profiles build on the functionality of the Networking and Dial-Up Connections, but they also support additional customizable features that further simplify and enhance implementation of custom remote connection support.

Consider implementing Connection Manager client software with CPS phone book support for your remote access solutions if you require:

- A pre-configured, turnkey solution that provides single-click access to your network.
- Branding, including custom graphics and information that reflects specific enterprise or group identities.
- Transparent roaming support for users requiring multiple points of presence (POPs) through which users can access the central network.
- An automated method of updating and delivering access numbers to users.
- Multiple phone books hosted on a single server.
- Multiple remote access solutions (such as dial-up and VPN, including ADSL support for VPN connections) or multiple versions of client software, each tailored to the requirements of a specific user group.
- Automatic launching and closing of resident applications during connections (for example, uploading and downloading routine information).
- Multiple users on a single computer (using different credentials).
- Centrally managed client solutions, including phone books.
- Support for a variety of Windows operating systems (using a single client software package).
- Outsourced support for client connections.
- Easy distribution.

Users can create their own Networking and Dial-Up Connection instead of using Connection Manager. However, the functionality and ease-of-use of Connection Manager make it the preferred solution for most remote access requirements. Use Networking and Dial-Up Connections instead of Connection Manager if your remote access solution requires:

- Support for callback, since Connection Manager does not support callback.
- Support for non-PPP connections.
- Support for X.25 connections.
- Support for terminal windows that cannot be addressed using a Connection Manager connect action or a dial-up script. Connection Manager does not support terminal windows directly.
- Support for dynamic bandwidth control for Multilink, using Bandwidth Allocation Protocol (BAP) and Bandwidth Allocation Control Protocol (BACP).

For more information about CMAK and Connection Point Services, see Windows 2000 Server Help.

Dial-Up Client Operating Systems

In addition to the dial-up networking support covered earlier in this chapter (such as protocol support, WAN connection options, and support for secure connections) Windows 2000 clients provide enhanced security and functionality. The benefits of deploying Windows 2000 for remote access clients include support for:

- Simplified setup of network and dial-up connections.
- Advanced authentication methods, such as EAP.
- Bandwidth allocation for multilink connections.
- Strong (128-bit) encryption.
- Layer Two Tunneling Protocol (L2TP) for VPN connections.

Consider using Windows 2000 clients if:

- Clients need to automatically connect to NASs. The autodial feature of Windows 2000 learns every connection made over the remote access link and automatically reconnects when the client accesses a resource for the second time.
- You want to automate the connection process for Windows 2000 clients by using a simple batch file and the **rasdial** command or by using a custom Windows NT and Windows 2000 application that recognizes remote access.
- You want to implement Connection Manager features that are not supported by other operating systems, such as EAP.

- You plan to implement L2TP as part of a VPN solution.
- Remote access clients require access to Shiva LAN Rover, Novell NetWare Connect, Serial Line Internet Protocol (SLIP), or other PPP-based communications servers.

  Note Although Windows 2000 Server does not support SLIP connections, remote access clients running Windows 2000 do support SLIP and can connect to any remote access server using the SLIP standard. This permits Microsoft® Windows NT® version 3.5 or later clients to connect to the large installed base of UNIX servers. Clients can use SLIP only if the port for the phone book entry is a serial COM port. In order to provide TCP/IP-based remote access, the TCP/IP protocol must be installed on the remote access computer.

If running other operating systems, verify in advance that they support all requirements and that they are configured appropriately for use with Windows 2000 Server. In addition to the potential reduced functionality supported in client operating systems other than Windows 2000 Server, interoperability and other limitations might exist. A remote access client running Windows NT 3.1 or Windows for Workgroups must use the NetBEUI protocol. The Windows 2000 remote access server then acts as a NetBIOS gateway for the remote client.

Remote Access Project Planning

The *Microsoft® Windows® 2000 Server Resource Kit Deployment Planning Guide* contains information about creating project plans for Windows 2000 Server deployment. Your project plan should define the components of your remote access solution and the extent of the changes required to implement the solution. When doing project planning for remote access, it is recommended that you:

- Include representatives, including security personnel, from all sites involved in server-side and client-side implementation of the solutions to ensure that geographic and site-specific constraints are addressed.
- Ensure that your cost analysis includes all remote resources. This includes equipment required for home offices, insurance appropriate to remote environments, and replacement costs for damaged or stolen equipment in non-secured environments.

Designing the Dial-Up Client Access Infrastructure

Your remote access plans should provide the information needed to translate your organization's remote access needs into network designs. After completing the design, you should have identified and tested server placement, routing, protocols, policies, and the other infrastructure components needed to deploy your dial-up access solution.

To design a dial-up client access infrastructure that meets the needs of your environment, you need to:

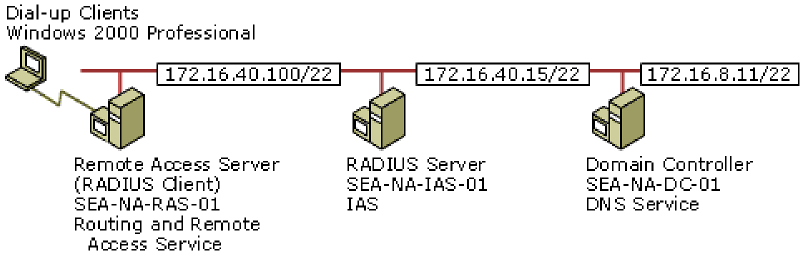
- Design the network infrastructure showing the physical layout for your dial-up client access solution.
- Develop server specifications for your dial-up client access components.
- Develop client-side specifications for your dial-up clients.
- Identify tools required to support implementation.
- Test your design and use the results to refine your dial-up access solution.

Use the information in this section to design your Routing and Remote Access and IAS solution.

Designing the Network Infrastructure

Your network design should identify equipment makes and models, resident programs, IP addresses, domain machine names, locations, and connections for all essential hardware and software components.

Figure 5.4 shows a sample network diagram containing initial network information. The information in this figure is based on the scenario covered at the end of this chapter.



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

Figure 5.4 Dial-up network infrastructure

To complete the network diagram, additional information should be added (either directly in the diagram or in tables attached to the diagram), including hardware platforms, WAN and LAN connections, subnet masks, gateways, and any information required to clarify the location of servers and relationships to other components and networks.

Defining WAN Connections

Windows 2000 Server supports a variety of analog and digital WAN connections. Select the method that is most appropriate for your user requirements. Table 5.1 shows the network and dial-up connection types that Windows 2000 Server supports.

Table 5.1 Windows 2000 Server WAN Connections

Connection Type	Communication Method	Example
Dial-up connections	Modem, ISDN, X.25 (Connection Manager supports only modem and ISDN).	Connect to a corporate network or the Internet by using remote access.
Local area connections	Ethernet, Token Ring, cable modem, DSL, Fiber Distributed Data Interface (FDDI), IP over ATM, Infrared Data Association (IrDA), wireless, WAN technologies (T1, Frame Relay).	Connect typical enterprise user.
VPN connections	Point-to-Point Tunneling Protocol (PPTP) or L2TP over IP Security (IPSec) VPN connections.	Connect securely to an enterprise network over the Internet.
Direct connections	Serial cabling, infrared link, DirectParallel	Synchronize information between a Handheld PC

	cable.	that is running Microsoft® Windows® CE and a desktop computer.
Incoming connections	Dial-up or VPN connections.	Receive a call or direct a connection (such as a DSL or cable mode connection) to a remote access server.

In addition, each server-side modem requires a serial port on the remote access server. For multiple modems (modem banks), use a multi-port serial adapter or a high-density combination card. Multi-port serial adapters allow connection of a large number of analog modems or ISDN modems to one remote access server. With a multi-port serial adapter, you can install one Peripheral Component Interconnect (PCI) or ISA card in your computer and create a large number of serial ports (4, 8, 16, 64, etc.) for your modems. A high-density combination card combines multiple modems and serial adapters into one device.

For dial-up connections, specify that ports must support inbound remote access connections only.

Specify the following for each LAN adapter:

- IP address and subnet mask assigned from the network administrator
- Default gateway of a local router
- DNS and WINS name servers of corporate intranet name servers

On your network diagram, indicate the names and IP addresses of servers and routers that are required to support your dial-up access solution.

Defining Servers

The type, number, and location of servers deployed to support your remote client access solution can impact availability, performance, and reliability. This section provides recommendations on effective deployment of the IAS servers, remote access servers, and other servers supporting remote access.

IAS Servers

In many cases, the IAS server can be installed on the same computer as the domain controller. High-latency connections between servers can negatively impact authentication times, causing retries and time-outs. Some of the most common factors that affect IAS performance are:

- Not installing IAS as a dedicated RADIUS server.
- Network latency between the IAS server computer and the domain controller.
- Network latency between the IAS server computer and the global catalog computer.
- Network latency between IAS and the NAS.
- Performance and the current load of the domain controller computer.
- The resolution of user principal names, resulting in an additional remote procedure call (RPC) query against the global catalog computer.
- EAP-based authentication methods, involving multiple challenge-response exchanges.
- The number of user accounts in the domain.
- Inappropriate hardware.

  Note Although recommended for performance reasons, IAS does not have to be installed on the same computer as a domain controller. If installed on a separate computer, IAS performs authentications of remote access user credentials and accesses dial-in properties of user accounts using a secured communication channel to a local domain controller.

IAS can scale to large numbers of accounts and authentications per second. Table 5.2 shows how IAS can scale using faster hardware.

Table 5.2 IAS Performance Scaling

Type of Organization	Authentications Per Second for Typical Use	Hardware Configuration
Small to medium-sized organizations with less than 1,000 users	1	Minimum hardware recommended for Windows 2000 Server
Large organizations with 50,000 users	10	Minimum hardware recommended for Windows 2000 Server
ISPs with 2 million users	50	200 MHz Pentium II or higher
ISPs with 20 million users	300	4-processor Xeon or higher

Table 5.3 lists performance numbers that can be used as guidelines for the throughput of a single IAS server.

Table 5.3 Maximum Authentication Rates

Hardware	Authentication Methods	Maximum Authentications Per Second
Minimum Windows 2000 Server recommended hardware and a remote Active Directory domain controller	CHAP, MS-CHAP v1, MS-CHAP v2	50
200 MHz Pentium II and a remote Active Directory domain controller	CHAP, MS-CHAP v1, MS-CHAP v2	200
4-processor Xeon and a remote Active Directory domain controller	CHAP, MS-CHAP v1, MS-CHAP v2	700

For redundancy, use multiple RADIUS clients and servers, so that the configuration you specify ensures that all clients and servers are known to each other.

In very large environments (such as an ISP with millions of remote access users and extremely heavy load conditions), where a large number of both authentication requests and accounting packets are being handled per second, consider:

- Using a faster domain controller to yield better throughput.
- Using separate IAS servers for authentication and accounting.
- Running the IAS server on a domain controller with a global catalog (to minimize latency and improve throughput.)

- Increasing the number of concurrent authentication calls in progress at one time between the IAS server and the domain controller (to achieve better throughput) by using the MaxConcurrentApi registry entry.
- Deploying multiple IAS servers and using an IP load balancing scheme to point NASs to a single IP address that represents a pool of IAS servers (if EAP works with your load-balancing scheme).

To ensure that your IAS servers provide the appropriate level of support, do the following:

- Ensure that the user accounts are available for authentication by making certain that all redundant IAS servers use the same user account authentication database.
- Ensure proper authentication and accounting by specifying that RADIUS clients use the redundant IAS servers to ensure proper authentication and accounting.
- Register the redundant RADIUS clients with the IAS servers to ensure proper authentication and accounting.

To further optimize the availability and performance of your RADIUS design, you can use Network Load Balancing (available on Windows 2000 Advanced Server) to distribute TCP/IP traffic between multiple servers. Network Load Balancing, however, cannot be used if you use the EAP authentication protocol.

Guideline If IAS authenticates users against a Windows 2000 Server-based domain controller that is running in native mode, the domain controller should also contain the global catalog.

To help protect your network, implement the following security measures:

- Install IAS on a computer dedicated solely as a RADIUS server
- Physically secure the computer with a key switch on the power switch
- Restrict physical access to the computer

Remote Access Servers

If you have one or more user groups that have high-priority access requirements, consider defining separate remote access servers for these user groups.

Remote access solutions with redundant servers can provide higher availability for both remote access clients. In instances where degradation of service is not a critical issue, you can use your primary remote access servers as backups for each other. If service degradation is not acceptable (if a remote access server becomes unavailable), provide redundancy by defining an extra server to provide failure protection.

Server Addresses

You can specify the address for RADIUS clients by IP address or DNS name.

- **Specifying a RADIUS client by IP address**. It is recommended that all servers are specified by IP address because IAS does not need to resolve host names at startup. As a result, IAS will start much more quickly than if you used DNS names, especially if your network contains a large number of RADIUS clients. Also, you won't need to have a name server available when IAS starts.
- **Specifying a RADIUS client by DNS name**. Use DNS names to specify RADIUS clients only if you want more than your usual administrative flexibility; for example, if you want to map multiple IP addresses of RADIUS clients to a single DNS name.

Server Logistics

The placement of a remote access server in a network can affect the delivery of data to remote access clients. It can also affect the data traffic flowing to other users on the network.

Subnet

Position the remote access server in a subnet or on the segment with the most client-accessible resources if:

- **There is a switched non-routed LAN with multiple physical segments**. This position minimizes unicast traffic flowing across segments, as the switch does not reflect traffic onto all segments.
- **There is a routed network with multiple routers**. Position the remote access server to minimize cross-subnet traffic. This position minimizes the effect of client data on the bandwidth available to other network users.

The data for all dial-up clients passes through the remote access server interface connected to the private network. Even when the client data speeds are moderate, the aggregate throughput resulting from this concentration can be significant. In any design, minimize the routed path to the resources that are used by the dial-up clients. Minimizing the routed path reduces both the client traffic delays, and the interaction of dial-up client traffic and normal network user traffic.

For example, consider a remote access server with 128*56 kilobits per second (Kbps) V.90 modems. If you assume the following conditions:

- At peak times all lines will be used.
- A multimedia training application is running on the remote access clients, requiring sustained throughput of 38 Kbps from server to client.

The aggregate bandwidth required will be:

38Kbps * 128 = 4.864 megabits per second (Mbps)

The simplified throughput calculation shows that the remote access server would use 49 percent of the available bandwidth on a 10 Mbps Ethernet segment. The LAN traffic of other network users would increase this usage further and might make it impossible to service the dial-up clients' multimedia needs. A possible solution in this example is to move the multimedia files onto the remote access server so that network access is not required.

Perimeter Network

Position the remote access server in a perimeter network (also known as a demilitarized zone, DMZ, or a screened subnet) if:

- Corporate policies state that client access must be processed by a firewall or filter.
- Clients use a VPN connection to connect to the private network.
- The remote access server contains other data made available to the public networks.
- The majority of client resources exist in the perimeter network.

Single Segment LAN

Position the remote access server based solely on physical network requirements if:

- There is a single segment, non-switched LAN.
- Clients are allowed to access only the remote access server resources.

Server Optimization

To maximize the efficiency of the remote access servers, do the following:

- For remote access clients, assign primary and backup telephone numbers that connect to different remote access servers.
- Add remote access servers.
- Upgrade the hardware resources of existing remote access servers.
- Replace existing remote access servers with higher performance servers.
- Upgrade to intelligent communications adapters (multiport serial boards) to offload processing from the remote access server.

  Note If a remote access server is also providing resources for remote access clients, the performance of the disk subsystems might become a limiting factor. Under these circumstances, the disk subsystem can be improved by using redundant array of independent disks (RAID).

Phone Book Service Server

To provide maximum administrative flexibility, install the Connection Point Services (CPS) Phone Book Service (PBS), which Connection Manager clients use to obtain phone book updates, on a separate machine other than Phone Book Administrator (PBA), which is used to maintain and update the access numbers posted to the PBS server. To determine how many PBS servers are needed (excluding redundant servers), calculate the average number of logons that your network receives during peak hours for one week. Table 5.4 shows the approximate number of hits the listed processors are capable of handling on a dedicated server with 128 MB of RAM.

Table 5.4 PBS Server Capacities

Processor	Hits Per Second	Hits Per Hour	Hits Per Day
Pentium II 350 MHz	70	250,000	6,000,000
Pentium II 300 MHz	60	215,000	5,160,000
Pentium II 233 MHz	50	130,000	4,320,000

Designing the IP Infrastructure

Creating a server-side infrastructure for your Windows 2000-based remote access solution requires determining how routing, addressing, and DHCP are to be used. When defining how these are to be handled, give careful consideration to how these elements can be best integrated with the existing network infrastructure.

IP Routing and Address Assignment

You can restrict access to private network resources by configuring how IP routing is handled for remote access connections. By default the forwarding of IP packets from one routing interface to another is enabled on the server and is required in order for LAN and demand-dial routing to occur. This allows IP-based remote access clients to access the entire network to which this server is attached. If IP-based remote access clients are to access this server only, IP routing must be disabled.

Each remote computer that connects to a remote access server running Windows 2000 Server through PPP on a TCP/IP network is automatically provided with an IP address during the Internet Protocol Control Protocol (IPCP) negotiation portion of the PPP connection establishment process. The remote access server obtains the IP addresses that are allocated to incoming remote access clients either from a DHCP server or from a static range of IP addresses. The remote access server can assign IP address by using:

- **DHCP leases**, which specifies that the server uses DHCP to obtain IP addresses assigned to TCP/IP-based remote access and demand-dial connections. When the remote access server is configured to use DHCP to obtain IP addresses, the DHCP server obtains 10 IP addresses from a DHCP server. The remote access server uses the first IP address obtained from DHCP for itself and allocates subsequent addresses to TCP/IP-based remote access clients as they connect. IP addresses that are freed when remote access clients disconnect are reused. When all 10 IP addresses are used, the remote access server obtains 10 more. When the Routing and Remote Access service is stopped, all IP addresses obtained through DHCP are released. If a DHCP server is not available when the Routing and Remote Access service is started, then Automatic Private IP Addressing (APIPA) addresses in the range from 169.254.0.1 through 169.254.255.254 are used.

  The remote access server uses a specific LAN interface to obtain DHCP-allocated IP addresses for remote access clients. For each remote access server, specify which adapter you want to use to obtain DHCP, DNS, and WINS addresses for dial-up clients. By default, the Routing and Remote Access service randomly picks a LAN interface to use. For a remote access server with multiple adapters, you should select the adapter that is connected to a network segment where DHCP-allocated addresses can be obtained. For more information about how to specify properties of the remote access server, see Windows 2000 Server Help.

- **Static address pool**, which specifies that the server use a configured range of IP addresses. If you specify one or more static IP address pools, then you need to ensure that the ranges of IP addresses in the remote access IP address pool are not assigned to other TCP/IP nodes either statically or through DHCP.

  If the static IP address pool consists of ranges of IP addresses that are for a separate subnet, then you need to either enable an IP routing protocol on the remote access server computer or add static IP routes consisting of the {IP Address, Mask} of each range to the routers of the intranet. Otherwise, remote access clients cannot receive traffic from resources on the intranet.

  Guideline If you use a DHCP server, configure the remote access server to use DHCP to obtain IP addresses for remote access clients. If you do not use a DHCP server, configure the remote access server with a static IP address pool that is a subset of the range of addresses of the subnet to which the remote access server is attached.

  If the IAS server computer is multihomed, you might need to add persistent static IP routes to the routing table of the IAS server. This prevents the NAS from discarding unrecognized messages when the Access-Accept message is returned using a different network adapter than the one on which the Access-Request message was received.

  When you use a computer running Windows 2000 Server as a remote access server, then remote access clients are assigned an IPX network ID. By default, the remote access server automatically chooses a unique IPX network ID. You can specify an IPX network ID or range of IPX network IDs so that remote access IPX traffic is identified by its source IPX network address. Set up the remote access server to automatically allocate the same IPX network ID to all remote access clients.

After you have defined how server-level IP routing and server-level address management are handled, you can further define IP handling individually for each remote access profile to specify:

- The IP address assignment policy
- Any IP packet filters to be applied during a remote access connection

For more information about IP routing and address management in remote access policies, see "Developing Specifications for Dial-Up Client Access" later in this chapter.

DHCP Relay Agents

For each IP network segment that contains DHCP clients, either a DHCP server or a computer acting as a DHCP Relay Agent is required for each remote access server and router. Remote access clients do not use DHCP to obtain IP addresses for the remote access connection. However, remote access clients running Windows 2000 do use the DHCPINFORM message to obtain DNS server IP addresses, WINS server IP addresses, and a DNS domain name.

If you use DHCP to obtain IP addresses for remote access clients, configure the DHCP Relay Agent on the remote access server with the **Internal** interface, representing all remote access clients.

If the remote access server is using a static IP address pool to obtain IP addresses for remote access clients, then you must configure the DHCP Relay Agent with the IP address of at least one DHCP server. Otherwise, DHCPINFORM messages sent by remote access clients are silently discarded by the remote access server.

Note If you specify TCP/IP filtering for Network and Dial-Up Connections or IP packet filters for the Routing and Remote Access service, ensure that it does not prevent the sending or receiving of DHCP traffic. The DHCP server needs to be reachable, so the firewall must allow access. DHCP traffic uses the User Datagram Protocol (UDP) ports of 67 and 68 so your firewall filtering strategy needs to include appropriate specifications for this support.

Developing Specifications for Dial-Up Client Access

In designing the infrastructure for your dial-up access solution, you should consider the following when developing your specifications:

- User accounts that have remote access.
- Locations from which users will be connecting.
- Maximum number of simultaneous user connections required.
- Types of resources to which the clients require access (local, remote, or both).
- Remote access policy restrictions that apply to a user or a group of users.
- Connection technologies and throughput requirements.
- Client authentication, security, and encryption requirements.
- Client connection protocols.
- Routing requirements.

The requirements, objectives, and solutions identified during the planning process are the basis for making all of the design decisions. The information covered in this section can help you to ensure that all required implementation decisions are addressed and that your design is complete before implementing.

Note The information in this chapter focuses on infrastructure design for RADIUS-based solutions using Routing and Remote Access service and IAS.

Identifying the Administrative Model for Remote Access Authorization

In Windows NT 3.5 and Microsoft® Windows NT® 4.0, authorization was based on a simple **Grant dial-in permission to user** option in User Manager or the Remote Access Admin utility. Callback options were also configured on a per-user basis.

In Windows 2000 Server, authorization is granted based on the dial-in properties of a user account *and* based on remote access policies. Determining the administrative model for implementing remote access permissions is one of the most important decisions to make when deploying a Windows 2000 remote access solution.

In Windows 2000 Server, there are three primary models for administering remote access permissions and connection settings. These models are:

- Restrict access by user
- Restrict access by policy in a Windows 2000 Server native-mode domain
- Restrict access by policy in a Windows 2000 Server mixed-mode domain

In each of these models, authorization can be based on one of three options:

- Explicitly allow access, which authorizes a connection based on the user account permission and specific criteria.
- Explicitly deny access, which denies connections by specific user accounts permission or specific criteria.
- Implicitly deny access, which denies a connection attempt if a user account is not found or if the connection attempt does not match specific criteria.

The way in which you configure these options is dependent on which administrative model you implement. The administrative model for authorization is determined by the Windows 2000 migration and upgrade plans for your enterprise. Some of the remote access features and functionality supported by Windows 2000 are available only in Windows 2000 Server native-mode domain, so the remote access permissions should be carefully designed and defined before you start implementation. These restrictions are summarized in this section and noted throughout this chapter where they affect specific deployment options.

Note The administrative models described here are the recommended ways of controlling remote access. You can administer remote access through a mixture of these models. However, be careful to ensure appropriate enforcement of access restrictions and permissions.

For more information about how to implement administrative models for remote access authorization, see "Internet Authentication Service" in the *Microsoft® Windows® 2000 Server Resource Kit Internetworking Guide*.

Access by User

In the access-by-user administrative model, remote access permissions are determined by the permissions on the **Dial-in** tab of the user account. You can use the access-by-user administrative model:

- On a stand-alone remote access server.
- On a remote access server that is a member of a Windows 2000 Server native-mode domain.
- On a remote access server that is a member of a Windows 2000 Server mixed-mode domain.
- On a remote access server that is a member of a Windows NT 4.0 domain.
- If you have Windows NT 4.0 RAS or IAS servers.

This model is used primarily for support where Windows 2000 Server native-mode or mixed-mode domains are not yet deployed.

Using dial-in user account properties, the following authentication features are available for granting remote access permissions to an IAS server on a Windows 2000 stand-alone server:

- Remote access permission (allow access, deny access, and control access through remote access policy)
- Caller ID
- Callback options
- Static IP address

- Static routes

These properties can be administered through the Network and Dial-Up Connections folder or through the Local Users and Groups folder.

Support for user principle names, universal groups, and Extensible Authentication Protocol-Transport Level Security (EAP-TLS) is not available in IAS running on a stand-alone Windows 2000 server.

Access by Policy in a Windows 2000 Server Mixed-Mode Domain

In an access-by-policy administrative model, the remote access permission on every user account is set to **Control access through Remote Access Policy** and remote access permissions are determined by the remote access permission setting on the remote access policy. Therefore, the permission setting on the remote access policy determines whether remote access is allowed or denied. Even though remote access policies are implemented only in Windows 2000 Server, you can implement access-by-policy in domains that contain both Windows 2000 and Windows NT 4.0 servers by using the Windows 2000 mixed-mode domain administrative model. This supports migration from Windows NT 4.0 to Windows 2000.

You can use this administrative model when deploying any remote access server running Windows 2000 Server that is a member of a:

- Windows 2000 mixed-mode domain.
- Windows NT 4.0 domain.

To maintain compatibility with Windows NT 4.0 domain controllers, dial-in properties of user accounts must match those found in Windows NT 4.0. Therefore, for an IAS server that is a member in a Windows 2000 mixed-mode domain, only the following authentication and remote access management features (available as dial-in user account properties) are supported:

- Remote access permission (only **Allow access** and **Deny access**)
- Callback Options

The Verify Caller ID, Assign a Static IP Address, and Apply Static Routes properties are not available.

When upgrading a stand-alone server running Windows 2000 Server to a mixed-mode domain controller, all values of dial-in properties that are configured while in stand-alone mode are preserved, including those that are now unavailable. The remote access permissions set to **Allow access** are preserved in the upgrade. The remote access permissions set to **Deny access** are set to **Control access through Remote Access Policy** during the upgrade.

If you have Windows NT 4.0 Routing and Remote Access Service (RRAS) servers, you can only use this administrative model if the RRAS servers are configured as RADIUS clients to a Windows 2000 IAS server, but you cannot use this administrative model for Windows NT 4.0 RAS servers.

Access by Policy in a Windows 2000 Server Native-Mode Domain

Like the mixed-mode domain administrative model, this administrative model uses remote access policies to control remote access. You can use this access-by-policy administrative model when deploying Windows 2000 remote access solutions in networks where all domain controllers are running Windows 2000 Server. The access-by-policy administrative model for a Windows 2000 native-mode domain also applies to stand-alone remote access servers that are not a member of a domain.

You cannot use this model with Windows NT 4.0 RAS or IAS servers.

When the mixed-mode domain controller is upgraded to a native-mode domain (containing only Windows 2000 domain controllers), all dial-in properties become available. Dial-in properties that are configured while the remote access server is in stand-alone mode that are not available in mixed mode are preserved for native mode. For example, if the Verify Caller ID property for a user account is set to 555-0001 when the remote access server is in stand-alone mode and then the Active Directory Installation Wizard is run, the Verify Caller ID property is unavailable. However, when you change the domain mode to native mode, the Verify Caller ID property is available and retains its original configured value of 555-0001.

Note Callback numbers that are configured while the computer running Windows 2000 is in stand-alone mode may be truncated when the computer is upgraded to a mixed-mode domain controller. Callback numbers may also be truncated when a remote access server running Windows NT 4.0 requests dial-in properties of a user account in a Windows 2000 native-mode domain.

Determining How to Set Up Remote Access Policies

Remote access policies are defined using the Routing and Remote Access service (or IAS, for RADIUS solutions), and remote access policies can be copied from one server to the other.

Remote access policies are the basis for controlling access and authentication in all Windows 2000-based remote access solutions. In a RADIUS solution, these policies are centrally implemented and managed for remote access servers. In a non-RADIUS implementation, they are defined for each remote access server individually. The way that you structure the policies and specify conditions for granting or denying access can significantly impact the effectiveness, security, and ease of management of your remote access solution.

Remote Access Policy Structures

The structure of your enterprise and the needs of your users should determine the structure of your remote access policies. The structure includes how many policies are required, the scope of the policies, and the users who are supported by each policy.

To define the structure for your remote access policies, start with the definition of a single remote access policy for the corporation, and then add additional policies for users and groups that are not covered by the primary policy. At a minimum, you should have individual policies for:

- Each solution (such as dial-up client access solution and VPN solution).
- Each user or group with a unique remote access security requirement (such as users or groups with specific day-and- time access restrictions).

List the policies in the order in which they are to be applied, with the most specific at the top of the list and the most general at the bottom of the list.

Conditions for Granting or Denying Remote Access

Remote access policy conditions are one or more attributes that are compared to the settings of the connection attempt after validation of the user name and password. If you define multiple conditions for each remote access policy, then all of the conditions must match the settings of the connection attempt in order for the connection attempt to match the policy.

Table 5.5 shows the condition attributes that you can specify for a remote access policy.

Table 5.5 Remote Access Policy Attributes

Attribute Name	Description
NAS IP Address	The IP address of the NAS. This attribute is a character string. You can use pattern-matching syntax to specify IP networks. This attribute is designed for the IAS server.

Service Type	The type of service being requested. Examples include framed (such as PPP connections) and login (such as Telnet connections). This attribute is designed for the IAS server. For more information about RADIUS service types, see RFC 2138.
Framed Protocol	The type of framing for incoming packets. Examples are PPP, SLIP, Frame Relay, and X.25. This attribute is designed for the IAS server.
Called Station ID	The phone number of the NAS. This attribute is a character string. You can use pattern-matching syntax to specify area codes. In order to receive called station ID information during a call, the phone line, the hardware, and the Windows 2000 Server driver for the hardware must support the passing of the called ID. Otherwise, the called station ID is manually set for each port.
Calling Station ID	The phone number used by the caller. This attribute is a character string. You can use pattern-matching syntax to specify area codes
NAS Port Type	The type of media used by the caller. Examples are analog phone lines (known as asynchronous), ISDN, and tunnels or VPNs (known as virtual).
Day and Time Restrictions	The day of the week and the time of day of the connection attempt. The day and time is relative to the date and time of the server providing the authorization.
Client IP Address	The IP address of the NAS (the RADIUS client). This attribute is a character string. You can use pattern-matching syntax to specify IP networks. This attribute is designed for the IAS server.
Client Vendor	The vendor of the NAS that is requesting authentication. You can use this attribute to configure separate policies for different NAS manufacturers who are RADIUS clients to an IAS server. This attribute is designed for the IAS server. Make sure that you also configure the NAS as a RADIUS client on the IAS server.
Client Friendly Name	The name of the RADIUS client computer that is requesting authentication. This attribute is a character string. You can use pattern-matching syntax to specify client names. This attribute is designed for the IAS server.
Windows Groups	The names of the Windows 2000 groups to which the user attempting the connection belongs. There is no condition attribute for a specific user name. It is not necessary to have a separate remote access policy for each group. Instead, you can use nested groups to consolidate group membership and delegate administration of group membership.
Tunnel Type	The type of tunnel being created by the requesting client. Tunnel types include PPTP and L2TP used by Windows 2000 remote access clients and demand-dial routers. You can use this condition to specify profile settings such as authentication methods or encryption strengths for a specific type of tunneling technology.

For more information about how to use pattern-matching syntax, see Windows 2000 Server Help.

Note You cannot use the built-in local groups of a stand-alone remote access server running Windows 2000 Server for the Windows Groups attribute.

As discussed earlier in this chapter, the administrative model that you select affects how permissions are handled. However, granting access through the user account permission setting or the policy permission setting is only the first step in accepting a connection. The connection attempt is then subjected to the settings of the user account properties and the policy profile properties. If the connection attempt does not match the settings of the user account properties or the profile properties, the connection attempt is rejected.

By default, the **Deny remote access permission** policy permission is selected.

Guideline If you are using remote access policies to restrict access for all but certain groups, create Active Directory groups with global scope for all users to whom you want to allow access, and nest them in groups with universal scope. Then create a remote access policy that grants access for that universal group. Do not put all users directly in the group with universal scope, especially if you have a large number of users on your network.

Use a user principal name to refer to users whenever possible. A user can have the same user principal name regardless of which domain the user belongs to. This indirection provides scalability that might be required in organizations with a large number of domains. For more information about domain and account naming, see Windows 2000 Server Help.

Defining RADIUS Support

Centralizing support of your remote access solution requires defining the RADIUS clients (NASs) that are included in the RADIUS design and specifying how to implement common and NAS-specific support for these servers. This section covers the elements that are specific to a RADIUS implementation. Other elements that are common to both RADIUS and non-RADIUS implementations (such as authentication and encryption) are covered later in this chapter.

RADIUS Client Properties

For each remote access server serving as a RADIUS client for IAS, specify the following in IAS:

- **Friendly name for RADIUS client**. This is the computer name that is specified in your network diagram.
- **Client IP or DNS Address**. In most cases, it is better to specify RADIUS clients by IP address because IAS does not need to resolve host names at startup. As a result, IAS will start more quickly than if you used DNS names and you do not need to have a name server available when IAS starts. The IP addresses and DNS names should be shown in your network diagram.
- **Client-Vendor**. For remote access servers running Windows 2000, Microsoft is the client-vendor.
- **Client must always send the signature attribute in the request**. Select this option only if your NAS supports the use of the digital signature attribute for verification.
- **Shared secret**. The shared secret must be the exactly the same as specified on the remote access servers.

RADIUS Realms

In some cases, user names in RADIUS messages must be converted before authentication processing begins. To do this, specify the rules to use for realm stripping, including the pattern (realm suffix or prefix) to find and the pattern to be used to substitute for it (which can be blank if realm stripping is all that is required). You cannot replace a realm suffix with a realm prefix or vice versa.

You can use this syntax to specify RADIUS realm information to be found. For information about Pattern Matching Syntax, see Windows 2000 Server Help. For information about implementing a RADIUS proxy (using Windows NT 4.0), see "Expanding and Securing Remote Client Access."

Advanced Settings for RADIUS Attributes

To provide NAS-specific support, add RADIUS standard attributes and vendor-specific attributes (VSAs) to remote access profiles. The manufacturer's documentation for the NAS should provide the information required to know which attributes are to be specified. VSAs allow vendors to support their own proprietary attributes that are not covered by RFC 2138. IAS includes VSAs from a number of vendors in its multi-vendor dictionary.

After you determine which attributes the NAS requires, determine which ones are supported RADIUS attributes in Windows 2000 Server and which ones require the addition of either conforming or non-conforming vendor-specific RADIUS attributes (attribute type 26). If it does not conform, specify the attribute value in hexadecimal format.

If you need to specify more than one VSA, arrange them in the appropriate order. For example, if you are using a filtering attribute that will automatically disconnect users who do not satisfy specific criteria, you should make sure that the attribute is specified at the top of the list.

For a list of the RADIUS attributes, including VSAs that are supported by the remote access server running Windows 2000 Server, see Windows 2000 Server Help.

Specifying Security and Other Access Control Elements

Whether you are deploying a RADIUS or non-RADIUS solution, you must determine how authentication, encryption, and security features and access controls are to be implemented. These decisions are critical to providing the integrity, privacy, and effectiveness required in a remote access solution.

Authentication Providers

The remote access server must authenticate and authorize remote access clients before they can access or generate traffic on the network. This authentication is a separate step from logging on. You must specify which authentication provider is to be used by each remote access server:

- Windows authentication
- RADIUS authentication

Unless a specific server has unique requirements, specify the same provider for all remote access servers.

Windows Authentication

A remote access server running Windows 2000 Server supports the use of Active Directory security or Windows NT primary domain controller (PDC) security (Microsoft® Windows NT® Server 4.0 and earlier) as an authentication provider to provide authentication of a remote access client. With Windows authentication, the server uses a Windows 2000 Server local account database, a Windows 2000 Server domain account database, or a Windows NT 4.0 domain account database to authenticate remote access or demand-dial connection credentials. The server also uses locally configured remote access policies to provide authorization of the remote access connection. Scenarios that support the use of Windows authentication include:

- A stand-alone server running Windows 2000 Server (a remote access server that is running Windows 2000 Server that is not a member of a domain). In this case, only the local accounts database is available for setting remote access permissions.
- A member server in a Windows NT 4.0 domain (a remote access server running Windows 2000 Server that is a member server in a Windows NT 4.0 domain).
- A member server in a mixed-mode or native-mode Windows 2000 Server domain (a remote access server that is running Windows 2000 Server and is a member server in a Windows 2000 Server mixed-mode domain or a Windows 2000 Server native-mode domain).
- A Windows NT 4.0 remote access server in a Windows 2000 Server domain (a server that is running Windows NT 4.0 and the Remote Access Service (RAS) or the Routing and Remote Access Service (RRAS) in LocalSystem security context, and that is a member of a Windows 2000 Server domain).

For more information about the use of Windows authentication, including the accounts databases that are used in each, how the dial-in properties are administered, and potential security issues for Windows 2000 authentication, see Windows 2000 Server Help.

RADIUS Authentication

A remote access server running Windows 2000 Server configured for RADIUS authentication provides RADIUS-based authentication and authorization for remote access connections. The RADIUS server has access to user account information and can check remote access credentials. If the user's credentials are authentic and the connection attempt is authorized, the RADIUS server authorizes the user's access based on the specified conditions.

To use IAS server to authenticate access attempts received by a remote access server, select RADIUS Authentication as the authentication provider and specify that the RADIUS servers to be queried for authentication. To do this, provide the following information for all remote access servers:

- Server name, which is the DNS name or IP address of the IAS server.
- Shared secret, which is the obscured shared secret that is used to verify communications between the NAS and the RADIUS server.
- Port, which is the UDP port that is used by the RADIUS server for incoming RADIUS authentication requests. The remote access server default value of 1812 is based on RFC 2138, and does not need to be changed when you are using an IAS server. The default ports on IAS are 1813 (the RADIUS standard) and 1646 (for down-level support).

For RADIUS authentication, you can also specify:

- Always use digital signatures, which requires that a digital signature attribute based on the shared secret be sent with each RADIUS message. EAP messages are always sent with a digital signature attribute. Select this option if your RADIUS server is a Windows 2000 Server–based computer that is running IAS.
- Time-out (seconds), which is the amount of time that the remote access server tries to obtain responses from a RADIUS server before trying another RADIUS server. The default is 5.
- Initial score, which is the initial responsiveness score of the RADIUS server. The score increases or decreases based on the ongoing responsiveness of the RADIUS server. The default is 30.

  Guideline In a global enterprise with large numbers of remote access servers deployed worldwide, centralized authentication and accounting by using IAS can be beneficial.

  Use long shared secrets. The longer the secret, the more secure it is. Use a variety of uppercase and lowercase letters, numbers, and punctuation in the shared secret to combat dictionary attacks.

Authentication Methods

Authentication methods typically use an authentication protocol that is negotiated during the connection establishment process. Some of the protocols supported by Routing and Remote Access provide enhanced authentication, whereas other protocols that provide less security give other benefits such as support for a wide diversity of remote access clients. The protocol that is used is determined by the negotiation of the authentication protocol during the PPP connection establishment process.

For dial-up client access, the following support is provided by Windows 2000 Server and Routing and Remote Access (listed in order from most secure to least secure):

- EAP-TLS

- Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAP v2)
- Microsoft Challenge Handshake Authentication Protocol version 1 (MS-CHAP v1)
- Extensible Authentication Protocol-Message Digest 5 Challenge Handshake Authentication Protocol (MD5 CHAP)
- Challenge Handshake Authentication Protocol (CHAP)
- Shiva Password Authentication Protocol (SPAP)
- Password Authentication Protocol (PAP)
- Unauthenticated access

Authentication methods can be specified for each remote access server and, if more detailed control is required, for each remote access policy. Additional information about the support provided by each protocol is covered later in this chapter.

Windows 2000 can use Microsoft Point-to-Point Encryption (MPPE) for dial-up networking connections that use MS-CHAP v1, MS-CHAP v2 or EAP-TLS authentication.

You can set up your remote access servers to accept multiple authentication protocols and to try to negotiate a connection using the most secure protocol first, and then the next less secure, and so on down to the least secure. Set up each remote access policy to support specific authentication methods appropriate to the security requirements of the users covered by the policy.

Table 5.6 provides information to help you map your requirements to the appropriate protocol.

Table 5.6 Authentication Protocol Support

Requirement	Select
Encrypted authentication support for Windows 95, Windows 98, or Windows NT 4.0 remote access clients (with the latest Dial-Up Networking upgrade).	MS-CHAP v1, MS-CHAP v2
Encrypted authentication support for Windows 2000 remote access clients.	MS-CHAP v1, MS-CHAP v2, EAP-MD5
Encrypted authentication support for remote access clients that use other operating systems.	CHAP
Encrypted authentication support for remote access clients by using Shiva LAN Rover software.	SPAP
Encrypted authentication support for user certification-based PKIs, such as those used with smart cards (when the remote access server is a member of a Windows 2000 Server mixed-mode or native-mode domain).	EAP-TLS
Unencrypted authentication when the remote access clients support no other protocol.	PAP
Authentication credentials are not supplied by the remote access client.	Unauthenticated Access

MS-CHAP v2 provides stronger security for remote access connections than MS-CHAP v 1, so you should not use MS-CHAP v1 unless your clients do not support MS-CHAP v2. Table 5.7 shows how MS-CHAP v2 solves security issues that exist with MS-CHAP v1.

Table 5.7 MS-CHAP v2 Enhanced Functionality

MS-CHAP v1	MS-CHAP v2
LAN Manager encoding of the response used for backward compatibility with older Microsoft remote access clients is cryptographically weak.	Does not allow LAN Manager encoded responses.
LAN Manager encoding of password changes is cryptographically weak.	Does not allow LAN Manager encoded password changes.
Only one-way authentication is possible. The remote access client cannot verify that it is dialing in to its organization's remote access server or a masquerading remote access server.	Provides two-way authentication, also known as mutual authentication. The remote access client receives verification that the remote access server that it is dialing in to has access to the user's password.
With 40-bit encryption, the cryptographic key is based on the user's password. Each time the user connects with the same password, the same cryptographic key is generated.	The cryptographic key is always based on the user's password and an arbitrary challenge string. Each time the user connects with the same password, a different cryptographic key is used.
A single cryptographic key is used for data sent in both directions on the connection.	Separate cryptographic keys are generated for transmitted and received data.

Remote access support for PPP dial-up networking clients is outlined in Table 5.8.

Table 5.8 Authentication Support in Windows Operating Systems

Dial-Up Networking Client	Supported Windows 2000 Remote Access Authentication	Unsupported Windows 2000 Remote Access PPP Authentication
Windows 2000	BAP, MS-CHAP v1, CHAP, SPAP, PAP, MS-CHAP v2, and EAP.	BAP using Connection Manager.
Windows NT 4.0	MS-CHAP v1, CHAP, SPAP, PAP, and MS-CHAP v2 (with Windows NT 4.0 Service Pack 4 and later).	BAP and EAP.
Windows NT 3.5	MS-CHAP v1, CHAP, SPAP, and PAP.	BAP, MS-CHAP v2, and EAP.
Windows 98	MS-CHAP v1, CHAP, SPAP, PAP, and MS-CHAP v2 (with the Windows 98 Service Pack 1 and later).	BAP and EAP.
Windows 95	MS-CHAP v1, CHAP, SPAP, and PAP (with the Windows Dial-Up Networking 1.3 Performance & Security Upgrade for Windows 95). **Note** Windows 95 with the Windows Dial-Up Networking 1.3 Performance & Security Upgrade for Windows 95 supports MS-CHAP v2 over VPN connections, but not MS-CHAP v2	MS-CHAP v2, BAP, and EAP.

	over dial-up connections.	

Guideline It is strongly recommended that you do not use PAP for authentication, unless you absolutely have to support clients that are running software that cannot authenticate with other protocols.

On both the remote access servers and in specific remote access policies, disable all protocols that you will not be using.

If you need to allow multiple protocols, set up your NASs to try to negotiate a connection starting with the most secure protocol first, then the next most secure, and so on to the least secure.

Use strong passwords that are more than 8 characters long and that contain a mixture of uppercase and lowercase letters, numbers, and permitted punctuation. Do not use passwords based on names or words. Strong passwords are more resistant to a dictionary attack, where an unauthorized user attempts to crack a password by sending a series of commonly used names and words.

Although EAP-TLS works with registry-based certificates, for security reasons it is highly recommended that you only use EAP-TLS with smart cards. For more information about smart cards and certificates, see "Expanding and Securing Remote Client Access"

If you are using MS-CHAP, use MS-CHAP v 2. You can obtain the latest MS-CHAP updates for Windows NT 4.0, Windows 98, and Windows 95 remote access clients from Microsoft. For more information about MS-CHAP v2, see Windows 2000 Server Help.

Data Encryption

Use data encryption for any remote access connection for which there is a risk of unauthorized interception of transmissions on the communications link between the remote access client and the remote access server.

For dial-up networking connections, Windows 2000 supports the use of MPPE. Encryption keys are determined at the time of the connection.

Windows 2000 uses MPPE for dial-up networking connections that use MS-CHAP, MS-CHAP v2 or EAP-TLS authentication. The following MPPE encryption keys are supported:

- None: Unauthenticated access or using EAP-MD5 CHAP, CHAP, SPAP, or PAP authentication.
- Basic: 40-bit encryption keys, for international use and to connect with earlier Microsoft operating systems that do not support 56-bit MPPE encryption keys.
- Strong: 56-bit encryption keys, for international use with operating systems that support it.
- Strongest: 128-bit encryption keys, for international use, subject to export restrictions.

The Windows 2000 High Encryption Pack that provides the support for 128-bit encryption is available for export from the U.S. to all customers worldwide, except to US embargoed destinations. For more details, see http://www.Microsoft.com/exporting/ .

Table 5.9 shows which authentication methods support specific encryption requirements.

Table 5.9 Encryption Support

Requirement	**Authentication Methods**	**Encryption Enforcement**
Unsecured password with no data encryption	PAP	Optional encryption (connect even if no encryption)
Secured password with no data encryption	CHAP, MS-CHAP v1, MS-CHAP v2	Optional encryption (connect even if no encryption)
Secured password with MPPE data encryption	MS-CHAP v1, MS-CHAP v2	Require encryption (disconnect if server declines)
Smart card with no data encryption	EAP-TLS	Optional encryption (connect even if no encryption)
Smart card with data encryption	EAP-TLS	Require encryption (disconnect if server declines)

Note Dial-up client access does not provide end-to-end data encryption. End-to-end data encryption is data encryption between the client application and the server that hosts the resource or service being accessed by the client application. It is supported only when using IPSec after the dial-up connection has been made. For more information, see "Expanding and Securing Remote Client Access."

Guideline Use the strongest authentication and level of encryption that your situation allows. Windows 95, Windows 98, and Windows NT 4.0 clients running the latest service pack and Dial-Up Networking upgrade support 128-bit encryption. You can force the use of strongest encryption for dial-up and VPN connections by configuring the encryption settings on the appropriate remote access policy.

Dial-in Constraints

To limit users' access to your network, specify controls to be applied to client connections. Controls that you can define for each remote access policy include:

- Restrict the amount of time a connection remains idle before disconnecting.
- Restrict the session to maximum length of time.
- Restrict access to specific days of the week and times of the day, either by specifying when access is to be permitted or when access is to be denied.
- Restrict dial-in to a single, specific number.
- Restrict dial-in media that are supported. This is useful for tailoring profiles to specific solutions. For instance, ISDN connections can have different dial-in constraints than analog modem connections.

Note By default, none of the above restrictions are set. If you want to apply any of these restrictions, specify how they are to be applied.

IP Addressing and Filtering by Policy

Although IP routing and address assignment are specified for each remote access server, a more detailed level of control of client access can be implemented by specifying IP addressing and filtering requirements for individual remote access policies.

IP Address Assignment for Policies

You have three options for IP address assignment:

- Server must supply an IP address
- Client can request an IP address
- Server settings define policy

By default, the remote access server automatically allocates an IP address and the client is not allowed to request a specific IP address.

Specify the appropriate options to be implemented on the remote access servers and, if appropriate, in the remote access policies. For more information about TCP/IP and remote access (including assigning IP addresses to remote access clients, remote access server and DHCP, and remote access server static IP address pools) see Windows 2000 Server Help.

IP Packet Filters in Remote Access Policies

Ensuring a secure network requires preventing traffic between the private networks and external networks. To prevent unwanted traffic, specify unique Routing and Remote Access packet filters for each router interface. Windows 2000 Server routing supports both IP and IPX packet filtering. These are layer three filters that specify which IP or IPX packets are sent or received by the interface (allowed into or out of the router interfaces). Your filter design can be based on a single criteria or any combination of the following:

- Source IP address or range
- Destination IP address or range
- IP protocol number
- TCP source or destination port number
- UDP source or destination port number
- Internet Control Message Protocol (ICMP) type and code

Specify filters to either accept or reject packets that match any of the filters assigned in the interface. Separate input and output filters can be configured.

In addition to being assignable to routing interfaces, you can also assign packet filters to remote access policies. Remote access policy profile filtering applies to all remote access connections that match the remote access policy.

Access to resources can be restricted for remote access clients by:

- Allowing access to only those resources that are on the remote access server. This restriction is set on each individual remote access server, and applies to all clients who connect to the server.
- Allowing access to resources on the routed network to which the remote access server is attached. This restriction is set on each individual remote access server, and applies to all clients who connect to the server.
- Allowing access to specific subnets by configuring remote access policy profile IP packet filters that define the traffic that is allowed to and from the remote access client.

Ensure that the packet filters you specify do not prevent the sending or receiving of DHCP traffic (for DHCPINFORM messages from remote access clients). DHCP traffic uses the UDP ports of 67 and 68.

Specifying Extended Support for PPP Clients

Windows 2000 provides support for PPP clients that can extend and enhance the user's access capabilities. Decide which of these features are appropriate in each remote access policy.

Multilink for PPP Clients

Multilink connections use PPP Multilink Protocol (MP) to allow remote access clients to combine multiple physical connections into a single logical connection to establish high-speed connections. You can implement Multilink support for PPP connections by specifying support on the remote access servers and in remote access policies.

While MP allows for multiple physical links to be aggregated, Multilink does not provide a mechanism for adapting to changing bandwidth conditions by adding extra links when needed or terminating extra links when unnecessary. If you want this additional capability to dynamically manage links, you must specify BAP support on the remote access server.

If you support Multilink on a remote access server, you can tailor how each remote access profile implements the support. Your options for the dial-up client access profiles are:

- Default to server settings.
- Disable Multilink (restrict client to a single port).
- Allow Multilink. If you choose this option, specify the maximum number of dial-in ports that Multilink can use.

  Note Unless you specify that Multilink is to be disabled, specify the conditions for reducing a Multilink connection by one line (by default, when the lines fall below 50 percent of capacity for a period of 2 minutes.) You can specify that BAP is required for dynamic Multilink requests.

When Multilink and BAP are used in combination with the callback feature set to **always call back to the same number**, a concentrator must exist on the caller side that can distribute incoming calls to the same number on various ports.

Each client that requires Multilink support must specify how support is to be implemented. If creating Connection Manager service profiles, Multilink is not supported in the CMAK Wizard, but can be implemented using advanced customization techniques (by setting IsdnDialMode to support bonding of the two Primary Rate ISDN [PRI] channels).

Note Connection Manager does not currently support BAP.

If the client uses Multilink support to dial a server that requires callback, then only one of your multilinked devices is called back. This is because you can only store one number in a user account. Therefore, only one device connects and all other devices fail to complete the connection. You can avoid this problem in the following ways:

- If the multilinked phone book entry uses a standard modem configuration, and the remote access server that your connection is calling uses more than one line for the same number.
- If the multilinked phone book entry is ISDN with two channels that have the same phone number.

  Note Connection Manager does not support callback.

Guideline Avoid configuring different remote access policies for the same user. If a user dials in by using a Multilink connection, all connections beyond the first one use the remote access policy that matched the first connection.

Link Control Protocol Extensions for PPP Clients

Determine if you require the Link Control Protocol (LCP) extensions that support the transmission of Time-Remaining and Identification packets and request callback during LCP negotiation. LCP extensions are enabled by default but can cause problems with NASs running older PPP software, so you might need to disable them if problems occur and you do not require the extensions.

Note In Connection Manager, LCP extensions are disabled by default. If LCP extension support is required in a Connection Manager service profile, specify client support using Connection Manager advanced customization techniques.

Software Compression for PPP Clients

Determine if you want to use Microsoft Point-to-Point Compression Protocol (MPPC) to compress data sent on the remote access or demand-dial connection. The MPPC algorithm is designed to optimize processor utilization and bandwidth utilization in order to support large numbers of simultaneous connections. For any data compression protocol to work, modems on both ends of the connection must support the protocol. MPPC can only be used with PPP clients.

If you use MPPC software compression, you can also use modem error correction, but you should not use hardware compression.

Defining Accounting and Logging Methods

Many of the decisions required to deploy accounting and logging for a remote access solution are dependent on whether you are deploying a RADIUS or non-RADIUS solution. Both solutions require the determination of what type of information is required and how it is to be implemented and used to manage the remote access environment.

Accounting Providers

Windows 2000 Server and Routing and Remote Access service support three accounting provider options:

- **Windows Accounting**. The remote access server logs connection accounting information locally in log files that are configured on the server.
- **RADIUS Accounting**. Each remote access server sends accounting information to the RADIUS server, where it is centrally logged in log files that are configured on the RADIUS server.
- **None**. No accounting information is logged.

In Windows 2000, you can configure the remote access server accounting provider separately from the authentication provider. Therefore, a remote access server can use Windows as its authentication provider and RADIUS as its accounting provider. For instance, if you want to manage authentication centrally, but maintain accounting logs locally, specify RADIUS authentication and Windows accounting.

Your decision to use Windows or RADIUS accounting providers should be based on the following considerations:

- Where is data collected? If data is to be collected in a central location, select RADIUS accounting. If central collection is not required, select Windows accounting.
- How is data analyzed, especially if using legacy analysis tools? For example, if your analysis tools are specific to individual NASs and do not support centralized accounting, select Windows accounting.

Windows Accounting

Use Windows accounting if you want the remote access server to log connection accounting information in log files specified for that individual remote access server.

RADIUS Accounting

If your dial-up solution includes IAS and Windows 2000 remote access servers, use RADIUS as your accounting provider to centralize logging for all remote access servers. To use RADIUS as your accounting provider for an IAS-based solution, specify the following for each remote access server:

- The server name, which is the host name or IP address of the IAS server.
- The secret that is to be shared between the remote access server (running Windows 2000 Server) and the IAS server to support encryption of messages sent between them. Configure both the remote access server and the IAS server to use the same shared secret.
- The port on the IAS server to which the remote access server must send its accounting requests. This is the UDP port to which the IAS server is listening. The remote access server default value of 1813 is based on RFC 2139 and does not need to be changed when using an IAS server. The defaults on IAS are 1813 (the RADIUS standard) and 1646 (for legacy support).

Remote Access Logging/Accounting

Both Windows accounting (for local logging) or RADIUS accounting (for centralized logging) require specification of how logging is to be handled.

Activities to Log

Specify what remote access connection activities are logged:

- Log accounting requests (such as accounting start or stop)
- Log authentication requests (such as Access-Accept or Access-Reject)
- Log periodic status (such as interim accounting requests)

It is recommended that you select the first two. Selecting the last one can result in extremely high-volume logs, so it is only recommended for troubleshooting.

Guideline Initially, turn on logging of both authentication and accounting records. Modify these selections after you have determined what is appropriate for your environment.

Log File Format

Specify the log file format:

- **Database-compatible file format** results in recording of access logs in a consistent format that is easily importable to a database and that can import a comma-separated input file.
- **IAS format** (the default) results in logs with events recorded in the ID-value paired format. The specific content of each record is dependent on the attributes supported by the remote access server.

The database-compatible file format does not log as many attributes as the IAS format, but it does provide a consistent structure for all log entries. This consistent structure enables the results to be readily imported into databases, which facilitates analysis and reporting using automated in-house or third party tools. Records can also be routed to databases using pipes. For more information about log file formats, including how to import logs into a database, see Windows 2000 Server Help.

Time Period for Logs

Specify when to start new logs:

- Daily.
- Weekly.
- Monthly.
- No automatic stop and start, with no limitation on maximum file size (default).
- When the log file reaches a specific size that you specify.

  Guidelines Ensure that event logging is configured with sufficient capacity to maintain your logs. The default is 512 KB but, depending on your configuration, it should be at least double this size.

  Back up all log files on a regular basis, as logs cannot be recreated if they are damaged or deleted.

Log File Directory

Specify the location where log files are to be kept. If you are using Windows accounting, specify a location for each remote access server. If using RADIUS accounting, logging is centralized, so for each IAS server, you specify a single location at which to maintain logs for all remote access servers.

Note The log file name is automatically determined by the time period specified for starting new logs. For example, an unlimited file size log has the name IASlog.log and a monthly log has the name IN*yymm*.log.

Guidelines Back up Ias.mdb before running IAS for the first time. The Ias.mdb file is stored in the *systemroot*\System32\ias folder, where *systemroot* is the folder in which Windows 2000 Server system files are located, typically C:\Winnt. It is also important that you back up the database whenever there is a change to your IAS configuration. If you do not back up the database and then inadvertently delete one file in the IAS folder or your system experiences a system-wide corruption, you can lose all of your configuration data.

You can use the RADIUS class attribute to track usage and simplify identification of which department or user to charge for usage. Although the class attribute is unique for each request, duplicate records can exist in cases where a response to the NAS is lost and the NAS re-sends the request. Depending on how you implement your tracking process, you might need to delete the duplicate requests from your logs to accurately track usage.

Note The class attribute is logged whether you select database-compatible or IAS formatting for the log files. If you use custom or third-party software to analyze and report results of log files, consider incorporating support for analysis of this attribute. For more information about how the class attribute is implemented in IAS, see Windows 2000 Server Help.

Event Logging

Specify the level of system event logging that you want to implement for your remote access servers by selecting one of the following options for the PPP properties of the remote access server:

- Log errors only
- Log errors and warnings (default)
- Log the maximum amount of information
- Disable event logging

Also specify the types of authentication events that should be recorded by IAS in the Windows 2000 Server event log:

- Log rejected or discarded authentication requests
- Log successful authentication requests

Additionally, you can specify whether the events in the PPP connection establishment process for remote access and demand-dial routing connections are written to the Ppp.log file for tracing. The Windows 2000 Server router has an extensive tracing capability. If the tracing function is enabled, you can enable tracing for each component of the Routing and Remote Access service.

Event logging and tracing both consume system resources and should be used sparingly to help identify network problems. Always return settings to their default state after problems are resolved.

Note Do not leave tracing enabled on multiprocessor computers.

For more information about using event logging and using tracing, including how to set up tracing, see Windows 2000 Server Help.

Defining Connection Manager Support for Dial-Up Client Access

To create Connection Manager client software, build one or more service profiles, each of which must include:

- A friendly name for your service profile
- A file name for your service profile
- A phone book containing at least one phone number

Providing appropriate branding and functionality is most effective if you also incorporate graphics, programs, and multiple access numbers in the Connection Manager service profile. To determine how Connection Manager options can best be used to meet your needs, evaluate the following.

- How to structure the service profiles to most efficiently and effectively meet requirements
- What additional programs and functions you need to integrate to support specific requirements
- How to optimize the connection experience for users
- How to distribute the client software

Use the information in this section and the worksheet in Windows 2000 Server Help to help evaluate all design options for your Connection Manager client software solution.

Client Software Structure

To define client software structure, including the number of service profiles required to support your users, analyze the user groups who require remote access. If users are a single group with common access requirements, a single Connection Manager service profile might be sufficient to meet their needs. However, if you have multiple groups with diverse requirements, it is better to create multiple service profiles. Some of the factors that might make it advantageous to create separate service profiles include:

- **Diverse operating systems**, especially if you want to support additional functionality of specific operating systems. For instance, if you have a local group with critical security requirements that can only be met using 128-bit dial-up encryption with EAP and you have another roaming group with much lower security requirements, then you can set up two profiles, one to be used on Windows 2000 clients for high-security access and one that can be used on other operating systems for lower security access.
- **Group identities**, which can be branded in a service profile. For instance, if you provide remote access support for multiple divisions, you can provide a separate branded service profile for each division.
- **Locations**, especially if you want to restrict access to a single network. For instance, if you have a sales office in one city and a research facility in another city, each with its own network, and you want users to directly access their own networks, you can provide a separate service profile for each location.
- **Points of presence (POPs)**, which provide access points for remote connections. For instance, if you have a group of local users whom you only want to use direct dial numbers, and you have another group of roaming users whom you only want to use VPN access points, you can create separate phone books and service profiles for each group. Or, to localize access for remote sites, you might set up separate service profiles for each region.

For each service profile you create, determine the following:

- **Profile names**. What service (friendly) name and file name do you want to use? Names should reflect the identity of your organization since they will be distributed to your users.
- **Realm names.** Do you need to append realm names (prefix or suffix) to ensure appropriate routing through a proxy server?

- **Phone books**. What access points do you want to provide with each service profile and what are the access numbers? Do you want to provide automatic updates for phone books so that users do not have to manually update access numbers? How do you want to structure your phone books (regions)? Who is the phone book administrator? What is the address of the Connection Point Services (CPS) server on which Phone Book Service (PBS) is installed? Do you want to include tariff and non-tariff numbers and, if so, do you want to provide user instructions on how to use these numbers? Do you want to import phone book data?
- **Merging of service profiles**. Do you want to automatically merge multiple profiles together to integrate features such as multiple phone books (with separate phone books for each location, each ISP, or other separately maintained list of access numbers)? Individual elements of a service profile are integrated differently when merging multiple service profiles. For more information about merging phone books and other features from existing service profiles, see Windows 2000 Server Help.

  Guideline Specify POP settings (also called service types) so that, in Connection Manager, users can search in their phone books for access numbers that suit their needs and filter out the ones they do not want.

Integrated Programs and Functions

You can use the CMAK Wizard to incorporate custom programs into a service profile that extend the functionality of Connection Manager. The functionality you can incorporate includes:

- **Connect actions and auto-applications**. Do you want to integrate your own programs to automatically run at specific times during the connection process?
- **Dial-Up Networking entries**. Do you want to specify how specific POPs are accessed to provide more effective handling of unique network authentication or routing requirements for individual access points, including assigning specific DNS or WINS addresses and/or specifying a custom Dial-Up Networking script (if required by the POP or your service)?
- **Domain name**. Does your enterprise require a domain name for authentication? If not, do you want to hide the domain name box on the Connection Manager logon screen?
- **License agreement**. Do you want to incorporate a custom license agreement with the service profile, which your users must accept before using the software?

User Connection Experience

You can incorporate graphics, information, and support in a Connection Manager service profile to brand the client software and to provide a better connection experience for users. The branding and user assistance you can provide includes:

- **Custom graphics and icons**. Do you want to replace the default graphics and icons with your own bitmaps and icons to provide a unique identity to a service profile?
- **Shortcut menu items**. Do you want to provide quick access to specific programs by adding entries to the status-area-icon shortcut menu that appears when a user right-clicks the program icon in the status area of the taskbar (in addition to the default actions: Status, Disconnect, and Open Network Connections folder)?
- **Support information**. Do you want to add a line of text to the logon dialog box to provide customer support information for your users?
- **Windows Help**. Do you want to customize the default online Help provided with Connection Manager (especially if you have added custom functionality, such as connect actions, that might need user support)?
- **User documentation and other additional files**. Do you want to use the templates provided with CMAK to create a custom Readme file and user documentation for your users? Do you want to incorporate other files, including any required to support additional functionality?

Security

You can enhance security for your users by using advanced customization techniques and code signing:

- **Save password and connect automatically**. Do you want to use advanced customization techniques (the HideRememberPassword option in the service profile) to disable the Save Password option for clients (which will also prevent automatic connections)?
- **Authentication and Authorization protocols**. Do you want to use advanced customization techniques to specify the authentication and authorization protocols to be used or to enable support for LCP extensions?
- **Code signing**. Do you want to sign the code with a digital signature before distributing it?

  Guidelines To prevent unauthorized access to the enterprise network, always disable the save password feature for connections to the enterprise, especially on portable computers.

  Use the most secure authentication and authorization protocol that the client supports.

  You should digitally sign your customized service profile and any custom programs to ensure that users do not receive warnings when they install Connection Manager. If not, users might be prevented from installing ActiveX controls and Java packages that are not signed.

Distribution of Client Software

You can specify options to make distribution and installation most effective, such as:

- **Connection Manager 1.2**. Do you want to include the Connection Manager 1.2 software in your service profile to provide support for users who are not running Windows 2000 and do not already have Connection Manager 1.2 installed?
- **Service profile distribution**. Do you want to distribute the service profile on floppy disk, on CD, by e-mail, by posting to a web site, by file server, or by using Microsoft Systems Management Server for installation?

Developing Specifications for Support Tools and Custom Software

A variety of tools is available to support implementation, administration, and management of your remote access solution. These tools include component Software Development Kits (s) provided for Windows 2000 in the Microsoft Platform SDK, support provided in Windows 2000, and additional in-house and third-party tools. Determine which tools and custom software you require, and then develop design specifications and implementation specifications for each.

Software Development Kits

Windows 2000 Server provides extended support for developing custom components and support for remote access solutions, including Software Development Kits (SDKs) for IAS and Routing and Remote Access. The Microsoft Platform SDK includes the following support:

- The Internet Authentication Service (IAS) application programming interface (API) enables software developers to write their own extensions to IAS. You can use the extensions to IAS to:
  - Return custom attributes to the remote access server in addition to those returned by IAS. This supports building custom plug-ins for assigning IP addresses.
  - Control the number of end-user network sessions, using a state server.

  - Extend the remote access authorizations provided by IAS (on Windows 2000 Server only).
  - Connect to Windows NT Domain authentication databases and Active Directory in Windows 2000 Server.
  - Import and audit data directly in an open database connectivity (ODBC)-compliant database.
  - Create custom authentication methods for Windows NT 4.0 Service Pack 5, and Windows 2000.
- The Routing and Remote Access Service API makes it possible to create applications to administer the routing and remote access service capabilities of Windows 2000 Server. You can use Routing and Remote Access Service API to implement your own protocols, including custom EAP functions that you can use to program authentication protocols, authentication providers, and accounting providers.

After examining these SDKs, determine if you require the additional functionality provided there and, if so, develop specifications for developing the extensions.

Windows 2000 Support Tools for Remote Access

Windows 2000 Server includes the following administration and management tools to support remote access:

- Routing and Remote Access and IAS administrative tools are the primary administration and management tools, both of which are implemented as snap-ins in Windows 2000 Server. With these tools, you can set up and maintain the Routing and Remote Access service, RADIUS clients, and IAS servers. Not all the capabilities of the Windows 2000 Server administration tools will work when administering a Windows NT 4.0 Routing and Remote Access (RRAS) router or a Windows NT 4.0 Remote Access Service (RAS) server. For more information about administration tools in mixed environments, see Windows 2000 Server Help.
- The Netsh command-line utility can be used to locally configure Windows 2000 Server remote access service from a Windows 2000 command prompt and can use script files to automate configuration tasks. For more information about Netsh commands for remote access, see Windows 2000 Server Help.
- CMAK is used to create custom client connection software.
- Phone Book Administrator (PBA) is used to specify the phone book entries for Connection Manager.
- You can monitor the health and performance of an IAS server using either Windows 2000 Server Performance Monitor or the Windows 2000 Server Simple Network Management Protocol (SNMP) agent and the built-in support for industry-standard RADIUS management information bases (MIBs). The two most commonly used counters for IAS performance monitoring are:
  - Access Requests/sec
  - Accounting Request/sec
- To help you gather information to troubleshoot problems with the remote access server, you can also use the following tools in Windows 2000 Server:
  - Authentication and accounting logging for remote access servers provides details of all access attempts, as covered earlier in this chapter.
  - Event Viewer provides application, system, and security logs of errors, warnings, and events that can be used to analyze hardware, software, and system problems and to monitor Windows 2000 security alerts.
  - PPP logging creates a log file of the PPP control messages that are sent and received during a PPP connection.
  - Tracing records the sequence of programming functions called during a process to a file.
- You can interpret IAS log data using iasparse.exe on http://www.microsoft.com .

For more information about the various administration tools provided with Windows 2000 Server, see "Deployment Tools" in the *Deployment Planning Guide*.

Additional Support Tools

In-house or third-party tools can also be appropriate to meeting your implementation goals. Determine which tools you need and how they are to be implemented. In particular, you should determine the tools that are to be used to analyze and report logging information. Although Windows 2000 provides extensive logging data, the information is useful for security monitoring and accounting only if it can be efficiently analyzed and understood.

Testing Your Dial-Up Design

Ensure that all remote access testing includes:

- All remote access policies to be implemented
- All protocols and encryption methods

Testing is critical to the security of any external connectivity solution and is important for ensuring that functionality works as planned. First, simulate both internal and external connections to prevent exposure and corruption of any part of your network in the event of problems.

Note To isolate problem areas, perform initial testing with a single NAS, a single client, a single location, and a single domain. Add components and locations only after the successful completion of the initial testing.

Guideline Test NASs locally first. Install and test each of your NASs (through local use) before making them RADIUS clients.

If you are implementing both dial-up and VPN solutions, test the dial-up solution before the VPN solution. If the solutions are to be integrated, test them together after testing them individually.

Identify troubleshooting procedures that are specific to dial-up access components, including all hardware and software that is to be deployed. For example, define separate troubleshooting procedures for analog and ISDN modems. Provide the final troubleshooting procedures to your customer support center so that they can use these procedures in the pilot and rollout phases of your deployment.

Implementing Your Dial-Up Client Access Design

To successfully implement external connectivity solutions in your environment requires that your network administrators must:

- Prepare the environment for implementation
- Develop custom software to support dial-up client access
- Install and configure solutions
- Validate the deployment
- Stabilize the environment

Members of your organization might go through these steps multiple times to successfully implement (pilot and rollout) a remote access solution.

Preparing for Implementation

Preparing for implementation requires that your core networking environment is stabile. The integration of Routing and Remote Access with other Windows 2000 Server components (including DHCP, WINS, DNS, and Active Directory) creates dependencies on these other components. If they are not fully deployed and stabilized, implementation of any Windows 2000-based remote access solution can be jeopardized.

Ensure that all plans and designs are finalized and that your pilot rollback plan is completed and covers both component-level and system-level rollback requirements.

Also before you start your implementation, ensure that all accounts and domains are set up in the enterprise network. Get the IP addresses from the appropriate network administrator.

Developing Custom Software to Support Dial-Up Client Access

You need to develop the custom software that you identified as appropriate during the design phase, including doing the following:

- Develop the SDK extensions for Internet IAS or Routing and Remote Access service.
- Install and run the CMAK Wizard to create the required Connection Manager service profile(s), based on the worksheet you completed during the design phase. This wizard is a Windows component that can be installed using Add/Remove Programs to add the Connection Manager components of Management and Monitoring Tools. Start the wizard from Administrative Tools.
- Install and run the Phone Book Administrator (PBA) to create the required phone book(s) so that it is ready to be posted to the server. Install PBA from the Valueadd directory of the Windows 2000 Server operating system CD. Start the wizard from Administrative Tools.

  Note At this point, build the phone book, but do not post it yet. Posting cannot be done until the Connection Point Services (CPS) server running PBS has been set up. This is done as part of the implementation process, covered later in this chapter.

  Guidelines Set up File Transfer Protocol (FTP) permissions and write access to FTP before attempting to publish phone books to PBS.

  Secure the PBA and PBS folders to avoid synchronization problems and to prevent unauthorized personnel from posting to the host server.

  Back up your phone book databases and other important files to preserve POP and region information.

  If you want to import phone book data, do it before you first post the phone book. You can import up to 32,000 POPs before posting, but only 6,000 POPs for each subsequent post.

  For more information about how to implement each of these Connection Point Services guidelines, see Windows 2000 Server Help.
- Develop Connection Manager extensions. There is no CMAK SDK, but the information needed to provide auto-installation of a Connection Manager service profile using command-line parameters for CMAK can be found in the Windows 2000 Server Help. For information about how to use the Internet Explorer Administration Kit to integrate Connection Manager with an Internet Explorer installation package, see the *Microsoft® Windows® 2000 Server Resource Kit Internet Explorer 5 Resource Kit*.
- Develop and/or acquire additional tools for accounting and other administrative support.

Installing and Configuring Dial-Up Access Components

The method of setting up RADIUS-compliant remote access connections using Routing and Remote Access services, IAS, and Connection Manager varies, based on your deployment plans. The information in this section provides a general approach to deployment of a dial-up client access solution.

Preparing Network Components

Before installing and configuring Routing and Remote Access services, IAS, and other Windows 2000 components of your dial-up client access solution, install the server-side components required to create the basic network infrastructure for your dial-up solution. This includes all server hardware and operating systems, as well as the drivers, adapters, and connections required to enable network connections.

Server Components

Install the operating systems and/or drivers for the following components:

- IAS servers.
- Remote access server(s).

  Note If you are using the Windows 2000 mixed-mode administrative model, you must configure support for remote access servers running Windows NT 4.0. For more information about providing support for Windows NT 4.0 remote access server in a Windows 2000 domain, see Windows 2000 Server Help.
- Phone book servers.
- Client computers.
- Routers.
- LAN adapter cards with certified Network Driver Interface Specification (NDIS) drivers.
- Modem bank with appropriate connections to a local telecommunications provider and a compatible adapter.

  Note To ensure modem compatibility, clients and servers should use the same kind of modem. This is not critical if your modems conform to industry standards, but it is still safer to choose the same model for both clients and servers.
- Multiport adapter for acceptable performance with multiple remote connections.
- ISDN adapter (if you are using an ISDN line).
- WAN connections.
- Encryption pack, if appropriate.

  Note To use the encryption pack, you will first need to download it from http://www.Microsoft.com .

WAN and Internet Connections

Configure the drivers for the modem bank adapter and ensure that it appears as a device with multiple modem ports.

On each LAN adapter that you install in the remote access and IAS servers, configure the following TCP/IP settings:

- IP address and subnet mask from the network administrator
- Default gateway of the local router

- DNS and WINS name servers

Configuring the Servers

Install and configure the required software on all servers. This includes remote access servers and RADIUS (IAS) servers, as well as all enterprise servers that are required to support the dial-up client access infrastructure, including the domain controllers.

Remote Access Servers

When you install Windows 2000 Server, the remote access component is automatically installed. However, the Routing and Remote Access service is installed in a disabled state.

To configure and start a dial-up remote access server, from the **Administrative Tools** menu open **Routing and Remote Access**, right-click the server name, and then click **Configure and Enable Routing and Remote Access**. Complete the **Routing and Remote Access Setup Wizard** to set up the protocols and IP addresses, and to specify the use of RADIUS. Do not configure the remote access policies yet.

Note If you need to install more protocols, from the **Start** menu, point to **Settings**, click **Network and Dial-Up Connections**, click **Local Area Connection**, and then click **Properties**.

When you start a remote access server for the first time, Windows 2000 Server automatically detects any modems that are installed and creates modem ports for them. Windows 2000 Server also creates ports for each parallel or serial cable connection that it detects. You can also configure the properties for these ports manually.

All of the modem bank ports are listed as separate ports under **Ports** in Routing and Remote Access. You should configure all the modem bank ports for remote access. For more information about how to configure ports on a remote access server, see Windows 2000 Server Help.

IAS Servers

First, verify that the IAS server is a member of the forest against which IAS will authenticate remote users. This is important since a trust relationship is required and all domains in Active Directory forests automatically have trust relationships with each other. If IAS and the user account are not in the same forest, the domain for the user account must have a trust relationship with the domain of which IAS is a member.

Next, log on with Local Administrative credentials, install IAS as an optional component, and then configure the following:

- IAS properties (including ports, realm stripping, as appropriate).
- RADIUS clients (adding one for each remote access server).

  Note Ensure that the authentication and accounting shared secrets in IAS match those specified for the remote access servers.
- Remote access policies (adding one per group or type of connection to be supported).
- Reversibly encrypted passwords (if using CHAP).
- Logging for user authentication and accounting.
- Event logging for IAS.

For more information about how to configure each of the above items, see Windows 2000 Server Help.

Use the netsh command to copy the client configurations, remote access policies, registry, and logging configuration to the backup IAS server. For more information about how to copy the IAS configuration to another server, see Windows 2000 Server Help.

Domain Controllers

To be able to authenticate users, the primary and backup IAS servers must be registered on the domain controllers in Active Directory in the built-in groups as members of the **RAS and IAS Servers**. If you are not a domain administrator, instruct your domain administrator to add the computer account of both IAS servers to the **RAS and IAS Servers** security group in the domain of which the servers are members. The domain administrator can add the computer account to the **RAS and IAS Servers** security group by using the Active Directory Users and Computers administrative tool or with the **netsh ras add registeredserver** command.For more information about how to register IAS servers with Active Directory by enabling the IAS server to read user objects in Active Directory, see Windows 2000 Server Help.

First, verify that the remote users are in the appropriate universal and nested groups, and that the computer on which IAS is installed has permission to read the user objects in the domain. Next, verify that the user's permissions have been set to allow dial-in access (either by user or based on remote access policies), and that the user names and passwords are valid (by testing their logon capabilities on the LAN). Ensure that the user's dial-in permission is configured appropriately.

If you specify that CHAP is to be supported, you need to configure support for reversibly encrypted passwords. For more information about CHAP, see Windows 2000 Server Help.

Log on to each remote access server using domain administrator credentials and open Routing and Remote Access. Verify that the properties for each remote access server are correct.

PBS Servers

Install and configure the Connection Point Services (CPS) Phone Book Service (PBS) as a Windows 2000 Server optional component and then post your phone book from Phone Book Administrator (PBA) to the server. To do this, set up an administrative account for your PBS host and set permissions, including administrative permission for the PBS folder, FTP accounts for known users, and write permissions for the FTP virtual directory.

Note Before anyone attempts to post to the server, verify that you have set the Write permission for the FTP virtual directory. Set this permission right before posting a phone book and clear it immediately after posting the phone book.

For more information about how to install and configure PBS and PBA, including how to set permissions and how to create and manage phone books, see Windows 2000 Server Help.

Configuring Addressing and Routing

Configure the methods of obtaining IP addresses and any static routes, as appropriate. Verify all routing before implementing the client-side components.

IP Addressing

Configure routing as follows:

- If the remote access server is using DHCP to obtain IP addresses for remote access clients, configure the DHCP Relay Agent. For more information about how to configure the DHCP Relay Agent, see Windows 2000 Server Help.
- If the remote access server is using a static IP address pool to obtain IP addresses for remote access clients, configure the DHCP Relay Agent with the IP addresses of each DHCP server to be used. For more information about how to configure the DHCP Relay Agent properties, see Windows 2000 Server Help. Configure a static IP address pool (with a starting address and an ending

address) to create an access pool for the required number of remote access clients.

Routing

To reach intranet locations, configure a static route on the remote access servers. To reach remote access clients, configure a static route on the router.

Note This is only necessary if the static pool is an off-subnet address pool.

Implementing Client Components

After server-side components are installed, distribute, install, configure, and test client-side components. This includes the client connection software and any additional components required for your implemention.

Client Connection Software

Distribute the client software (each service profile you have created), have users install the service profile, and verify that the remote dial-up users can use it to access the network.

For more information about how to prepare for delivery and installation of Connection Manager service profiles, see Windows 2000 Server Help.

Additional Components

If implementing high encryption, ensure that client machines have the appropriate software to support the specified encryption method.

If users require phone books (that were not delivered in the service profiles), ensure that users are provided information on the automatic down-load process for phone.

Validating Dial-Up Access Deployment

Successfully managing outsourced remote access requires ongoing tracking of implementation status and identifying changes required to meet evolving requirements, including continued capacity planning, performance optimization, and planning for future updates. To do this requires:

- Continuous risk mitigation.
- Performance monitoring.
- Data collection and analysis.
- Verification of functionality, security, availability, management and performance.
- Identification of design inconsistencies.

Effective management might require updating the business strategy or just fine-tuning the design.

Stabilizing the Environment

To identify ways to stabilize the environment and to create the basis for future deployment efforts, determine the best ways to:

- Analyze network communications process.
- Analyze outbound connections.
- Analyze inbound connections.
- Identify critical decision points.
- Identify interoperability and migration issues.
- Validate protocols.
- Streamline operations.
- Integrate other connection types (ADSL, 56K, ISDN with Multilink, cable modem, etc.) and solutions (such as VPN and extended security features).
- Enhance RADIUS performance.
- Enhance RADIUS availability.
- Optimize routers.
- Provide the optimum number of servers and other remote access equipment.
- Reduce costs, especially long-distance costs.
- Tailor Connection Manager profiles for group-specific requirements.

Scenarios

The Microsoft Windows 2000 Resource Kit Deployment Lab Scenarios include a variety of scenarios on key aspects of Windows 2000 deployment. Windows 2000 Resource Kit Deployment Lab Scenarios document solutions that provide example configurations showing the deployment of Windows 2000 technologies on an actual network, simulating a large organization and the Internet. One of the scenarios provided there is "Connecting Dial-Up Remote Access Users to an Intranet." This scenario shows how a specific set of requirements and objectives can be met by Windows 2000 dial-up client access solutions. Table 5.10 summarizes sample enterprise requirements that are supported by the scenario.

Table 5.10 Remote Client Access Requirements and Goals for the Organization in the Scenario

Area	General Requirements and Goals in this Scenario
Business	Provide a method for specific user groups to work remotely without negatively impacting their productivity or the quality of their work products. The long-term goal is to enable: • All local sales personnel to work remotely 95 percent of the time. • All corporate personnel to telecommute 20 percent of the time. • Local consultants to connect from their individual locations, working remotely 90 percent of the time, with no in-house office requirements. Ensure security of all external information and applications accessed remotely (especially research and development information) by allowing only encrypted passwords and data.
User	Provide 300 members of sales team with the software and portable equipment required to access sales order databases, reporting tools, product information, and e-mail at the central corporate location. Provide 10,000 corporate personnel with the software and home PCs required to access the central network, including all applications used in-house.

	Provide each corporate department with portable computers for employees to use while traveling. Ensure that remote access client software does not require users to be technically competent.
IT	Provide sufficient bandwidth and performance to support real-time requirements of all users. Provide fully staffed technical support during business hours and emergency support for all other times. Implement a system that can be centrally managed.

Table 5.11 shows a sample of measurable objectives developed to reflect the enterprises's implementation requirements.

Table 5.11 Remote Client Access Objectives for the Organization in the Scenario

Area	Objectives
Functionality	Support dial-up clients with a mixture of 33.6 Kbps and 56 Kbps analog modems. Log 100 percent of access attempts, and analyze all data within 24 hours of logging to determine inappropriate access attempts. Use existing remote access servers where possible. Use Active Directory to control user access.
Security	Support a minimum of 40-bit encryption for 100 percent of remote communications authentication and data. Provide access to the network strictly on an as needed basis; not all remote client access users need access to all areas of the network. For users with access to sensitive areas of the network, only allow access if using 128-bit encryption. Provide real-time analysis of access logs to alert support personnel within 10 minutes of any significant unauthorized access attempts
Availability	Provide access support, 24 hours a day, 365 days per year. Ensure that reliability is 98 percent or greater.
Performance	Ensure that access can be established within 2 minutes, and wait times for execution of any single transmission are less than 30 seconds for 95 percent of activities. Provide dial-up access support for up to 10,000 users, with up to 100 simultaneous remote clients accessing the system at any time.
Management	Ensure that 95 percent of users are able to install and run the client software with no calls for assistance and a maximum of 10 minutes for setup and initial connection. Manage 90 percent of corporate NAS administration from a single central location. Enforce account lockout any time that three successive attempts to make a remote connection to a user account fail. Provide reports of access problems daily and make summaries of problem areas to management weekly. Maintain and update client software with only minimal user involvement.

Table 5.12 shows additional sample objectives for a single group, specifically a group of sales representatives with local territories.

Table 5.12 Sample Group Objectives for Sales Representatives with Local Territories

Area	Objectives
Functionality	Support local sales representatives accessing the network by using laptop computers and public switched telephone network (PSTN) technology for dial-up connections. Support remote access to shared folder resources on Windows 2000 and Novell NetWare 3.*x*–based servers, and to Web-based applications and files
Security	Restrict access by local sales representatives to the sales/order database and the internal e-mail servers.
Availability	Support remote access to corporate resources, regardless of a single server failure, for at least 300 remote staff members, with 99.9 percent or greater reliability.
Performance	Support download of weekly sales charts by sales representatives with a maximum of 5 minutes required for any single download. Support sales representatives access to order information, with a maximum of 2 minutes required to obtain access. Support multimedia presentations requiring sustained 28 Kbps throughput.
Management	Update phone book access numbers within 24 hours of availability of new access points, with daily user access. Enable sales representatives to set up client software in 10 minutes or less, regardless of technical background. Enable automatic phone book maintenance and updates that can be completed in less than 1 minute, with no user action required other than logging on to the network.

Sample Design for Dial-Up Client Access

To meet these objectives, the enterprise decides to implement the following:

- Remote access servers, each running the Routing and Remote Access service component of Windows 2000 Server and connected to the LAN. The remote access server operates as a RADIUS client and is responsible for passing user information to the appropriate RADIUS servers (IAS), and then acting on the response.
- Primary and backup IAS servers, each running Windows 2000 Server and connected to the local area network.
- Connection Manager connection software to support standard dial-up access capabilities using PPP and providing a Connection Point Services phone book containing both primary and backup access numbers. All users are divided across all remote access servers; for each group, one of the servers is designated as the primary remote access server.
- Windows 2000 Professional clients.

An example of how to implement an IAS-based dial-up solution that supports the above objectives is covered in the Microsoft® Windows® 2000 Resource Kit Deployment Lab Scenario, "Connecting Dial-Up Remote Access Users to an Intranet," which can be found at http://www.reskit.com .

The design and implementation for any dial-up client access solution is dependent on the requirements of the environment and the decisions made to support those requirements. For more information, see Windows 2000 Server Help.

Related Information in the Resource Kit

- For more information about the Internet Authentication Service (IAS), see "Internet Authentication Service" in the *Internetworking Guide*.
- For more information about using the Routing and Remote Access service as a remote access server, see "Remote Access Server" in

the *Internetworking Guide*.

- For more information about virtual private networks (VPNs) and remote access security, see "Expanding and Securing Remote Client Access."

Send feedback to Microsoft