Dial-Up Networking overview

Dial-Up Networking is the client version of Windows NT Remote Access Service (RAS).

Dial-Up Networking lets you connect to your office network from a remote site, such as your home, a hotel, or anywhere there is an outlet for your computer and phone jack for your modem. Dial-Up Networking works by calling the dial-up server and establishing a telephone connection with the network. Once you have connected, you work with all your applications as though you were physically in the office, directly connected to the network or local database.

For example, you can:

- Access remote databases through the Windows NT Explorer.
- Send and receive electronic mail.
- Print files on the office printer.

Dial-Up Networking clients can use TCP/IP, IPX, or NETBEUI to connect to any SLIP, PPP or Microsoft RAS server over a modem, ISDN line, X.25, or PPTP connection.

Microsoft does not support access to Macintosh volumes and AppleTalk printers over dial-in lines.

A list of all the entries in the current phonebook. Select an entry and then click **Dial**. You can also edit, clone, or delete entries by clicking **More**.

The default phonebook is the system phonebook (rasphone.pbk). To select a different default phonebook, click **More** and choose **User preferences**. In the **Phonebook** tab select a personal or alternate phonebook.

Click to add an entry to the phonebook.

Click to see more commands such as edit, delete, or clone an entry.

Displays the complete number that will be dialed, including prefixes, suffixes and telephony dialing properties. Click **Location** to change how the number appears or type a new number in the box to temporarily override the number associated with the entry.

Specifies the location from which you are dialing.

If you have a laptop computer, it might be useful to set location properties for your various locations, such as your office, home, or hotel. Thus, depending on your location setting, your phonebook entries can be customized to use specific area codes or calling card numbers.

Click to change the properties of the selected location or create a new location.

The dialog box that appears depends on whether or not you selected the **Use Telephony dialing properties** check box in the **Basic** tab. By default, this check box is not selected and the prefix and suffix controls from previous versions of RAS are available.

Select the check box if you want to use the telephony dialing features. The circumstances when you might want to use these features are when you are calling long distance or using a credit card.

Click to dial the phonebook entry selected in the **Phonebook entry to dial** box.

Click to close the dialog box

Type the name of the entry you want to dial (company name or server name). Choose any name you like, from 1 to 256 characters. Typically, the name of the remote server or the type of connection is a good choice, for instance, "PPP Internet connection" or "SLIP Internet connection".

This name appears in the phonebook list.

An optional box for you to store notes on the entry.

Choose the country of the dial-up server you are calling.

Type the area code of the dial-up server you are calling.

If the dial-up sever is in a country other than the United States, type the city code here, but do not include the leading 0. For example, if the city code is 071, just type 71.

Type the phone number of the dial-up server. See Phone Number Modifiers for special command sequences.

Click to add secondary phone numbers to the entry. If the first phone number cannot be reached, the secondary phone numbers are dialed until a successful connection is made.

Select the preferred device to dial. If the first device fails, any other devices of the same type will be used to try to make a connection if you select the **Use another port if unavailable** check box.

In the **Dial using** box you can also select multiple lines to be used when you are dialing. This uses Multilink functionality which combines multiple physical links into a logical ‘‘bundle’’ to create an aggregate link that increases your bandwidth.

To use Multilink, both the clients and servers must have Multilink enabled.

Click **Configure** to choose which modems or adapters to use for the connection.

Click to configure device-specific settings. For example, if you are using modems to make a connection, click to set the speed of your modem and enable modem compression.

Select this check box to use the telephony dialing features. These are useful when you are calling long distance or using a credit card. Selecting this check box brings up the telephony dialing page when you click **Location** in the **Dial-Up Networking** dialog box. If you do not select this check box, the prefix and suffix controls from previous versions of RAS appear when you click **Location**.

Do not select this check box if you are dialing a number within your internal corporation.

Choose the dial-up sever type. If you are not sure, choose **PPP**. If you are calling a SLIP server, choose SLIP. If you are dialing a server that uses an older RAS protocol, you should choose **Windows NT 3.1**, **Windows for Workgroups 3.11**.

Some of the protocols and other options in the **Server** tab may not be available depending on your selection.

Network protocols are the protocols you use to communicate with servers on the LAN once you are connected to a dial-up server. See your network administrator if you do not know which protocol to select.

You can select more than one protocol. Protocols already installed on the computer will be checked by default.

The Transmission Control Protocol/Internet Protocol (TCP/IP) is a networking protocol that provides communication across interconnected networks.

TCP/IP is the suite of network protocols used on the Internet.

The NetWare suite of protocols used in a Novell network.

NetBEUI is network protocol native to Microsoft Networking. This protocol is the Microsoft implementation of the NetBIOS standard.

Click to set TCP/IP settings for the phonebook entry. If you are calling a Microsoft server (Windows NT, Windows 95, Windows for Workgroups, or other Microsoft RAS server) you do not need to configure TCP/IP settings.

Dial-Up Networking offers software data compression in addition to supporting modem compression. So, you do not have to turn on modem compression to benefit from a faster throughput.

Select this check box to enable software compression.

For recommendations about getting the most out of compression, see Compression Recommendations.

Select this check box to enable newer PPP features. These extensions may cause problems when calling servers with older PPP software. Clear the check box only if consistent problems occur.

Clearing this check box prevents LCP from sending Time-Remaining and Identification packets and requesting callback during the LCP negotiation of PPP.

Select this check box if you do not want to use a script or terminal after dialing.

Select this check box to use a terminal box after dialing.

See Using RAS Terminal for Remote Logons

Select this check box to use a script after dialing.

Select which script to use after dialing. These scripts are part of Switch.inf, in which you can modify or create new scripts.

See Automating Remote Logons Using SWITCH.INF Scripts

Click to instantly access Switch.inf in order to modify or create new scripts.

Click to update the script list box after editing Switch.inf.

Click to use a script before dialing, for instance, when using an intermediary device on the client side.

You can choose the rules used to negotiate authentication and encryption with the dial-up server. Authentication deals with verifying clients to servers and setting encryption prevents someone from monitoring data on the communication line.

Permits connection using any authentication requested by the server (MS-CHAP, MD5-CHAP, SPAP, PAP). This setting is the most permissive and can be used when you are not worried about passwords. This option is useful if you are calling a non-Microsoft server.

Permits connection using any authentication requested by the server except PAP.

This option is useful if you are calling a non-Microsoft server and do not want to transmit clear text passwords on the communication line.

Permits connection using MS-CHAP authentication only.

This option is useful if you are calling a Microsoft server. You can also choose to use data encryption or change password support over Dial-Up Networking.

All data sent over the wire is encrypted. This option is available only on Windows NT version 3.5 or later RAS computers. Windows NT RAS provides data encryption using the RSA Data Security Incorporated RC4 algorithm.

If you select this check box, the connection will hang up if it does not encrypt.

This option is an optimization appropriate for those using a home computer as an alternate workstation on an office network. Selecting this option causes the credentials entered at CTRL+ALT+DEL logon to be used for the RAS connection. This setting eliminates the need to logoff/logon when you are attempting a RAS connection after the account password has been changed on the office workstation.

If you have previously chosen to save your password in the dialog box that prompts you for your username, password and domain when dialing an entry, you can click to erase that password.

Choose the name of the X.25 network you are calling.

Enter the X.25 address (the X.25 equivalent of a phone number) for the dial-up server you want to call.

Filling in these boxes is optional, in most cases you do not need to type anything further.

Enter additional connection information required by the X.25 host computer. Typically, you should leave this field blank unless your system administrator advises otherwise.

Enter any additional facility parameters you want to request from your X.25 provider. For example, some providers support **/R** to specify reverse charging. For details, consult your X.25 documentation or provider.

Select this check box to view and edit the phone` number you are dialing in the **Dial-Up Networking** dialog box.

Clear the check box to prevent the phone number from being displayed in the dialing status popup during the connection sequence.

Select this check box to view and edit the location setting in the **Dial-Up Networking** dialog box.

Select this check box to start Dial-Up Networking Monitor before dialing a number.

Select this check box to see the connection status during a call.

Clear the check box if you prefer connections to silently connect and show status only when success or failure has been determined This is most useful with Autodial.

Select this check box to close Dial-Up Networking after a successful connection.

Select this check box to enable you to edit the Dial-Up Networking phonebook when you are logging in to Windows NT and have selected the **Logon using Dial-Up Networking** check box.

Select this check box to enable a user to create new TAPI dialing locations when a user is logging in to Windows NT and has selected the **Logon using Dial-Up Networking** check box.

Clear this check box to prevent a user that is logging in from changing the dialing locations or creating a new location.

Select this check box to use the Dial-Up Networking wizard to create new phonebook entries.

Select this check box to receive a prompt before a connection is automatically established. This feature is useful for tracking every autodial connection and being aware, for instance, that an expensive ISDN line is being used.

The Remote Access Autodial service must be running in order for this option to take effect.

Select each location where you want to enable RAS Autodial.

RAS Autodial maps and maintains network addresses to phonebook entries, allowing them to be automatically dialed when referenced-whether from an application or from the command line. A network address can be an Internet host name, an IP address, or a NetBIOS server name.

The Remote Access Autodial service must be running in order for this option to take effect.

See RAS Automatic Dialing

Specify the number of times to automatically redial the number. No redial means zero.

Specify the number of seconds to wait before automatically redialing. This gives the remote device time to reset.

Specify the amount of idle seconds before a connection hangs up.

Keep in mind that the dial-up server also has a disconnect timer. If this control is set to a high timeout number, there is no guarantee that the connection will not disconnect before the time passes. This is because the server may choose to disconnect you before the time set here.

The Remote Access Autodial service must be running in order for this option to take effect.

Select this option if you do not want the dial-up server to call you back.

This option is for the convenience of a remote user who calls from various places. It is not a security feature. Select **Set By Caller** for clients that call from various locations and different phone numbers. When the user's call reaches the remote access server, the following steps occur:

1 The server first determines if the user name and password are correct.

2 If they are, the **Callback** dialog box appears on the user's computer.

3 The user types the current callback number in the dialog box and waits for the server to return the call.

Set this option to minimize telephone charges for anyone calling in from various locations, such as field representatives.

Select this option if you want the dial-up server to ask whether or not you want to be called back during the connection process.

Select this option if you want the dial-up server to call you back. You must then supply phone numbers for each device.

Select the device to be used during callback and click **Edit** to enter a phone number.

Click to enter a phone number for the dial-up server to use when calling you back.

Click to delete the selected device from the callback list.

Enter the number for the dial-up server to use when calling you back.

Use the following options to select the default phonebook for use in the **Dial-Up Networking** dialog box.

Select this option to use the system phonebook. This is the default phonebook (rasphone.pbk in the \SYSTEM32 folder)

Select this option to use a personal phonebook. A personal phonebook is created with protection mode so that another user who logs on to the same computer will not be able to see your phonebook. Password protection mode only works on NTFS file partitions.

Select this option to use a phonebook that is located outside the \SYSTEM32 folder. For example, a phonebook on another computer.

Select a phonebook from the list or type the complete path to the phonebook.

Click **Browse** to search for a phonebook.

Click to find other phonebooks on your computer or to see a list of phonebooks on other computers.

Select the type of ISDN connection. The choices are in order from the highest quality (64K Digital) to the lowest (56K Voice).

Select this check box to start at the selected line type and negotiate to a lower quality line type, depending on the line's condition.

Note: Some ISDN cards negotiate both the line type and the number of channels if the Negotiate line **type** check box is selected. In other words, not only will the card start negotiating at highest quality line type (64K digital) and fall back to lowest quality (56K voice), but in many cases it will also fall back from multiple channels to fewer channels if necessary.

Select this check box if the server you are dialing into supports only proprietary protocols. For instance, using DigiBoard devices on both the server and the client.

Clear this check box to use Multilink over multiple ISDN lines. Multilink does not require proprietary protocols on the server or client.

Select this check box to compress data before transmitting it. If you enable hardware compression, turn off software compression.

Note: Not all ISDN cards offer hardware compression. If this feature is turned on and your card does not offer compression, your data throughput will not improve. If you do not know whether your card has compression, check with the card's manufacturer.

If your card allows you to aggregate more than one ISDN channel, and the remote access server's ISDN card is configured to allow channel aggregation, you can select more than 1 channel to improve throughput. See the section "ISDN Phone Numbers" in Adding/Editing/Cloning an Entry.

Not all ISDN drivers let you restrict channel aggregation. If you have a non-restricting driver and your computer is configured to receive calls, ask clients dialing in to specify only one or two channels. Otherwise, one user with several ISDN cards could monopolize all channels on the server.

Note: You cannot connect through more channels than the number available on your ISDN card(s). In fact, selecting more than the maximum available may prevent you from connecting.

Displays the installed modem.

Note: To change your modem or install a new modem, choose the Network icon in Control Panel. In the **Services** tab, select **Remote Access Service** and then click **Properties**. See the online Help in the dialog boxes for more information.

Select the speed at which your modem begins to negotiate with the remote access server's modem. The speed, in bits per second (bps), may increase or decrease during negotiation.

Selecting a hardware feature that is not supported by your modem has no effect on performance.

Select this check box to enable hardware handshaking. This feature enables the modem to tell remote access software when the line is congested or clear, so that the remote access software can temporarily stop transmitting data when necessary. This handshaking streamlines data transmission, prevents overrun errors, and thus improves overall data throughput.

Select this check box to check errors on blocks of data through cyclic redundancy checks (CRCs). Modem error control causes the modem to retransmit garbled data, ensuring that only error-free data passes through the modem. For more information, see MNP4 and V.42.

Select this check box to compress the modem-to-modem data stream, reducing the number of bytes transmitted and therefore reducing the transmission time. The reduction achieved depends on the amount of redundancy in the transmitted data.

Note: Software compression is more effective than hardware compression because a much larger pattern buffer is available on the computer than on the modem. In addition, modem compression delays the first transmission while the modem's pattern buffer is filled at computer-to-modem speed. Software compression accomplishes this task at the much faster memory speed and transmits compressed data over the entire computer-to-computer link rather than just the modem-to-modem segment.

In general, you should not enable modem compression and software compression at the same time, because no benefit is gained from compressing pre-compressed data. In fact, it may actually increase the size of the transmitted data, depending on the algorithm used by the modem.

Select this check box to enter AT commands to the modem manually when dialing rather than executing the scripted commands. Enable this feature when testing modem strings for new entries in the modem script file (MODEM.INF) and for unusual situations where interaction is required midway in the dial sequence.

In general, do not enable this feature when dialing with the telephone keypad, for example, when connecting through a switch controlled by a human operator.

Select this check box if you do not want to hear the modem dial tone and connection sounds.

Your Windows NT domain password has expired. Please change your password now by filling in the fields in this dialog box. Passwords are case-sensitive. Remember your use of uppercase and lowercase letters when you type a new password.

Type the current password.

Type the new password.

Type the new password again to confirm it.

The dial-up server is configured to call you back at a number you specify for convenience purposes, such as reversing the calling charges.

You can automatically answer this dialog box by choosing the **User preferences** command from the **More** button and then selecting options in the **Callback** tab.

Type the number at which you want the remote access server to call you back.

Your modem (or other connecting device) has reported an error. If you are using a supported modem, turn the modem off and then back on. Close and restart the Remote Access Service, and then redial.

If your modem is not supported by Remote Access, contact your modem's manufacturer. For a list of supported modems, see the Windows NT Hardware Compatibility List.

Make sure you have correctly configured your modem for Remote Access. To check your configuration, see Reconfiguring Dial-Up Networking.

Counts down the number of seconds until redialing based on settings in the **Dialing** tab in the **User preferences** dialog box.

At least one of the protocols selected for the entry failed to connected.

Click **Accept** to connect using the protocols shown.

Select the check box to use only the protocols that connected the next time you dial. Or, to change the connection protocols for an entry, in Dial-Up Networking, select an entry and click **More**. Select **Edit entry and modem properties**. In the **Server** tab, select the network protocols you want to use for the connection.

Click to connect using the protocols shown.

Click to hang up the connection.

Select this check box to use only the protocols that connected the next time you dial.

To change the connection protocols for an entry, in Dial-Up Networking, select an entry and click **More**. Select **Edit entry and modem properties**. In the **Server** tab, select the network protocols you want to use for the connection.

Dial-Up Networking Authentication credentials are typically the same as your network logon credentials. Dial-Up Networking uses these credentials to verify that you have the right to physically access the network. Dial-Up Networking does not actually log you on, so after your connection is established you may need to log on (by pressing CTRL+ALT+DEL for Windows NT) to access protected network resources.

Type your remote access user name.

Type your remote access password.

If you are calling a non-Microsoft server, you do not have to enter a domain.

If you are calling a Microsoft server, the domain name you enter should be the Windows NT domain that the Windows NT RAS server or your Dial-Up Networking account is in. This is not the DNS domain name given by some PPP/SLIP providers. For example, you would enter accounting, not www.halcyon.com. For information about domains and trust relationships, see the *Windows NT Server Concepts and Planning Guide*.

If you are connecting to MSN, type msn*username* in the **Username** box and leave the domain name blank.

Select this check box to save your password for the entry. The next time you make a connection with this phonebook entry, this authentication dialog box will not appear.

If select this check box and later want to change the password for the entry, you must edit the phonebook entry and in the **Security** tab, click **Unsave password**.

Dial-Up Networking clients must have an IP address. Select this option for an address to be assigned automatically by the dial-up server.

Select this option if you require a specific IP address as a Dial-Up Networking client and enter the required IP address.

Enter the required IP address. The dial-up server must be configured to permit clients that use a specific IP address.

Dial-Up Networking clients may require a server that maps the IP addresses used by computers to the friendly names used by people. For example, 198.105.232.1 is an IP address that users refer to as ftp.microsoft.com.

Domain Name Service (DNS) servers are used on TCP/IP networks worldwide. Windows Internet Name Service (WINS) servers have been introduced in Windows NT version 3.5 and later. Both can provide name resolution to Windows NT Dial-Up Networking clients.

Select this option to allow the dial-up server to assign DNS or WINS servers to Dial-Up Networking clients.

Select this option to specify the DNS and WINS servers (and alternate or backup servers).

Any address set to 0.0.0.0 or left blank does not change the configuration for that particular name server address, as if the server had rejected the option.

Enter an IP address to use a specific DNS server.

Enter an IP address for an alternate DNS server.

Enter an IP address to use a specific WINS server.

Enter an IP address for an alternate WINS server.

This check box sets Van Jacobson IP header compression during log on and negotiation with a PPP server.

When checked (the default) Dial-Up Networking will attempt to use VJ compression. This may or may not be successful depending on the capabilities of the remote PPP server, however, failure to negotiate VJ compression does not prevent the connection from working.

When cleared, Dial-Up Networking will not request or accept VJ compression. Some older versions of non-Microsoft PPP server software do not work with Windows NT Dial-Up Networking when VJ header compression is enabled. You should clear this box only when you successfully connect but you cannot transfer IP data in one or both directions.

If cleared, this check box overrides the registry values:

\\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Rasman\PPP\IPCP\AcceptVJCompression and RequestVJCompression.

This check box applies only to Dial-Up Networking clients that are simultaneously connected to a LAN and using a network card. When checked, packets that cannot be routed on the local network are forwarded to the default gateway on the remote network. In addition, address conflicts between the remote and local networks will be resolved in favor of the remote network.

Dial-Up Networking clients can connect to a SLIP server and must supply an IP address. You can pre-enter the IP address here that you would normally enter in the Terminal window. Only enter an address here if the IP address the server assigns you at connection time is the same every time you connect.

Specifies the DNS and WINS servers (and alternate or backup servers).

Any address set to 0.0.0.0 or left blank does not change the configuration for that particular name server address, as if the server had rejected the option.

Enter an IP address to use a specific DNS server.

Enter an IP address for an alternate DNS server.

Enter an IP address to use a specific WINS server.

Enter an IP address for an alternate WINS server.

Dial-Up Networking SLIP supports Van Jacobson (VJ) TCP/IP packet header compression. VJ is a protocol optimization widely supported in SLIP implementations. Some SLIP implementations do not support VJ.

When this check box is cleared (the default) Dial-Up Networking SLIP attempts to detect compressed packets and, if found, automatically shifts into VJ mode. This gives the best chance of a successful connection and, in most cases, the best performance available.

In some cases where both ends are attempting to detect compression, compression may not be activated. If you are certain that the remote server supports VJ compression, select this check box to activate compression and improve performance. You can verify that compression is occurring by monitoring the compression information in the Dial-Up Networking Monitor Status tab.

Note: If this check box is selected and the remote server does not support VJ compression, inbound traffic will continue normally but outbound traffic will not succeed. In this case, since most applications require communication in both directions the session will usually appear stopped.

This check box applies only to Dial-Up Networking clients that are simultaneously connected to a LAN and using a network card. When checked, packets that cannot be routed on the local network are forwarded to the default gateway on the remote network. In addition, address conflicts between the remote and local networks will be resolved in favor of the remote network.

Choose an outgoing frame size. The default setting is 1006; 1500 is also available if your remote access server accepts 1500-byte packets.

RAS Terminal is a character-based window that displays the logon sequence from the remote computer. Typically, you can use this window to interact with the remote computer for logging on. Alternatively, you can automate this manual logon using scripts. See Using RAS Terminal for Remote Logons for more information.

To change your before and after dialing options, use the **Script** tab in Dial-Up Networking.

Enter an IP address for the remote computer.

Click after you have completed all interactions with the remote computer.

Dial-Up Networking Multilink combines multiple physical links into a logical "bundle." This aggregate link increases your bandwidth. The most common use is bundling ISDN channels, but you can also bundle two or more modems or a modem and an ISDN line. To use Multilink, the dial-up server must have Multilink enabled.

Select the devices you want to link together during a call.

Click to add new or alternate phone numbers for the device.

Click to configure device-specific settings. For example, if you are using modems to make a connection, click to set the speed of your modem and enable modem compression.

Choose a device on your computer to view its connection status.

When a connection is active, this shows the current use of the device - for clients it shows the phonebook entry, for servers, it shows the user connected to the phonebook entry.

If the condition is inactive then there are no current connections based on the entry.

The speed in bits per second (bps) at which data is being transferred between modems.

The number of seconds since a physical connection was established.

Displays the status for incoming data.

Displays the status for outgoing data.

Displays the errors you might have during a connection.

The total number of bytes received over this connection. This number represents the bytes after they have been decompressed.

The number of logical network frames received from the server. The format of the frame depends on the network protocol in use. The maximum size of a frame is 1514 bytes. Well-written client/server applications transmit a small number of full or almost full frames. If you observe large numbers of small frames, the application you are running was probably not designed to run efficiently across slow links.

The ratio of compression achieved on received data, where higher is better. For example, if 400 incoming bytes decompress into 1,000 bytes, the compression ratio is 60 percent. This value refers to software compression only. The compression ratio depends on the amount of redundancy in the data received. For example, text and bitmaps compress well, but executable files and previously compressed data do not.

Connections using IP protocol VJ header compression (if active) is figured into this number. This entry may be non-zero even when Disable Software Compression (which applies only to data, not headers) is selected.

Note: Software compression is not attempted on some frames, for example, multicast datagrams or very small frames. Such frames are not included in the compression computation.

The total number of bytes sent over this connection. This number represents the bytes before they have been compressed.

The number of logical network frames sent to the server. The format of the frame depends on the network protocol in use. The maximum size of a frame is 1514 bytes. Well-written client/server applications transmit a small number of full or almost full frames. If you observe large numbers of small frames, the application you are running was probably not designed to run efficiently across slow links.

The ratio of compression achieved on transmitted data, where higher is better. For example, if 1,000 bytes are compressed into 400 bytes before transmission, the compression ratio is 60 percent. This value refers to software compression only. The compression ratio depends on the amount of redundancy in the data being transmitted. For example, text and bitmaps compress well, but executable files and previously compressed data do not.

Connections using IP protocol VJ header compression (if active) is figured into this number. This entry may be non-zero even when **Disable Software Compression** (which applies only to data, not headers) is selected.

Note: Software compression is not attempted on some frames, for example, multicast datagrams or very small frames. Such frames are not included in the compression computation.

Errors caused by the failure of a cyclic redundancy check (CRC). A CRC error indicates that one or more characters in the data packet arrived garbled from the server.

An expected character was not received in time. When this happens, the software assumes that the data has been lost and asks for it to be resent.

A condition in which a character received is not the one expected. An alignment error usually happens when a character is lost or when a timeout error occurs.

An error in which an asynchronous character is received with an invalid start or stop bit. If this error occurs and the computer is unable to establish a remote access connection, the computer-to-modem (DCE-to-DTE) bps rate may be incorrect. This problem suggests that the modem configured for remote access may not be correct for the modem you're using. Changing the bps rate or the hardware flow control setting may alleviate the problem. Contact your system administrator if this error occurs continually and if you are unable to connect through Dial-Up Networking.

The number of times the sending computer has transmitted characters faster than the receiving computer can process at the hardware level. If this problem persists, reduce the bps rate.

The number of times the sending computer has transmitted characters faster than the receiving computer can process at the software level. If this problem persists, reduce the bps rate or lower the CPU load on the computer.

Resets the statistics for this connection to zero

Displays details about the network connection for the device.

Click to hang up the connection.

The text sent from the local modem to the computer when the modems have finished negotiating. The text typically begins with the word CONNECT, often followed by the status of negotiated features and line speed. For example, the text might show that V.42 *bis* is in use. This section will be empty if you are using an ISDN line. Refer to your modem documentation for a specific interpretation of the response.

The number of bytes received by the device before the bytes have been decompressed.

The number of bytes sent by the device after the bytes have been compressed.

You can see which networks and devices on your computer are connected, and which users are connected to them.

Displays details about the network connection for the device.

Click to hang up a connection.

You can configure your computer to play sounds to communicate the following connection messages.

Select this check box to hear a sound when a connection is successful.

Select this check box to hear a sound when a connection is dropped.

Select this check box to hear a sound when data is transmitted.

Select this check box to hear a sound when an error occurs.

Select this check box to see a button for the Dial-Up Networking Monitor icon appear in the taskbar after Networking Monitor is started.

Dial-Up Networking Monitor can be configured to show status lights in two forms, as an icon or as a window on the desktop.

Select this check box to see status lights in the Dial-Up Networking Monitor icon next to the clock in the taskbar.

Select this check box to see status lights in the Dial-Up Networking Monitor window on the desktop.

Select this check box to see the title in the Dial-Up Networking Monitor window.

Select this check box to have the Dial-Up Networking Monitor window always appear on top of other windows.

Click to choose which devices on your computer should show status lights.

Click to immediately apply your changes in Dial-Up Networking Monitor.

Select this check box to control how much space the lights take up in the Dial-Up Networking Monitor window.

Select the devices on your computer for which you want to see status lights.

The selected device or connection.

The protocol the device is using for connection.

Lists the address assigned to the computer by the dial-up server. The Address will be displayed only for the protocols enabled for dial-out connections.

The IP address for the RAS server.

The IPX network number assigned to the computer by the dial-up server.

The IPX node identifies a particular computer.

Your computer name.

You can assign more that one phone number to each entry in Dial-Up Networking. This is useful if you have a pool of phone numbers to connect to.

To add additional phone numbers to an entry, type a new phone number and click **Add**.

Click to add an additional phone number to an entry.

Click to replace the phone number selected in the **Phone numbers** box with a new one.

The list of additional phone numbers for an entry.

Click to raise the order of the selected phone number in the **Phone numbers** box until the phone number is in the correct order**.** Dial-Up Networking dials the numbers in order until a connection is made.

Click to lower the order of the selected phone number in the **Phone numbers** box until the phone number is in the correct order**.** Dial-Up Networking dials the numbers in order until a connection is made.

Click to delete the selected phone number from the **Phone numbers** box.

Select this check box to move phone numbers that connected successfully to the top of the list. The next time you dial the phonebook entry, these numbers will be tried first.

Prefixes allow you to add extra numbers to the beginning of phone book entries.

To add a prefix to the list of available prefixes, type a prefix in the box and click **Add**.

Click to add a new prefix to the list of available prefixes.

Click to replace the prefix highlighted in the **Prefixes** box with a new prefix.

The list of available prefixes.

Select a prefix and then click to move the prefix up until it is in the correct order.

Select a prefix and then click to move the prefix down until it is in the correct order.

Select a prefix and then click to delete it.

Suffixes allow you to add extra numbers to the end of phone book entries.

To add a suffix to the list of available suffixes, type a suffix in the box and click **Add**.

Click to add a new suffix to the list of available prefixes.

Click to replace the suffix highlighted in the **Suffixes** box with a new prefix.

The list of available suffixes.

Select a suffix and then click to move the suffix up until it is in the correct order.

Select a suffix and then click to move the suffix down until it is in the correct order.

Select a suffix and then click to delete it.

Choose a location from which to dial.

Click to add a new location. You can then choose this new location in the **Dialing from** box in the **Dial-Up Networking** dialog box.

Prefixes allow you to temporarily add extra numbers to the beginning of all phone book entries without changing every entry.

Choose a prefix to use for the selected location.

Click to add a new prefix.

The prefix list is specific to each user on the computer.

Suffixes allow you to temporarily add extra numbers to the end of all phone book entries without changing every entry.

Choose a suffix to use for the selected location.

Click to add a new suffix.

The suffix list is specific to each user on the computer.

Type the name of a new location in the box.

Click to add the new location to the list of locations.

Click to replace a selected location in the **Locations** box with the new name.

The list of possible locations for your computer.

Select a location and click to delete it.

Screen text is good enough. Maybe one wording change though - "The Close on dial option hides the phonebook (can we say Dial-Up Networking instead?) while dialing and closes it as soon as you connect."

Select this check box if you do not want to use a script or terminal before dialing.

Select this check box to use a terminal box before dialing.

See Using RAS Terminal for Remote Logons

Select this check box to use a script before dialing.

Select which script to use before dialing. These scripts are part of Switch.inf, in which you can modify or create new scripts.

See Automating Remote Logons Using SWITCH.INF Scripts

Click to instantly access Switch.inf in order to modify or create new scripts.

Click to update the script list box after editing Switch.inf.

Select this check box to use other ports of the same device type if the device specified in **Dial using** box is not available. For example, if "Standard modem (COM1)" is selected in the **Dial using** box and this check box is selected, the modem on COM2 will be automatically used if the COM1 modem is busy.

Clearing this check box is useful for determining what is wrong with the first device when multiple devices are configured.

RAS is trying to reconnect a failed link. You can set this feature in Dial-Up Networking by clicking **More** and choosing **User preferences**. In the **Dialing** tab, clear the **Redial on link failure** check box.

RAS Autodial must be running for this feature to work. To start Autodial, in the **Services** icon in Control Panel, double-click **Remote Access Autodial Manager**. Select **Automatic** or **Manual** startup types and click **OK**. Then click **Start** in the **Services** dialog box.

Select this check box to enable the redial on link failure feature, which causes a link to be automatically reconnected when it fails. This feature works only when the Remote Access Autodial service is running.

To start the Autodial service, in the **Services** icon in Control Panel, double-click **Remote Access Autodial Manager**. Select **Automatic** or **Manual** startup types and click **OK**. Then click **Start** in the **Services** dialog box.

Special Dialing Options

Using Multiple Phone Numbers for One Entry

Using Prefixes and Suffixes

Pulse/Rotary Dialing

Touch-Tone Dialing

Phone Number Modifiers

Operator-Assisted Calls or Manual Dialing

Redial Settings

Phone Numbers for <entry>

You can assign more that one phone number to each entry in Dial-Up Networking. This is useful if you have a pool of phone numbers to connect to.

To add additional phone numbers to an entry

1 In Dial-Up Networking, in the **Basic** tab, click **Alternates**.

2 In the **New phone number** box type a new phone number.

3 Change the order of phone numbers in the **Phone numbers** box by selecting a phone number then clicking **Up**, **Down**, or **Delete**, until the phone number is in the correct order. Dial-Up Networking will dial the numbers in order until a connection is made.

4 Click **OK**.

Using Prefixes and Suffixes

You can configure Dial-Up Networking to use prefixes or suffixes. Prefixes and suffixes allow you to temporarily add extra numbers to all phone book entries without changing every entry. The prefix and suffix will apply to every phonebook entry dialed through your modem. The prefix and suffix will also apply to entries with multiple phone numbers.

For example, if you are staying at a hotel which requires you dial an 8 for an outside line, and you want use a credit card to bill calls to, you can use this dialog to specify the hotel's access code and long distance area codes as a prefix, and your credit card and PIN as a suffix to the phone number.

Special Codes

The prefixes 0, 9, and 8 are common access prefixes for business telephone systems. Call waiting can interfere with modem operation. On many US phone systems call waiting is blocked using the 70# prefix.

International phone systems and capabilities vary. Consult your local phone company or long distance carrier for other special codes.

To add a prefix or suffix to a Phone Book entry

1 In the Dial-Up Networking dialog box, click **Location**.

2 Select the desired prefix and/or suffix from the drop-down lists. To add prefixes or suffixes not diplayed in the drop-down list, click **Prefix list** or **Suffix list**.

3 Click **OK**.

See Also

Phone Number Prefixes

Phone Number Suffixes

Phone Number Prefixes

Prefixes allow you to add extra numbers to the beginning of phone book entries.

To add a prefix to the list of available prefixes

1 In the **Dial-Up Networking** dialog box, click **Location**.

2 In the **Location Settings** dialog box, click **Prefix list**.

3 In the **New prefix** box type the new prefix.

4 Click the **Add** button. The prefix will be added to the list. Use the **Replace** button to replace the prefix highlighted in the **Prefix** box with the new prefix.

5 Change the order of prefixes in the **Prefixes** box by selecting a prefix then clicking **Up, Down,** or **Delete**, until the prefix is in the correct order.

Click **OK**.

Phone Number Suffixes

Suffixes allow you to add extra numbers to the end of phone book entries.

To add a suffix to the list of available suffixes

1 In the **Dial-Up Networking** dialog box, click **Location**.

2 In the **Location Settings** dialog box, click **Suffix list**.

3 In the **New Suffix** box type the new suffix.

4 Click the **Add** button. The suffix will be added to the list. Use the **Replace** button to replace the suffix highlighted in the **Suffix** box with the new suffix.

5 Change the order of suffixes in the **Suffixes** box by selecting a suffix then clicking **Up, Down**, or **Delete**, until the suffix is in the correct order.

6 Click **OK**.

Pulse/Rotary Dialing

To use pulse/rotary dialing instead of touch-tone dialing, insert a "P" at the point in the phone number where you want pulse/rotary dialing to begin.

For example, if you use the following phone number:

555-5678P555-1234

Dial-Up Networking will dial 555-5678, switch to pulse/rotary mode, and then dial 555-1234 using pulse/rotary dialing.

See Also

Touch-Tone Dialing

Touch-Tone Dialing

To use touch tone dialing instead of pulse/rotary dialing, insert a "T" at the point in the phone number where you want touch tone dialing to begin.

For example, if you use the following phone number:

555-5678T555-1234

Dial-Up Networking will dial 555-5678, switch to touch tone mode, and then dial 555-1234 using touch tone dialing.

See Also

Pulse/Rotary Dialing

Phone Number Modifiers

Character	Function
, (comma)	Pauses briefly (two seconds for most modems) before continuing.
@	Waits for extended silence before continuing.
P	Switches from touch-tone to pulse/rotary dialing.
T	Switches from pulse/rotary to touch-tone dialing.
W	Waits for a dial tone before continuing (for modems with 2400 baud rate or greater).

For example, when dialing in from a hotel room, you may have to add 9 to the number you're calling to get an outside line. Your number would then look similar to the following:

9,555-2390

The comma after the 9 pauses long enough to get the outside line before continuing with the full number.

Operator-Assisted Calls or Manual Dialing

This feature lets you override automatic dialing in situations where intervention is required, for example, when calling through a manually operated switchboard.

To dial through an operator or to dial manually

1 In Dial-Up Networking, select a phonebook entry to dial and click **More**.

2 Select **Operator assisted or manual dialing** and click **Dial**.

The **Operator assisted or manual dial** dialog box appears only if the **Operator assisted or manual dialing** option is checked on the **More** menu.

3 Pick up the telephone handset, and dial the number or ask the operator to dial it for you.

The number assigned to the entry is displayed in the dialog box for easy reference.

4 Click **OK** immediately after you have finished dialing.

5 Hang up the handset only after the modem takes control of the line, typically signaled by a click followed by silence.

It is always safe to replace the handset once Dial-Up Networking begins verifying your user name and password. The status dialog will remind you of this.

Redial Settings

This feature lets you determine the number of times Dial-Up Networking automatically redials when you fail to connect to the selected entry. You can also set this feature to reconnect you automatically when the link is dropped because of inactivity.

To turn on automatic redialing

1 In Dial-Up Networking, click **More** and select **User Preferences**.

2 In the **Dialing** tab, in the **Number of redial attempts** box select the number of times the selected entry is automatically redialed if the first attempt to connect fails.

3 In the **Seconds before redial attempts** box select the number of seconds to pause between the end of one attempt and the beginning of another. This pause lets the device reset itself before redialing. The default is 15. If that is not enough time, increase this setting. You can also experiment with shorter times, but if you make the pause too short, the device will not have time to reset itself.

4 In the **Idle seconds before hanging up** box specify the amount of idle seconds before a connection hangs up. Keep in mind that the dial-up server also has a disconnect timer. If this control is set to a high timeout number, there is no guarantee that the connection will not disconnect before the time passes. This is because the server may choose to disconnect you before the time set here.

5 When you have finished, click **OK**.

Adding/Editing/Cloning an Entry

In Dial-Up Networking, click

- **New** if adding an entry to the phonebook.
- **More** and select **Edit entry and modem properties** if modifying a phonebook entry.
- **More** and select **Clone entry and modem properties** if creating a new phonebook entry from a copy of an existing one.

ISDN Phone Numbers

To connect through ISDN, you must specify a phone number for each channel you request when requesting more than two. For example, if you request three channels, you must specify three phone numbers (separated by colons, no spaces). Insert the phone numbers in the **Phone number** box in the **Basic** tab, as you would when adding, editing, or cloning any other entry: For example:

555-1234:555-1234:555-5678

If you request four channels, specify four phone numbers, for example:

555-1234:555-1234:555-5678:555-5678

Note: If there are more channels specified than phone numbers given, the extra channels will attempt to use the last number. For this reason you can use one number for a two-channel call since ISDN lines normally support two channels each. However, some ISDN phone companies require a unique number for each channel. Check with your ISDN provider.

See Also

Phone Number Modifiers

Reconfiguring Dial-Up Networking

If you change modems, add devices, or make another serial port available to Dial-Up Networking, you need to reconfigure the Remote Access Service.

1 Install the new device, and restart your computer.

2 From the Windows NT Control Panel, double-click **Network**.

3 In the **Services** tab, select **Remote Access Service**, and click **Properties**.

4 Click **Add** if configuring a new port for remote access.

5 In the **Remote Access Setup** dialog box, select the port you want to configure for the new device, and click **Configure**.

6 In the **Configure Port Usage** dialog box, select whether or not to dial out only, receive calls only, or both.

7 Click **OK** and in the **Remote Access Setup** dialog box, click **Continue**.

8 In the **Network** dialog box, click **Close**, and restart your computer.

Network Protocol Settings

Network protocols are the protocols you will use to communicate with servers on the LAN once you are connected to a RAS server. See your network administrator if you do not know which protocol to select.

PPP is the primary WAN protocol for Dial-Up Networking. You can run native TCP/IP, IPX and NetBEUI applications using the PPP protocol. SLIP is an older standard and is provided on Dial-Up Networking clients to permit them to connect to the installed base of SLIP servers.

To select a network protocol

1 In the Dial-Up Networking **Server** tab, select the type of dial-up server you are dialing. If you are not sure, choose **PPP**. If you are calling a SLIP server, choose **SLIP**. If you need to use the Microsoft RAS protocol used in previous versions of Microsoft RAS (Windows NT 3.1 Windows for Workgroups, and LAN Manager), choose **Windows NT 3.1, Windows for Workgroups 3.11**.

2 In the **Network protocols** box, select TCP/IP, IPX, or NetBEUI.

3 If you are using PPP or SLIP TCP/IP you can also specify that you want to use a specific IP address by clicking **TCP/IP Settings**.

4 Select the **Enable software compression** check box to enable software data compression.

5 Select the **Enable PPP LCP extensions** check box to enable newer PPP features. These extensions may cause problems when calling servers with older PPP software. Clear the **Request LCP extensions (RFC 1570)** check box only if consistent problems occur.

   Clearing this check box prevents LCP from sending Time-Remaining and Identification packets and requesting callback during the LCP negotiation of PPP.

Answers to Common Questions

1. Why doesn't my modem work with Dial-Up Networking. Answer
2. Why can't I connect to the server? Answer
3. When I try to connect, a message says the server is not responding. What should I do to correct this? Answer
4. Why does my modem always connect at lower bits-per-second (bps) rate than specified. Answer
5. The sessions to a server on the network keep getting dropped. How can this be corrected? Answer
6. What should I do when I encounter an abnormal disconnection? Answer
7. Why am I getting a hardware error when I try to connect. Answer

Check the list of compatible modems in the *Hardware Compatiblity List*.

If your modem appears on the list, make sure the modem is connected properly to the correct port on your computer.

If your modem isn't on the list, you must add a section for it in the MODEM.INF file.

To add a new section to MODEM.INF

1. Back up MODEM.INF.
2. Copy one of the sections already in the file and put the copy at the end.
3. Change the section name to the name of your modem.
4. Make modifications according to the modem's documentation.
5. If you have problems, call the modem's manufacturer.

The remote access server may not be running. Ask your system administrator to make sure it is running. If it is down, the administrator should check the error and audit logs to see why the service stopped, and then restart the service. If the service is running, the administrator should see whether some other remote workstations can connect properly. If other clients can connect, the problem may be specific to your workstation.

If the server is running, one or more of the following may be the cause:

- You may not have a valid user account or remote access permission.
- You may have dialed the wrong number, or dialed the correct number but forgotten to dial an external line-access number, such as 9.
- Your modem may not be able to negotiate with the server's modem. See if using the same type of modem on the client and server solves the problem.
- The modem cabling is faulty. In particular, do not use one of the 9-to-25-pin converters that come with most mouse hardware because some of them do not carry modem signals. To be safe, use a converter made especially for this purpose. See Cabling Requirements.
- The telephone line (in your hotel room, for example) may not accommodate your modem speed. Select a lower bps rate or call the hotel manager to request a direct line.
- Most modems work only with analog phone lines. Make sure you have analog phone lines installed or, if you have digital phone lines installed, make sure servers and clients have digital modems.

One or more of the following may be the cause:

- At higher bits-per-second (bps) rates, your modem is incompatible with the server's modem.
- There is a lot of static on the phone line, which prevents modems from connecting at a higher bps rate.
- There is some kind of switching equipment between the client and server that prevents the modems from negotiating at a higher bps rate.

Take one of the following actions:

- Make sure the modem and telephone line are operating correctly. Excessive static on the telephone line causes sessions to be dropped. You can use the Port Status dialog box to confirm whether this is happening. Try to redial.
- Ask your administrator to make sure the target server is running properly. If other workstations are having the same problem, there may be problems with server applications or hardware. If not, the problem is specific to your workstation.
- Have the administrator check the cabling between the Remote Access server and the target server.

Take the one of the following actions:

- Check whether the phone has call waiting. If so, disable call waiting. For information on how to disable call waiting, contact your local telephone-service provider.
- Try calling again. The remote access server might have disconnected you because of inactivity.
- See if someone picked up the phone. Picking up the phone automatically disconnects you.
- Check the modem cable to make sure it's connected properly.

Take the one of the following actions:

- The remote access server may not be running. Ask your system administrator to make sure the server is running.
- Your modem may be unable to negotiate correctly with the remote access server's modem. Try a lower speed. See Setting Modem Features
- Your computer's serial port may not be able to keep up with the speed you have chosen. Try connecting at a lower initial port speed. See Setting Modem Features

Take the one of the following actions:

- Make sure your modem is turned on. If the modem was turned off, turn it on and redial.
- If your modem was turned on, make sure it's functioning properly by testing it through Windows NT Terminal. See Testing Your Modem.
- If your modem communicates through Terminal, but not through Dial-Up Networking, the cable attaching your modem to the computer is probably incompatible. Install a compatible cable. See Cabling Requirements.

Serial Ports

Note that Com1 and Com3 share interrupt (IRQ) level 4. Com2 and Com4 share interrupt (IRQ) level 3. As a result, you will not be able to use COM1 and COM3 simultaneously, or COM2 and COM4 simultaneously for serial communications, for example, Dial-Up Networking on COM1 and Terminal on COM3.

This rule applies if you are using the mouse in addition to other serial communications programs such as Dial-Up Networking or the Windows NT Terminal program.

However, the rule does not apply if you are using intelligent serial adapter cards such as the DigiBoard serial cards.

ISDN Troubleshooting

When you dial through ISDN and fail to connect, the error message "No answer" appears. This message can mean one of several things may be wrong, such as:

- The remote access server did not answer because it was turned off, the modem wasn't connected, or so on. Contact your system administrator.
- The line is busy.
- There's a problem with your hardware. Make sure your ISDN cards have been installed and configured correctly.
- A poor line condition, such as too much static, interrupted your connection. Wait a few minutes and try dialing again.
- You did not enable line-type negotiation in the ISDN Settings dialog box, and a connection could not be made with the line type you chose in the ISDN Settings dialog box.
- Your ISDN switching facility may be busy. Try again later.

Check for any of these potential problems. When you have fixed the problem, redial the number.

X.25 Troubleshooting

1 After connecting through a dial-up PAD, the server consistently fails to authenticate the client. Solution

2 A connection has been established, but network drives are disconnecting, and you are dropping sessions or getting network errors. Solution

3 While transferring files, you frequently get the error messages "Network drive disconnected" or "Network drive no longer exists." Solution

4 Newly created entries in MODEM.INF and PAD.INF do not work. Solution

5 A modem connected to a dial-up PAD connects a lower speed than it should. Solution

If the remote access server is running and clients cannot connect to it directly through an X.25 smart card or an external PAD, the dial-up PAD may have the wrong X.3 parameters or serial settings. Ask your administrator for the correct settings, listed in the Chapter 9 "X.25 PAD Support" in the *Networking Supplement*.

Congestion on the remote access server's leased line may be the cause. The administrator should make sure that the speed of the leased line can support all the COM ports at all speeds clients use to dial in.

For example, four clients connecting at 9600 bps (through dial-up PADs) require a 38,400-bps (four times 9600) leased line on the server end. If the leased line does not have adequate bandwidth, it can cause timeouts and degrade performance for connected clients. This example assumes the Remote Access Service is using all the bandwidth. If it is sharing the bandwidth, fewer connections can be made.

On X.25 smart cards, change the Negotiate network parameters option in the X.25 settings to Yes. This problem arises when X.25 parameters, such as the size of the send and receive window, are set differently for the server, the network, and the client X.25 software.

By enabling the Negotiate network parameters option on the client's (if using the direct X.25 connection) and the server's X.25 software, you let the server, the network, and the client use commonly negotiated X.25 network parameters.

In MODEM.INF, check other entries for direct connections and external PADs, and see the comments that go with them. You may need a line analyzer or a terminal program to see the response for the PAD. For dial-up PAD entries, use an entry in PAD.INF as an example, paying attention to the comments that go with it.

Replace the modem with a compatible one from the list in the Setup program.

Getting Started

Dial-Up Networking is the client version of RAS and is used to connect to dial-up servers. The Dial-Up Networking icon is located in the **My Computer** dialog box and in the Accessories folder on the **Start** menu.

1 In Dial-Up Networking, click **New** to create a new entry in the phonebook, or click **More** and select **Edit entry and modem properties**.

2 Click **Dial** to make a remote connection.

Connecting to the Network

To connect to the network

1 In Dial-Up Networking, dial the entry you want to connect to.

2 If prompted, type your authentication user name, password, and domain in the **Authentication** dialog box.

Note: The domain name you enter in the **Authentication** dialog box should be the Windows NT domain that the Windows NT RAS server is in. This is not the DNS domain name given by some PPP/SLIP providers. For example, you would enter accounting, not www.halcyon.com.

Once connected to the network, you can minimize Dial-Up Networking and use your computer as if it were connected to the LAN directly. In other words, use your e-mail, the Explorer, and so on as though you were in the office.

Note: Authentication credentials are typically the same as your network logon credentials. Dial-Up Networking uses these credentials to verify that you have the right to physically access the network. Dial-Up Networking does not actually log you on, so after your connection is established you may need to log on (by pressing CTRL+ALT+DEL for Windows NT) to access protected network resources. But you can avoid this step by logging on to your domain account when starting your Windows NT-based computer (before you establish the remote access connection). This is the same as logging on with your network cable unhooked and then plugging it in.

Using the Network

When you have connected to a remote access server, you can access data files across the telephone line; you cannot run programs remotely. Running a program across a telephone wire is unacceptably slow for most applications. For the best performance, install licensed copies of the applications you need on your local computer.

See Also

Monitoring Connections and Status Reporting

Special Dialing Options

Allowing Dial-In Access to Your Computer

To let others access your computer

1 Through the Remote Access Administrator's utility, grant access permission to users who you want to let access your computer. For more information see Setting Remote Access Permissions

2 From the Remote Access Administrator's utility, start the Remote Access Service.

To accept incoming calls immediately after starting your computer

1. From the Windows NT Control Panel, click the Services icon.
2. Select **Remote Access Server**.
3. Click **Startup**.
4. In the **Startup Type** box, select the **Automatic** option.
5. Click **OK**.

Dial-Up Networking Overview

Dial-Up Networking is the client version of Windows NT Remote Access Service (RAS).

Dial-Up Networking allows remote users on the following systems to work as if they were connected directly to the network: Windows NT, Windows for Workgroups, MS-DOS version 3.1 or later (RAS version 1.1a), and MS OS/2 version 3.1 (RAS version 1.1). Microsoft does not support access to Macintosh volumes and AppleTalk printers over dial-in lines.

A Windows NT RAS configuration includes the following components:

Dial-Up Networking clients Windows NT, Windows for Workgroups, MS-DOS (with Microsoft network client software installed), and LAN Manager RAS clients can all connect to a Windows NT RAS server. Clients can also be any non- Microsoft PPP client.

RAS servers The Windows NT Server RAS permits up to 256 remote clients to dial in. Windows NT Workstation permits one remote client to dial in. The RAS server can be configured to provide access to an entire network or restrict access to the RAS server only.

LAN protocols LAN protocols transport packets across a local-area network (LAN), whereas remote access protocols control the transmission of data over the wide-area network (WAN).Windows NT supports LAN protocols such as TCP/IP and RAS, IPX and RAS, and NetBEUI and RAS, which enable access to the Internet and to NetWare and UNIX servers. Windows Sockets applications over TCP/IP or IPX, named pipes, Remote Procedure Call (RPC), and the LAN Manager API are supported.

Remote access protocols Windows NT supports Remote Access Protocols such as PPP, SLIP on RAS clients, and the Microsoft RAS Protocol.

WAN options Clients can dial in using standard telephone lines and a modem or modem pool. Faster links are possible using ISDN. You can also connect RAS clients to RAS servers using X.25, an RS-232C null modem, or using the Point-to-Point Tunneling Protocol (PPTP).

Security features Windows NT logon and domain security, support for security hosts, data encryption, and callback provide secure network access for remote clients.

Internet support RAS enables Windows NT to provide complete services to the Internet. A Windows NT Server computer can be configured as an Internet service provider, offering dial-up Internet connections to a PPP client. A computer running Windows NT Workstation can dial into an Internet-connected computer running Windows NT Server 3.5 or later or to any one of a variety of industry-standard PPP or SLIP-based Internet servers. For more information, see the *Windows NT Resource Kit Internet Guide*.

Dial-Up Networking Clients

Clients connecting to Windows NT RAS servers can use Windows NT, Windows 95, Microsoft Windows for Workgroups, MS-DOS (with Microsoft network client software installed), LAN Manager, or any PPP client. The client must have a modem (9600 baud or above is recommended for acceptable performance), an analog telephone line or other WAN connection, and remote access software installed.

Connecting is automatic with the RAS AutoDial feature. AutoDial learns every connection made over the RAS link and automatically reconnects you when you access a resource for the second time.

Connecting can also be automated for any Microsoft client with a simple batch file and the **rasdial** command or with a custom, RAS-aware application using the appropriate Application Programming Interface (API) for RAS. You can also schedule automatic backups to or from remote computers by using RAS and the **at** command.

Windows NT Version 3.5, 3.51 and Windows 95 Clients

Windows NT version 3.5x and Windows 95 clients can take full advantage of Windows NT version 4.0 RAS features, except for Multilink functionality. Windows NT version 3.5x and Windows 95 clients can also connect to any non-Microsoft remote access PPP server or SLIP server.

Windows NT version 3.5x and Windows 95 clients negotiate logon and authentication with the server, whether the server is a Microsoft RAS server, a PPP server, or a SLIP server. You can also configure RAS phonebook entries to use scripts that can completely automate logon.

Windows NT Version 3.1 Clients

Windows NT version 3.1 clients use the Microsoft RAS protocol and are fully compatible with all versions of Microsoft RAS.

These clients do not support the PPP protocol introduced in Windows NT version 3.5. Only Windows NT version 3.5x or other PPP clients provide the support necessary to run TCP/IP or IPX applications on clients that directly communicate with servers on the LAN using TCP/IP or IPX.

Windows For Workgroups, MS-DOS, and LAN Manager Clients

Windows NT Server provides a Microsoft Network Client version 3.0 for MS-DOS and a Windows for Workgroups client that provide remote access. Separately purchased Windows for Workgroups and LAN Manager RAS clients can also connect to Windows NT version 3.5 RAS servers. These clients are fully compatible with all versions of Microsoft RAS.

The Microsoft Network Client version 3.0 for MS-DOS must be set up to use the full redirector (the default setting.) If the basic redirector is used, the Remote Access program **rasphone** will not start.

The Windows for Workgroups, MS-DOS, and LAN Manager clients can use the RAS NetBIOS gateway to access NetBIOS servers running TCP/IP, IPX, or NetBEUI, but these clients cannot run applications that must use TCP/IP or IPX on the client.

These clients also do not support the PPP protocol introduced in Windows NT version 3.5.

PPP Clients

Non-Microsoft PPP clients using TCP/IP, IPX, or NetBEUI can access a Windows NT version 3.5 or later RAS server. The RAS server will automatically negotiate authentication with PPP clients; the Windows NT RAS software needs no special configuration for non-Microsoft PPP clients.

For more information about your PPP client, see the software documentation for your PPP client.

Remote Access Protocols

Remote access protocols control transmission of data over the wide-area network (WAN). The operating system and LAN protocol(s) used on remote access clients and servers dictate which remote access protocol your clients will use. The remote access protocols are of four types: Point-to-Point Protocol (PPP), Serial Line Internet Protocol (SLIP), Microsoft RAS Protocol, and NetBIOS Gateway.

Point-to-Point Protocol (PPP)

Windows NT supports the Point-to-Point Protocol (PPP) in RAS. PPP is a set of industry standard framing and authentication protocols that enable remote access solutions to interoperate in a multi-vendor network. Microsoft recommends that you use PPP because of its flexibility and its role as an industry standard as well as for future flexibility with client and server hardware and software.

PPP support enables computers running Windows NT to dial into remote networks through any server that complies with the PPP standard. PPP compliance also enables a Windows NT Server computer to receive calls from, and provide network access to, other vendors' remote access software.

The PPP architecture also enables clients to load any combination of IPX, TCP/IP, and NetBEUI. Applications written to the Windows Sockets, NetBIOS, or IPX interface can be run on a remote Windows NT Workstation computer.

PPP has become the standard for remote access.

Remote Access protocol standards are defined in *Requests for Comments* (RFCs), which are published by the Internet Engineering Task Force and other working groups. The RFCs supported in this version of Windows NT RAS are

- RFC 1549 PPP in HDLC Framing
- RFC 1552 The PPP Internetwork Packet Exchange Control Protocol (IPXCP)
- RFC 1334 PPP Authentication Protocols
- RFC 1332 The PPP Internet Protocol Control Protocol (IPCP)
- RFC 1661 Link Control Protocol (LCP)
- RFC 1717 PPP Multilink Protocol

If your remote clients connect to third-party PPP servers, they might need to enable a post-connect terminal script to log on to the PPP server. After the server informs them it is switching to PPP framing mode, the user must start Terminal to complete logon.

Serial Line Internet Protocol (SLIP)

Serial Line Internet Protocol (SLIP) is an older remote access standard typically used by UNIX remote access servers. Windows NT Dial-Up Networking clients support SLIP and can connect to any remote access server using the SLIP standard. This permits Windows NT version 3.5 clients to connect to the large installed base of UNIX servers. The Windows NT Remote Access server does not support SLIP clients.

The RFCs supported in this version of Windows NT RAS are

- RFC 1144 Compressing TCP/IP Headers for Low-Speed Serial Links
- RFC 1055 A Nonstandard for Transmission of IP Datagrams Over Serial Lines: SLIP

Microsoft RAS Protocol

The Microsoft RAS protocol is a proprietary remote access protocol supporting the NetBIOS standard. The Microsoft RAS protocol is supported in all previous versions of Microsoft RAS and is used on Windows NT version 3.1, Windows for Workgroups, MS-DOS, and LAN Manager clients.

A RAS client dialing into an older version of Windows (Windows NT version 3.1 or Windows for Workgroups) must use the NetBEUI protocol. The RAS server then acts as a gateway for the remote client, providing access to servers that use the NetBEUI, TCP/IP, or IPX protocols.

NetBIOS Gateway

Windows NT continues to support NetBIOS gateways, the architecture used in previous version of Windows NT and LAN Manager. Remote users connect using NetBEUI, and the RAS server translates packets, if necessary, to IPX or TCP/IP. This enables users to share network resources in a multi-protocol LAN but prevents them from running applications which rely on IPX or TCP/IP on the client. The NetBIOS gateway is used by default when remote clients are using NetBEUI.

An example of the NetBIOS gateway capability is remote network access for Lotus Notes users. Although Lotus Notes does offer dial-up connectivity, dial up is limited to the Notes application. RAS complements this connectivity by providing a low-cost, high-performance remote network connection for Notes users which not only connects Notes, but offers file and print services, and

access to other network resources.

WAN Options

Clients can connect to servers through phone lines and modems, ISDN, X.25, RS-232C null modem, or Point-to-Point Tunneling Protocol (PPTP).

Phone Lines and Modems

The most common WAN connection is a standard analog telephone line and a modem. Standard analog phone lines are available worldwide and will meet most RAS needs for roving users. Note that standard analog phone lines are also called PSTN (Public Switched Telephone Network) or POTS (Plain-old Telephone Service).

More than 200 modems are compatible with Windows NT. Most modems that comply with industry standards should interoperate. However, many difficult-to-detect problems can come from incompatible modems. To prevent such problems, use the same modem on clients and servers.

Modems are automatically detected. Automatic modem detection is especially useful for users who are not sure what modem is installed (for example, an internal modem).

Third-party modem pools can be used on either the client side or the server side. Modem pools are made available to RAS using the Network option in Control Panel. Consult your modem pool documentation for more information.

Modem data compression and error control are available. However, built-in software compression offers enhanced performance over modem data compression.

ISDN

To enhance WAN speeds at a stationary remote site or at sites that will use RAS, use an Integrated Services Digital Network (ISDN) line. Whereas standard phone lines typically transmit at 9600 bits per second (bps), ISDN lines can transmit at speeds of 64 or 128 kilobits per second (KBps).

An ISDN line must be installed by the phone company at both the server and at the remote site. ISDN also requires that an ISDN card be installed in place of a modem in both the server and remote client. Costs for ISDN equipment and lines can be higher than standard modems and phone lines. However, the speed of communication reduces the duration of connections, possibly saving toll charges.

An ISDN line comes with two B channels that transmit data at 64 KBps, and one D channel for signaling that transmits data at 16 KBps. You can configure each B channel to operate as a port. Some ISDN drivers allow you to aggregate the channels. This means you can statically assign a higher bandwidth by configuring both B channels to act as a single port. With this configuration, line speed increases to 128 KBps. Channel aggregation schemes are specific to each driver, so you must use the same driver and equipment on the client and server.

X.25

X.25 is a standard packet-switching communication protocol (or transport) designed for WAN connectivity.

Windows NT RAS supports connections based on the X.25 standard using Packet Assemblers/Disassemblers (PADs) and X.25 smart cards. You can also use a modem and special dial-up X.25 carriers (such as Sprintnet and Infonet) in place of a PAD or smart card on RAS clients.

RS-232C Null Modem

Suppose two or more networks are in the same location but are not physically connected. To use resources on both networks from one computer, use an RS-232C null modem. The client connects an RS-232C cable from a COM port to a COM port on the RAS server. RAS is used to create network access.

An RS-232C null modem can also be used as a substitute for a network card in a computer located physically near (less than 50 feet of cable) a RAS server.

Point-to-Point Tunneling Protocol (PPTP)

A RAS server is usually connected to a PSTN, ISDN, or X.25 network, allowing remote users to access a server through these networks. RAS now allows remote users access through the Internet by using the Point-to-Point Tunneling Protocol (PPTP).

PPTP is a new networking technology that supports multiprotocol virtual private networks (VPNs), enabling remote users to access corporate networks securely across the Internet by dialing into an Internet Service Provider (ISP) or by connecting directly to the Internet. PPTP offers the following advantages:

- Lower Transmission Costs

- Lower Hardware Costs
- Lower Administrative Overhead
- Enhanced Security

Security Features

Windows NT is a secure operating environment, designed to meet the requirements of C-2 level (U.S. Department of Defense) security:

- Access to system resources can be discretely controlled.
- All system access can be recorded and audited.
- Access to the system requires a password and leaves an audit trail.

Windows NT Server uses a *trusted domain, single-network logon* model:. Users and groups of one domain can be granted access to resources in a trusting domain. After being authenticated, users carry access credentials that are presented whenever access to a resource is requested on the network. A Windows NT Server computer can be locked-down using software, provided the computer is secured physically.

This single-network logon model extends to RAS users. RAS access is granted from the pool of all Windows NT user accounts. An administrator grants the right to dial into the network, and users then use their domain logon to connect via RAS. After being authenticated by RAS, users can use resources throughout the domain and in any trusted domains.

Finally, Windows NT provides the Event Viewer for auditing. All system, application, and security events are recorded to a central secure database which, with proper privileges, can be viewed from anywhere on the network. Attempts to violate system security, to start or stop services without authorization, or to gain access to protected resources are recorded in the Event Log and can be viewed by the administrator.

RAS Servers

Windows NT Server administrators use the Remote Access Admin program to control the RAS server, view users, grant permissions, and monitor remote access traffic. For more information about using the Remote Access Admin program, see Rasadmin.hlp.

The server must have a multiport adapter or modems (9600 baud or above is recommended for acceptable performance), analog telephone lines or other WAN connections, and the RAS software installed. If the server will provide access to the network, a separate network adapter card must be installed and connected for each network the server will provide access to.

RAS servers are configured during initial RAS setup. You must specify whether access will be to the entire network or to the RAS server only. You must also select the protocols to use on the LAN (IPX, TCP/IP, and NetBEUI) and an authentication encryption option. For more information about remote access protocols and LAN protocols, see those sections elsewhere in this chapter.

Ports on RAS servers are configured individually. Each port can be set to **Dial Out Only**, **Receive Calls Only**, or **Dial Out And Receive Calls**. These settings affect only the port specified, not all ports. For example, your RAS server can be configured to provide access to the entire network, COM1 can be configured to receive calls, and COM2 can be configured for dial out and receive. A remote user can call in on either COM port, but a local user can use only COM2 for outbound RAS calls.

Events and errors are recorded in Event Viewer on Windows NT RAS clients and servers. Evaluating the log in Event Viewer can help you determine the source of problems.

In Control Panel, use the Network option to install and configure RAS, and the Panel Services option to specify startup options.

The Windows NT Server RAS permits up to 256 remote clients to dial in. The RAS server can be configured to provide access to an entire network or restrict access to resources on the RAS server only.

For more information about installing and configuring RAS, see Installing Dial-Up Networking.

LAN Protocols

Windows NT supports LAN protocols such as TCP/IP, IPX, and NetBEUI, and Remote Access Protocols such as PPP, SLIP, and the Microsoft RAS Protocol. LAN protocols transport packets across a local-area network (LAN), whereas remote access protocols control the transmission of data over the wide-area network (WAN). See Remote Access Protocols for more information.

The protocol(s) used in the existing network affect how you plan, integrate, and configure RAS.

Windows NT RAS supports TCP/IP, IPX, and NetBEUI. This support means you can integrate Windows NT RAS into existing Microsoft, UNIX, or NetWare networks using the PPP remote access standard. Windows NT RAS clients can also connect to existing SLIP-based remote access servers (primarily UNIX servers).

When you install and configure RAS, any protocols already installed on the computer (TCP/IP, IPX, and NetBEUI) are automatically enabled for RAS on inbound and outbound calls.

You must also specify if you want to provide access to the entire LAN; otherwise, users will be able to access only the RAS server. If you provide access to the entire LAN using TCP/IP or IPX, you must also configure how the server will provide IP addresses or IPX net numbers. If you provide access to the entire LAN using NetBEUI, no additional configuration is needed.

See Also

IPX and RAS

TCP/IP and RAS

NetBEUI and RAS

IPX and RAS

IPX is the native NetWare protocol used on many Novell networks. Because it is a routable protocol, IPX is suitable for enterprise-wide networks. This section explains how to integrate Windows NT RAS clients and servers into a NetWare IPX network. For more information, see the *Networking Supplement*.

Windows NT Support for NetWare

If Windows NT RAS computers must see a Novell NetWare network, the client computer must run a NetWare redirector. In Windows NT Workstation computers, this redirector is called the *Client Service for NetWare* ; in Windows NT Server computers this is called the *Gateway Service for NetWare*.

A Windows NT RAS server is also an IPX router and Service Advertising Protocol (SAP) agent for RAS clients only. RAS servers and their clients use the PPP IPX Configuration Protocol (IPXCP) defined in RFC 1552 to configure the remote access line for IPX. Once configured, RAS servers enable file and print services and the use of Windows Sockets applications over IPX on the NetWare network for RAS clients.

RAS servers provide clients connecting to an IPX network with an IPX net number and act as their SAP agent. The following section explains the addressing options available for Windows NT RAS using the IPX protocol.

IPX Addressing for Remote Clients

RAS clients are always provided an IPX address by the RAS server. The IPX network number is either generated automatically by the RAS server, or a static pool of network numbers is given to the RAS server for assignment to RAS clients.

For automatically generated IPX network numbers, the Windows NT RAS server uses the NetWare Router Information Protocol (RIP) to determine an IPX network number that is not in use in the IPX network. The RAS server assigns that number to the remote client.

You can override the automatic assignments of network numbers. Manual assignments can be useful if you want more control of network number assignments for security or monitoring. When assigning IPX network numbers to a RAS server, ensure that duplicate network numbers are not assigned and that other NetWare services cannot assign the RAS IPX addresses. You can also assign the same network number to all clients to minimize RIP announcements from the RAS server.

TCP/IP and RAS

TCP/IP is one of the most popular protocols. Its routing capabilities provide maximum flexibility in an enterprise-wide network.

On a TCP/IP network, you must provide IP addresses to clients. Clients might also require a naming service or method for name resolution. This section explains IP addressing and name resolution for Windows NT RAS servers and clients on TCP/IP networks.

For information about implementing the Microsoft TCP/IP protocol in a network, see Chapter 1, ‘‘Microsoft TCP/IP and Related Services for Windows NT" in the *Networking Supplement*..

Assigning IP Addresses to RAS Clients

In Windows NT, each remote computer connecting to a RAS server through PPP on a Microsoft TCP/IP network is automatically provided an IP address from a static range assigned to the RAS server by the administrator during setup.

Windows NT RAS clients can also use a preassigned IP address specified in their phonebook. In this case, the Windows NT RAS server must be configured to permit users to request a specific address.

Name Resolution for RAS Servers and Clients

In addition to requiring an IP address, RAS servers and clients on a TCP/IP network might require a mechanism to map computer names to IP addresses. Four name resolution options are available on a Windows NT network: Windows Internet Name Service (WINS), broadcast name resolution, Domain Name System (DNS), and the HOSTS and LMHOSTS files.

RAS servers can use all these name resolution methods for operations performed on the server.

RAS clients are assigned the same WINS and DNS servers that are assigned to the RAS server. You must use the Registry to override this automatic assignment.

RAS clients in small networks where IP addresses do not change can use a HOSTS or LMHOSTS file for name resolution. By using these files on the local drive, you do not need to transmit name resolution requests to a WINS server and wait for the response over the modem.

For information about name resolution on a Microsoft TCP/IP network, see Chapter 3, ‘‘Implementation Considerations" in the *Networking Supplement*..

Connecting to Third-party Remote Access Servers Using IP

The Windows NT RAS server enables remote clients to share subnet addresses with computers on the LAN, thereby conserving IP addresses.

Note that remote access servers from other vendors might require that remote clients have a different subnet address than clients on the LAN. If remote clients dial into another vendor’s remote access server and cannot connect to resources on the LAN, check the following configuration on your remote access server:

If your third-party remote access server does not support proxy-ARP (Address Resolution Protocol), your remote clients must be assigned a different subnet address than LAN clients. Be sure your server is configured to assign remote clients with a subnet address that is unique on your LAN.

Ensure that your network routers are configured so that remote access clients can use the **ping** command on target hosts (and vice versa) in the following order:

1 Remote client to target server, then remote client to remote access server, then remote access server to target server.

2 Target server to remote client, then target server to remote access server, then remote access server to remote client.

SLIP on TCP/IP Networks

Support for Serial Line Internet Protocol (SLIP) allows Windows NT RAS clients to connect to third-party remote access servers that use the SLIP remote communication standard. Clients can use SLIP only if the port for the Phonebook entry is a serial COM port.

When a user connects to a SLIP server, a **Windows Terminal** dialog box pops up for an interactive logon session with the UNIX SLIP server. The UNIX logon overrides and prevents the RAS logon from appearing. After a connection is established, remote network access becomes transparent to the user.

NetBEUI and RAS

NetBEUI is suited for use in small workgroups or LANs. A NetBIOS gateway and the NetBEUI client protocol are installed by default on all Windows NT RAS servers and most Windows networking clients. Previous Windows NT RAS clients, LAN Manager RAS clients, MS-DOS RAS clients, and Windows for Workgroups RAS clients require NetBEUI.

Installing Dial-Up Networking (RAS)

RAS installation varies slightly, depending on which network protocols are installed. If you will use the TCP/IP or IPX protocol with RAS, install the protocol before you install RAS. Note that selecting an uninstalled protocol will cause that protocol to be installed at the conclusion of RAS Setup. For information about installing either protocol, see *Windows NT Server Start Here*.

To install and configure RAS, you must be logged on as a member of the Administrators group.

To add the remote access software

1. In Control Panel, double-click the Network option.
2. On the **Services** tab, click **Add**.
3. In the **Network Service** box, click **Remote Access Service** and then click **OK**.
4. When prompted for the path to the distribution files, type the path and then click **OK**.

   The RAS files are copied to your computer.
5. When prompted, you can either have RAS Setup automatically detect the modem connected to the selected port or select your modem from a list of supported modems.
6. In the **Add RAS Device** dialog box, select the port you will use for remote access and click **OK**. If you have successfully installed a multiport adapter, ISDN card, X.25 card, or other device, it will appear in the list.
7. In the **Remote Access Setup** dialog box, click **Configure**.
8. In the **Configure Port Usage** box, select one of the following and then click **OK**:
   - **Dial out only** if the computer will be a RAS client only.
   - **Receive calls only** if the computer will be a RAS server only.
   - **Dial out and Receive calls** if the computer can be a client or server. The computer cannot be both at the same time.
9. To configure RAS network-wide settings, click **Network**. For more information, see Configuring RAS to Use LAN Protocols.

Note: You must restart your computer for the remote access installation and configuration take effect.

The remote access software includes the following applications:

- Dial-Up Networking is the client version of RAS and is used to connect to dial-up servers. The Dial-Up Networking icon is located in the **My Computer** dialog box and in the Accessories folder on the **Start** menu.
- Dial-Up Networking Monitor, which is used to monitor connections and devices, is located in Control Panel.
- Remote Access Admin, which is used to monitor remote users connecting to a RAS server, is located in the Administrative Tools folder on the **Start** menu.

Hardware Requirements for RAS

Before you install RAS, all hardware should be installed and working. Depending on your network and requirements, you might need the following hardware:

- Network adapter card with a certified Network Driver Interface Specification (NDIS) driver
- One or more compatible modems (see the *Hardware Compatibility List* or the Remote Access Setup program) and an available COM port
- Multiport adapter card for acceptable performance with multiple remote connections
- X.25 smart card (if using an X.25 network)
- ISDN card or modem (if using an ISDN line)

See the *Hardware Compatibility List* to verify the compatibility of all hardware in a Windows NT computer.

Configuring RAS to Use LAN Protocols

Because RAS provides access to a LAN, you must select and configure the protocols to use on the LAN. A Windows NT Workstation or Server computer can be either a RAS server or a client. You must configure the LAN protocols RAS will use in each role. A RAS computer's role is determined when you specify how RAS-enabled ports will be used.

Setting network LAN protocols affect all RAS operations for all RAS-enabled ports. For example, you must enable TCP/IP for the LAN before you can choose to use TCP/IP for a specific RAS entry.

To configure RAS to use LAN protocols

1. In Control Panel, double-click the Network option.
2. On the **Services** tab, click **Remote Access Service** and then click **Properties**.
3. In the **Remote Access Setup** dialog box, click **Network**.
4. In the **Dial out Protocols** box of the **Network Configuration** dialog box, select the protocols to use for dialing out as a RAS client to another computer. If you do not select a protocol in this box, you will be unable to select that protocol later when you configure a phone book entry for dialing out.

   If no ports are configured for dial out, this box is dimmed.
5. In the **Server Settings** box, select the LAN protocols the RAS computer can use for receiving calls from remote clients.

   If no ports are configured to receive calls, this box is unavailable.
6. Select an encryption option, as follows:

- **Allow any authentication including clear text** permits connection using any authentication requested by the client (MS-CHAP, SPAP, PAP). This option is useful if you have different RAS clients.
- **Require encrypted authentication** permits connection using any authentication requested by the client except PAP.
- **Require Microsoft encrypted authentication** permits connection using MS-CHAP authentication only.
- **Require data encryption** means all data sent over the wire is encrypted.

7. To combine multiple physical links into a logical "bundle," select the **Enable Multilink** check box. This aggregate link increases your bandwidth. The most common use is bundling ISDN channels, but you can also bundle two or more modems or a modem and an ISDN line.

   This check box only applies to Windows NT Server computers.
8. When you are finished selecting protocols, click **OK**.
9. In the **Remote Access Setup** dialog box, click **Continue** to exit Remote Access Setup.

Note: You must restart your computer for the changes to take effect.

See Also

Configuring a RAS Server to Use TCP/IP

Configuring a RAS Server to Use IPX

Configuring a RAS Server to Use NetBEUI

Configuring Name Resolution for RAS Clients

Choosing a Protocol for a RAS Entry

Configuring a RAS Server to Use NetBEUI

NetBEUI gives the best performance for NetBIOS applications in small LANs. Removing NetBEUI still allows you to use RAS with TCP/IP or IPX. You can configure whether NetBEUI clients can access the entire network or the RAS computer only.

To configure a RAS server to use NetBEUI for network connections

1 In Control Panel, double-click the Network option.

2 On the **Services** tab, click **Remote Access Service** and then click **Properties**.

3 In the **Remote Access Setup** dialog box, click **Network**.

4 In the **Server Settings** box, select the **NetBEUI** check box and click **Configure**.

5 In the **RAS Server NetBEUI Configuration** dialog box, select whether to allow NetBEUI clients to access the entire network or the RAS computer only, and then click **OK**.

6 In the **Network Configuration** dialog box, click **OK**.

7 In the **Remote Access Setup** dialog box, complete any other port configurations and then click **Continue**.

Note: You must restart your computer for the changes to take effect

Configuring a RAS Server to Use TCP/IP

You can use the Network option in Control Panel to configure or reconfigure the TCP/IP settings for RAS connections.

The RAS server has two TCP/IP configurations:

- Its own basic configuration and IP address as a server on the LAN. For information on this configuration, see the TCP/IP Help file.
- Its RAS configuration to supply IP addresses to RAS clients. This topic explains how to configure RAS to supply IP addresses to RAS clients.

To configure a RAS server to use TCP/IP for network connections

1. In Control Panel, double-click the Network option.
2. On the Services tab, click **Remote Access Service** and then click **Properties**.
3. In the **Remote Access Setup** dialog box, click **Network**.
4. In the **Server Settings** box, make sure the **TCP/IP** check box is selected, and then click **Configure**.
5. In the **RAS Server TCP/IP Configuration** dialog box, select whether to allow TCP/IP clients to access the entire network or the RAS computer only.
6. To obtain IP addresses for remote clients from a dynamic host configuration protocol (DHCP) server, click **Use DHCP to assign remote TCP/IP client addresses.**

   Or, if a DHCP server is not available, click **Use static address pool** and then provide a range of IP addresses to a RAS server for assignment to clients. The range must be valid for the subnet the RAS server is in.
7. Type the Begin and End IP addresses from the range allocated for RAS clients. You must assign at least two IP addresses: one address is for a remote client and one address is assigned to the network adapter on the RAS server.

   These values should be entered in dotted decimal notation (for example, 110.11.0.0). These numbers should be assigned by the network administrator.
8. To define excluded addresses within the IP address pool range, use the Excluded Range controls, as follows:
   - Type the first IP address that is part of the excluded range in the **From** box, and type the last number in the **To** box. Then choose the **Add** button. Continue to define any other excluded ranges in the same way.
   - To exclude a single IP address, type the number in the **From** and **To** box and then choose the **Add** button.
   - To remove an IP address range from the excluded range, select the range in the **Excluded Ranges** box, and then choose the **Remove** button.
9. Select the To allow remote workstations to request a predetermined IP address check box, if required.
10. Click **OK.**
11. In the **Network Configuration** dialog box, click **OK**.
12. In the **Remote Access Setup** dialog box, complete any other port configurations and then click **Continue**.

Note: You must restart your computer for the changes to take effect.

Configuring Name Resolution for RAS Clients

RAS client name resolution is based on the available network services and on the RAS server configuration:

- If the RAS server is configured to use a WINS server and a DNS server on the network, RAS clients will use them as well.
- If the RAS server has multiple network adapter cards, clients will use the WINS servers on the first network configured for INS and DNS.

Note that clients can also specify addresses of WINS and DNS servers on a per-entry basis by configuring TCP/IP Settings on the **Dial-Up Networking Server** tab.

RAS clients in small networks where IP addresses do not change can use a HOST file and LMHOSTS file for name resolution. Using these files on the local drive saves transmitting the name resolution request to the WINS server and waiting for a response over the modem.

Note: Standard broadcast name resolution does not work over RAS. Users must have a name resolution method, such as WINS or a LMHOSTS file, or they must use IP addresses.

Choosing a Protocol for a RAS Entry

Dial-Up Networking clients can enter and maintain names and telephone numbers of remote networks. Clients connect to and disconnect from remote networks using the Dial-Up Networking program. Users can select the network protocols to use for a specific Phonebook entry, depending on the type of server you are dialing (PPP, SLIP, or Microsoft RAS).

To choose a protocol for a RAS phonebook entry

1 In Dial-Up Networking, select a phonebook entry and then click **More.**

2 Click either **Edit entry and modem properties** or **Clone entry and modem properties**.

3 On the **Server** tab, select the type of server you are dialing. If you are not sure, select **PPP**.

4 Select the network protocol you want to use. If you are dialing a SLIP or PPP server you can choose to configure TCP/IP settings by selecting **TCP/IP** and then clicking **TCP/IP Settings.**

Configuring a RAS Server to Use IPX

You configure or reconfigure the IPX settings for RAS connections using the Network option in Control Panel.

To configure a RAS server to use IPX for network connections

1. In Control Panel, double-click the Network option.
2. On the **Services** tab, click **Remote Access Service** and then click **Properties**.
3. In the **Remote Access Setup** dialog box, click **Network**.
4. In the **Server Settings** box, make sure the **IPX** check box is selected (if IPX is installed) and then click **Configure**.
5. In the **RAS Server IPX Configuration** dialog box, select whether to allow IPX clients to access the entire network or the RAS server only, and then choose a method for allocating IPX network numbers by selecting one of the following check boxes:

- **Allocate network numbers automatically**. The Windows NT RAS software uses the NetWare Router Information Protocol (RIP) to determine an IPX network number that is not in use in the IPX network. The RAS server assigns that number to the remote client.
- **Allocate network numbers** (manual override). Manual assignments can be useful if you want more control of network number assignments for security or monitoring purposes.

  If you choose to allocate network numbers manually, type the first network number in the **From** box. RAS automatically determines the number of available ports and inserts the ending network number for you.
- **Assign same network number to all IPX clients.** This allows you to assign the same network number to all IPX client using either the automatic or the standard allocation method.

6. To allow the remote client to request its own IPX node number rather than use the node number provided by the RAS server, select the **Allow remote clients to request IPX node number** check box.
7. Click **OK.**
8. In the **Network Configuration** dialog box, click **OK**.
9. In the **Remote Access Setup** dialog box, complete any other port configurations and then click **Continue**.

Notes: You must restart your computer for the changes to take effect.

Allowing remote clients to choose their own node number is a potential security threat to your network. Choosing their own node number allows a client to impersonate a previously connected client and access network resources accessed by the other client.

Configuring Stand-alone Remote Servers to Appear to Local Network Browsers

Users who set up a RAS server at home and dial into it from a computer at work must do the following to have the name of their home server appear in the browsing list of remote clients.

To configure a remote RAS server to appear to local network browsers

1. On the RAS server at home, in Control Panel, double-click the Network option.
2. On the **Identification** tab, click **Change**.
3. In the **Identification Changes** dialog box, type the new domain or workgroup name that matches the domain or workgroup name of the client dialing in and then click **OK**.
4. On the **Adapters** tab, click **Add**.
5. In the **Network Adapter** box, select the **MS Loopback Adapter** and then click **Continue**.
6. In the **MS Loopback Adapter Card Setup** dialog box, click **OK**, type the path to the Windows NT distribution disk(s) and then click **OK**.

   Do not change the default frame type; RAS will work with the default.
7. In the **Network** dialog box, click **OK** to restart your computer.

Note: After restarting, configure the remote RAS server to enable access to the entire network, even though the computer might not be connected to a network. This is described in Configuring RAS to Use LAN Protocols.

Configuring Other Vendors' Dial-Up Servers for NetBIOS IP and IPX

If Windows NT clients dialing into other vendors' dial-up servers must access NetBIOS resources using IP and IPX, the dial-up servers must be configured to forward NetBIOS broadcast traffic. Such forwarding might result in poor performance over the RAS connection if the LAN has substantial NetBIOS activity. For information about configuring a server to forward NetBIOS broadcasts, see NwLnkRip Parameters.

For better performance on TCP/IP networks, Windows NT clients can use WINS servers or proxies when dialing into other vendors' servers if the server can provide access to a Windows NT Server WINS server or proxy agent on the LAN.

Granting Remote Access Permissions

After installing RAS on a server, you must grant remote access permissions to users. Without them, users cannot successfully connect to the RAS computer (even if Dial-Up Networking client software is installed on their computers).

To grant remote access permission to users

1 To start the Administrator's utility, on the **Start** menu, double-click the Remote Access Admin icon in the Administrative Tools folder.

2 Select the server or domain you want to set permissions for.

3 On the **Users** menu, click **Permissions**.

The **Remote Access Permissions** dialog box appears.

4 For further instructions, click the **Help** button.

Note: Microsoft does not recommend granting guest accounts dial-in permission. If you do, be sure to assign a password to the guest account.

ISDN Wide-Area Network Installation

ISDN offers a much faster communication speed than the telephone line. Standard modems typically communicate at 9600 bits per second (bps), whereas ISDN communicates at speeds of 64 or 128 kilobits per second (KBps). Costs for ISDN equipment and lines can be higher than standard modems and phone lines. However, the speed of communication reduces the duration of connections, possibly saving toll charges. Businesses that need this kind of speed usually have a large telecommuting work force or need to do extensive administrative tasks remotely, such as installing software on off-site workstations.

An ISDN line comes with two B channels that transmit data at 64 kilobits per second, and one D channel for signaling that transmits data at 16 kilobits per second. Install ISDN cards on the server and on each client. (For instructions, see the card's documentation.)

You can configure each B channel to operate as a port. Some ISDN drivers allow you to aggregate the channels. This means you can statically assign a higher bandwidth by configuring both B channels to act as a single port. With this configuration, line speed increases to 128 kilobits per second. Channel aggregation schemes are specific to each driver, so you must use the same driver and equipment on the client and server.

Rasdial

Starts the Remote Access Service and connects to the specified entry.

rasdial entryname [username [*password* | ***]] [**/domain:***domain*] [**/phone:***phonenumber*] [**/callback:***callbacknumber*] [**/phonebook**:*phonebookpath*] [/**prefixsuffix**]

rasdial [entryname] **/disconnect**

Parameters

none

Used without parameters, **rasdial** displays the status of current RAS connections.

entryname

Specifies an entry in the current .PBK file, located in the *systemroot*\SYSTEM32\RAS directory. Enclose the entryname in quotation marks (") if the entryname contains spaces or special characters.

The RASPHONE.PBK file will be used unless the Personal Phonebook option is selected. If the Personal Phonebook option is selected the file *username*.pbk will be used. The name is shown on the RASPHONE title bar when Personal Phonebook is selected. Numbers are appended if name conflicts occur.

You can change the location of the .PBK file by changing the registry entry

HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Network\RemoteAccess\PersonalPhonebookPath.

username [*password* | ***

Specifies a username and password with which to connect. If an asterisk is used, the user will be prompted for the password, but will not display the characters typed.

/domain:*domain*

Specifies the domain the user account is located in.

If not present, the last value of the Domain field in the **Connect To** dialog box is used.

/phone:*phonenumber*

Substitutes the specified phone number for the entry's phone number in RASPHONE.PBK.

/callback:*callbacknumber*

Substitutes the specified callback number for the entry's callback number in RASPHONE.PBK.

/disconnect

Disconnects the specifed entry

/**phonebook**:*phonebookpath*

Specifies the path to the phonebook file. The default is *systemroot*\SYSTEM32\RAS*username*.PBK. You can specify a full path to the file.

/**prefixsuffix**

Applies the current prefix/suffix settings (or TAPI location dialing property settings if the entry is configured to use those instead) to the phone number. These settings are configured in Dial-Up Networking. This parameter is off by default.

More Information About Rasdial

Rasdial--Notes
Rasdial--Examples

Rasdial--Notes

Rasdial is the command line equivalent of the Remote Access program (RASPHONE.EXE) **Dial/HangUp** buttons, and is typically used for establishing connections from batch files. There are a few RASPHONE.EXE features not supported in **rasdial**:

- Cannot connect entries requiring Terminal mode user entry during the dial sequence.
- Cannot perform automatic redialing on link failure. However, if RASPHONE is running it will perform redial on entries connected with RASDIAL.
- Does not support operator-assisted or manual dialing.

More Information About Rasdial

- Rasdial--Examples
- Rasdial

Rasdial--Examples

To connect to the OFFICE entry in RASPHONE.PBK, type:

```
rasdial office
```

To connect to the OFFICE 2 entry in RASPHONE.PBK and specify a callback number , type:

```
rasdial "office 2" /callback:555-8086
```

To disconnect from the EAST OFFICE entry, type:

```
rasdial "EAST OFFICE" /d
```

More Information About Rasdial

Rasdial
Rasdial--Notes

Rasadmin

Starts the Remote Access Admin program using the specifed parameters.

rasadmin [*domainname* | *servername*] [**/l**] [**/h**]

Parameters

domainname

Specifies the domain to administer . The RAS servers in the specified domain will be displayed.

servername

Specifies a server to administrate. The logged on user must be a member of the Administrator group.

/l

Sets the Administrator's utility to operate in the low-speed connection mode. This option disables browsing for domains and user names, which can take a long time over a telephone line. For better performance, set this option when you do not need to browse for servers or users. (letter L)

/h

Sets the Administrator's utility to operate in the default connection mode, high-speed. This option enables browsing for domains and user names.

More Information About Rasadmin

Rasadmin--Notes
Rasadmin--Examples

Rasadmin--Notes

You can specify either a domain name or a server name, but not both.

The mode of operation (low- or high-speed) for each domain or server you have previously selected is saved in the Registry. So, if you need to change the previous setting from a low speed to a high speed connection, you must specify /h as a parameter to **rasadmin**.

More Information About Rasadmin

- Rasadmin--Examples
- Rasadmin

Rasadmin--Examples

To administer a server named NT_SERVER01 over a low-speed connection, type:

```
rasadmin \\nt_server01 /l
```

More Information About Rasadmin

- Rasadmin--Notes
- Rasadmin

Overview of Security Features

Windows NT user accounts and domains provide security with encrypted authentication. RAS provides additional security features such as callback and data encryption. You can also install 3rd-party security hosts to prevent unauthorized access to your LAN.

This section covers the following RAS security features:

- Setting RAS up in a domain
- Granting RAS permission to user accounts
- Setting RAS security on user accounts
- Data encryption
- Callback security
- Support for security hosts
- Auditing

Setting RAS up in a Domain

Applying RAS security to clients involves three steps: Setting RAS up in a Windows NT domain, granting RAS permission to Windows NT user accounts, and then setting RAS security on these accounts.

This topic explains Windows NT user accounts and approaches for implementing domain-based security for RAS. This topic assumes you have a domain structure established and provides information about integrating RAS into your existing domain scheme. RAS servers using Windows NT Server domain-based security can be centralized in a single domain or distributed among several domains that might have trust relationships.

Centralized Servers

If your goal is to simplify administration, centralize all remote access servers in a single domain: Only one user account database will need to be maintained, and the system administrator will be able to monitor all RAS servers and users at one time. (Use trust relationships if departments maintain their own user accounts.)

Note: Because the domain is logical rather than physical, centralized servers can be in different locations and still be part of the same domain.

In a trusted domain model, it is best to set up a user account on only one domain for each user, especially for users dialing in through RAS version 1.1 or earlier. If the RAS server cannot find the user's account in the server's domain, it simultaneously checks the trusted domains and accepts the first response. If the first response comes from a domain where the user has a different password or does not have remote access permission, authentication fails even though a second response from another domain might have the same user account with remote access permission.

Distributed Servers

Smaller organizations that value flexibility and local control, or organizations that have no clear need for centralized security, might prefer a *distributed server system,* in which individual departments or workgroups set up and maintain their own remote access domains. Trust relationships can be used to permit access across domains.

Note: If you use Windows NT Server, and you want additional information about user accounts and domains, see the *Windows NT Server Concepts and Planning Guide*.

Granting RAS Access and Permissions

After a RAS server is installed, you must specify who can dial in to it. Use the **Remote Access Admin** utility or User Manager to select a computer's or domain's user accounts. Then grant RAS permission to the user accounts, as shown in the following topics. After passing remote access authentication and connecting to the LAN, remote users can access resources on the application server for which they have permission. Remember: You grant or revoke remote access privileges on a user-by-user basis. So although RAS is running on a Windows NT Server computer, access to the network must be explicitly granted to each user who needs it.

Note: Remote users are subject to Windows NT Server security, just as they are at the office. In other words, they cannot do anything for which they lack sufficient privilege, nor can they access resources for which they do not have permission.

You do not need to create user accounts just for RAS users. RAS servers use the user accounts of any trusted domain or computer on the Windows NT network.

For information about adding a remote client to a domain, see Control Panel Help.

Setting up RAS Security on Accounts

Remote users must be authenticated by a remote access server before they can access or generate traffic on the network. This authentication is a separate step from logging on to Windows NT. User passwords and the authentication procedure are encrypted when transmitted over phone lines.

You can restrict remote users' access to the network and to the remote access server. This allows an administrator to tightly control what information is available to remote users, and to limit their exposure in the event of a security breach.

For more information about granting RAS permission to users, see Setting Remote Access Permissions

Granting and Preventing Network Access

By enabling and disabling sets of protocols and adapters called *bindings*, you dictate network access by remote users:

- Enable bindings to grant user access to resources.
- Disable bindings to prevent user access to resources.

For more information about bindings, see the Network icon in Control Panel and Control Panel online Help.

Restricting Remote Users to the Dial-In Server

Even if the remote access server is connected to a network, you can restrict remote users to the server they dial in to, making the network unavailable to them. You specify if users can access the Entire Network or This Computer Only during RAS Setup. See Configuring RAS to Use LAN Protocols

How Security Works at Connection

The following steps show what happens during a call from a client to a RAS server:

1 Through Dial-Up Networking, a client dials a remote access server.

2 The server sends a challenge to the client.

3 The client sends an encrypted response to the server.

4 The server checks the response against the user database.

5 If the account is valid, the server checks for remote access permission.

6 If remote access permission has been granted, the server connects the client.

If callback is enabled, the server calls the client back and repeats steps 2–6.

Note: When using RAS in a domain environment, changes in remote access permission do not take effect immediately on all servers. It can take up to 15 minutes for replication of the change to other servers in the domain. If necessary, you can resynchronize the domain to ensure that a user with revoked permissions cannot gain access to the network before the change is automatically replicated.

Configuring Callback

As an additional measure of security, RAS offers a Callback feature, which ensures that only users from specific locations can access the RAS server. It also saves toll charges for the user.

When using call back, the user initiates a call and connects with the RAS server. The RAS server then drops the call and calls back a moment later to the pre-assigned call-back number. This security method thwarts most impersonators.

You configure each user's callback privilege when granting remote access permission. (For information about granting permission, see Granting Remote Access Permissions)

In **Remote Access Admin**, the **Remote Access Permissions** dialog box contains three callback options to choose from:

- **Preset To**
- **Set By Caller**
- **No Callback** (the default)

Note: Until the user has been authenticated and called back (if Callback is set), no data from the remote client or the remote access server is transferred.

To change a user's callback option

1 Start Remote Access Admin.

2 From the **Users** menu, choose **Permissions**.

3 Select a user.

4 Assign a different callback option.

Preset To

For maximum security, select **Preset To** and type the number of the phone to which the user's modem is connected. When the user's call reaches the remote access server, the server takes the following steps:

1 Determines whether the user name and password are correct.

2 If they are, responds with a message announcing that the user will be called back.

3 Disconnects and calls the user back at the preset number.

Set this option for stationary remote computers, such as those in home offices.

Set By Caller

Although **Set By Caller** is not really a security feature, it is useful for clients who call from various locations and phone numbers. It also minimizes telephone charges for these users. When the user's call reaches the remote access server, the following events occur:

1 The server first determines if the user name and password are correct.

2 If they are, the Callback dialog box appears on the user's computer.

3 The user types the current callback number in the dialog box and waits for the server to return the call.

No Callback

If the user account has not been configured for callback, RAS establishes a connection as soon as the user's name and password is authenticated.

Connecting Through Intermediary Devices

RAS supports various kinds of *intermediary devices* (security hosts and switches) between the remote access client and the remote access server. These devices include

- Modem-pool switch
- Security host
- X.25 network

Before connecting to the remote access server, a client can have one of two possible dialogs (user input and computer response screens) with each intermediary device:

- Static (a dialog that's always the same and requires no input from the user)
- Interactive (a dialog that always changes, requiring input from the user)

You must configure the client to work with each intermediary device.

If you require both static and interactive dialogs, you must take two steps:

1 Write a script for the static dialog. (See Writing Scripts for Intermediary Devices)

2 Activate terminal mode for the interactive dialogs. (See Activating Terminal Mode on the Client.)

If you require only one kind of dialog, take only one of the above steps. For example

- If your clients connect through only one intermediary with a static dialog (such as an X.25 network), skip step 2.
- If your clients connect through a security host with an interactive dialog, skip step 1.

Writing Scripts for Intermediary Devices

Each script for static dialogs is a section of the SWITCH.INF file. You add a script for each intermediary device to the SWITCH.INF file. (See the PAD.INF file for an example of X.25 network scripts.)

When connecting through modem pools or security hosts you must have a dialog with that device. The dialog will occur either before dialing or after dialing. Although preconnect and postconnect dialogs can be either static or interactive, the preconnect dialog is normally static and the postconnect is normally interactive.

The SWITCH.INF file included in Windows NT provides a generic script that will probably work with little or no modification when connecting to many PPP servers. Try to connect using the generic script. If that does not work, you can copy—then modify—the generic script to match the logon sequence of the remote computer you want to connect to.

See Also

Automating Remote Logons Using SWITCH.INF Scripts

Security Hosts

A *security host* is a third-party authentication device that verifies whether a caller from a remote client is authorized to connect to the RAS server. This verification supplements security already supplied by RAS and by Windows NT Server.

The security host sits between the remote user and the RAS Server. The security host generally provides an extra layer of security by requiring a hardware key of some sort in order to provide authentication. Verification that the remote user is in physical possession of the key takes place before access to the RAS Server is granted. This open architecture allows customers to choose from a variety of security hosts to augment the security in RAS.

For example, one kind of security system consists of two hardware devices: the security host and the security card. The *security host* is installed between the remote access server and its modem. The *security card* is a small unit the size of a credit card, resembling a pocket calculator without keys. The security card displays a different access number every minute. This number is synchronized with the same number calculated in the security host every minute. When connecting, the remote user sends the number on the security card to the host. If the number is correct, the security host connects the remote user with the remote access server.

Another kind of security host prompts the remote user to type in a username (which may or may not be the same as the remote access username) and a password (which differs from the remote access password).

The security host must be configured to allow the RAS server to initialize the modem before the security functions take effect. The RAS server must also be able to directly initialize the modem connected to the security host without security checks from the security host. The security host might interpret the RAS server's attempt to initialize the modem as an attempt to dial out.

You should also set up the host for a fixed bits-per-second (bps) speed rather than autobaud. The fixed bps should equal the value of the **MAXCONNECTBPS** parameter for the entry you created for this device in the Modem.inf file.

To make third-party security devices work with the Remote Access Service

1 If the remote access server's modem is different from the modem in the security host's section in Modem.inf, the Modem.inf file on the remote access server needs to be customized to link the security host to the server's modem. See Customizing the Remote Access Server's MODEM.INF and Installing Security Hosts.

2 The remote user must activate Terminal mode to interact with the security host. See Activating Terminal Mode on the Client.

Note: To use a Security Dynamics security host, you must order two connectors through your Security Dynamics provider to permit initialization of the RAS modem. When you order, specify that you want the dial-out option. The provider will then send you an AND gate and a jumper box. For the ACM/400 security host, you will also receive different software.

Customizing the Remote Access Server's MODEM.INF

When you install a security host between the remote access server and its modem(s), the server's modem and the security host act together as a new type of modem. The MODEM.INF file is shipped with a template for each supported security host paired with a particular modem. For example, the ACM/400 is paired with an AT&T® Comsphere 3820 modem.

To use the security host with a different modem, you will have to modify the MODEM.INF file. For details about MODEM.INF, see Modifying MODEM.INF.

To customize MODEM.INF

1 Make a backup copy of the MODEM.INF file.

2 In the security host's section, replace all of the values for the _**on** and _**off** macros (such as **speaker_on=M1**) with the values from the section for the modem you'll be using.

3 In the security host's section, replace all COMMAND_INIT= lines with the COMMAND_INIT= lines from the section for the modem you'll be using.

The security host section must have the same number of COMMAND_INIT lines as the section for the modem you want to use. Do not change any other line in the security host section.

Note: LOOP= lines are not needed for all modems. However, if you are in doubt, leave them in.

Installing Security Hosts

After customizing the security host section in MODEM.INF, install the security host and modem on the RAS server using the Control Panel **Network** option.

To install a security device

1. In Control Panel, choose the **Network** icon.
2. In the **Services** tab, select **Remote Access Service** and click **Properties**.
3. In the **Remote Access Setup** dialog box, select the security device connected between the remote access server and its modem, and click **Continue**.

   You must also ensure that Hardware Flow Control is not changed from the default, which is on.
4. In the **Network** dialog box, click **OK**.
5. Click **Yes** to restart the computer.

Activating Terminal Mode on the Client

Remote Access Terminal lets the remote user send the correct access number to the security device. If the number is correct, the user is connected to the remote access server.

To prepare the client for Terminal mode

1 In the Dial-Up Networking Phonebook, select the entry you want to connect to.

2 Click More and select **Edit entry and modem properties**.

3 In the **Script** tab, select **Pop up a terminal window**.

4 Click **OK**.

To connect to the remote access server

1 In Dial-Up Networking, select the entry you have just prepared for Terminal mode.

2 Click **Dial**.

When prompted, type your username and password, and click **OK**.

3 When Terminal appears, type the access information required by your security host, for example, your personal identification number, followed by the number on the security card, or a username and password.

4 As soon as the security host indicates that you have been authenticated, click **Done**. The indication varies from one security host to another. For example, you may get an **OK**, or the cursor may just drop to the next line.

Authentication on the remote access server begins.

Modifying the Registry

When you install the Remote Access Service on a server, the Setup program adds the **RemoteAccess** key to the Windows NT Registry. The **RemoteAccess** key and its subkeys contain parameters specific to Remote Access.

The Remote Access Setup program adds Remote Access keys to the Windows NT Registry.

Remote Access generally supplies good default values for RAS parameters, which you normally do not need to override. Still, for some systems, you might want to adjust individual parameters to suit your particular needs.

There are several sets of parameters you can modify or add. To override their defaults, add or change the appropriate key in the Registry. You can find these keys on the paths indicated in each section below.

To edit the Registry

1 In the **Start** menu, click **Run**.

2 In the **Open** box, type **regedt32**.

This command can also be run from the Command Prompt.

For detailed information on how to add a parameter to a key in the Registry, see online Help for the Windows NT Registry editor.

RemoteAccess Parameters

The default values of these parameters work well for all Windows NT operations.

The Parameters subkey for RemoteAccess has the following Registry path:

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RemoteAccess\Parameters.`

AuthenticateRetries **REG_DWORD**

Range: *0 to 10*

Sets the maximum number of unsuccessful retries that are allowed if the initial attempt at authentication fails.

Default: 2.

AuthenticateTime **REG_DWORD**

Range: *20 - 600 seconds*

Sets the maximum time limit, in seconds, within which a user must be successfully authenticated. If the client does not complete the authentication process within this time, the user is disconnected.

Default: 120 seconds.

AutoDisconnect **REG_DWORD**

Range: *0 - 1000 minutes*

Sets the time interval after which inactive connections are terminated. Inactivity is measured by lack of NetBIOS session data transfer, such as copying files, accessing network resources, and sending and receiving electronic mail. You might want to set this parameter to 0 minutes if clients are running NetBIOS datagram applications. Setting this parameter to 0 turns off **AutoDisconnect**.

Default: 20 minutes.

CallbackTime **REG_DWORD**

Range: *2 - 12 seconds*

Sets the time interval that the server waits before calling the client back when the Callback feature has been set. Each client communicates the value of its own callback time when connecting to a Remote Access server. This value can be found in the Modem.inf file for the client. If this value is not communicated (that is, if the client does not communicate a value for the callback time, as with Remote Access version 1.0 and 1.1 clients), then the value of the **CallbackTime** parameter becomes the default.

Default: 2 seconds.

EnableAudit **REG_DWORD**

Range: *0 - 1*

Determines whether Remote Access auditing is turned on or off. If this feature is enabled, all audits are recorded in the Windows NT event log. You can see these audits in the Windows NT Event Viewer.

Default: 1 (enabled).

NetbiosGatewayEnabled **REG_DWORD**

Range: *0 - 1*

Makes the server function like a NetBIOS gateway, allowing clients to access the LAN. If disabled, remote clients can access only the resources on the Remote Access server in a point-to-point connection; dial-in users cannot see the network or access network resources. This parameter should never be modified directly. Use RAS Setup to modify this parameter because RAS Setup also modifies bindings when changing this parameter.

Default: 1 (enabled).

NetbiosGateway Parameters

The Registry path for these entries is the following:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
\RemoteAccess\Parameters\NetbiosGateway
```

DisableMcastFwdWhenSessionTraffic **REG_DWORD**

Range: *0 - 1*

Allows NetBIOS session traffic (for example, Windows NT–based applications) to take priority over multicast datagrams (such as server messages). In other words, multicast datagrams are transferred only when there is no session traffic. Unless you're using an application that depends on multicast datagrams, leave this parameter enabled.

Default: 1 (enabled).

EnableBroadcast **REG_DWORD**

Range: *0 - 1*

Determines whether broadcast datagrams are forwarded to remote computers. Broadcast datagrams are not often useful and take up too much bandwidth on a slow link. Unless you're using an application that relies on broadcast datagrams, leave this parameter disabled.

Default: 0 (disabled).

See also **MultiCastForwardRate**.

EnableNetbiosSessionsAuditing **REG_DWORD**

Range: *0 - 1*

Turns on and off Remote Access auditing of the establishment of NetBIOS sessions between the remote clients and the Windows NT servers. Turning this parameter on helps the administrator track the NetBIOS resources accessed on the LAN.

Default: 0 (disabled).

MaxBcastDgBuffered **REG_DWORD**

Range: *16 - 255*

Sets the number of broadcast datagrams that the gateway buffers for a client. If you're using an application that communicates extensively through multicast or broadcast datagrams, then increase this parameter so that the Remote Access server can deliver all datagrams reliably.

Default: 32.

MaxDgBufferedPerGroupName **REG_DWORD**

Range: *1 - 255*

Sets the number of datagrams that can be buffered per group name. Increasing this value buffers more datagrams per group name but also takes up more virtual memory.

Default: 10.

MaxDynMem **REG_DWORD**

Range: *131072 - 4294967295*

Sets the amount of virtual memory used to buffer NetBIOS session data for each remote client.

Note: Because the Remote Access server is a gateway between the slow line and the LAN, data is stored (buffered) in its memory when coming from the fast line (LAN) before it is forwarded to the slow line (asynchronous line).

The Remote Access server minimizes the usage of the system's physical memory by locking only a minimal set of pages (about 64K per client) and making use of virtual memory (up to **MaxDynMem**) to buffer the rest of the data.

So, as long as you have space on your hard disk to expand Pagefile.sys, you can increase this parameter if needed.

You might have problems if you have an application with a LAN (fast) sender and an asynchronous (slow) receiver, and if the sender is sending more data than the Remote Access server can buffer in **MaxDynMem**. The Remote Access server tries to apply a form of NetBIOS level flow control by not submitting Ncb.receive on the session until it has enough buffer space to get incoming data.

For this reason, if you have such an application, you should increase your NetBIOS SEND/RECEIVE time-outs on the application server so that it waits for all data to be transmitted over the slow link to the remote client.

Default: 655350.

MaxNames **REG_DWORD**

Range: *1 - 255*

Sets the number of unique NetBIOS names each client can have, with a limit of 255 names for all clients together.

Default: 255.

Note: Remote clients running Windows NT and Windows for Workgroups might need as many as seven or eight names each. To accommodate these computers, make sure **MaxNames** is set to 8 or greater. If you have Windows NT or Windows for Workgroups clients dialing in to servers running Remote Access version 1.1 or earlier, set this parameter to 8 or greater.

MaxSessions **REG_DWORD**

Range: *1 - 255*

Sets the maximum number of simultaneous NetBIOS sessions each client can have, with a limit of 255 sessions for all clients together. If you have multiple clients connecting simultaneously with each running 4 or 5 sessions, decrease the value of this parameter so that the total number of sessions does not exceed 255.

Default: 255.

MultiCastForwardRate **REG_DWORD**

Range: *-1 (disabled), 0 - 32,767 second*

Governs the multicasting of group name datagrams to all remote computers. This parameter filters datagrams sent on group names by forwarding them at a time interval specified by the parameter.

Default: 5.

The value - 1 disables forwarding. The value 0 guarantees delivery of group name datagrams. The value n forwards datagrams every n seconds, where
$1 \leq n \leq 32{,}767$.

If the **EnableBroadcast** parameter is set to 0, then broadcasts are not forwarded even if the **MultiCastForwardRate** parameter is set to a positive number (in this case, only multicast datagrams are forwarded). If **MultiCastForwardRate** is set to -1, broadcasts are still not forwarded even if **EnableBroadcast** is set to 1. See also **EnableBroadcast**.

To save bandwidth for session traffic, you should filter the datagrams. However, if you have an application based on multicast datagrams, set this parameter to 0. Setting it to 0 guarantees delivery of all datagrams sent on group names from the LAN to the remote client.

NumRecvQueryIndications **REG_DWORD**

Range: *1 - 32*

Allows a Remote Access client to initiate multiple network connections simultaneously. If a remote client is running a NetBIOS application that does multiple NCB.CALL commands simultaneously, increase this parameter to improve performance.

Default: 3.

See Also

Nbf Parameters

RcvDgSubmittedPerGroupName **REG_DWORD**

Range: *1 - 32*

Determines the number of NetBIOS commands of the type Receive Datagram that can be submitted simultaneously per group name on the LAN stack. Keep this setting as small as possible to minimize the amount of memory consumed by system resources. Each datagram command received locks about 1.5K of physical memory in the system.

Default: 3.

RemoteListen **REG_DWORD**

Range: *0 - 2*

Sets the level of access that a LAN client has to a remote client's resources. This is done by posting NCB.LISTEN commands on the NetBIOS names of the client.

Default: 1 (messages).

Setting	Meaning	Remark
0	Allows no access.	Because every remote listen posted consumes one session, setting this parameter to 0 saves sessions.
1	Makes the Server and Messenger services available on the client.	A remote client running the Server service can make its resources (such as disks and printers) available to LAN users. A remote client running the Messenger service can receive messages from LAN users, printers, and so on.
2	Enables NCB.LISTEN for all remote client NetBIOS names.	This setting allows any NetBIOS application running on a client to answer NCB.CALL commands issued by LAN applications.

Note: It is best to leave the **RemoteListen** parameter set to the default, 1 (messages).

Allowing NCB.LISTEN capability on remote clients can significantly drain system resources and therefore is not recommended. If the **RemoteListen** parameter is configured to 2, Remote Access posts an NCB.LISTEN on all NetBIOS names of Remote Access clients. Considering that the average Windows NT client has about 7 or 8 NetBIOS names assigned to it, the total number of NetBIOS names for which an NCB.LISTEN would be posted is 7 or 8 * 256 (the maximum number of clients per Remote Access server).

SizWorkBufs **REG_DWORD**

Range: *1024 - 65536*

Sets the size of work buffers. The default setting is optimized for the server message block (SMB) protocol, the protocol between the client and the server running Windows NT Server.

Default: 4500.

IP Parameters

The Registry path for these entries is the following:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
\RemoteAccess\Parameters\IP
```

WINSNameServer **REG_SZ**

Value: *IP Address*

Change this parameter in a RAS server's Registry to override the automatic assignment of the RAS server's WINS server to the RAS client.

This parameter appears in the Registry only during an active connection to a RAS server.

WINSNameServerBackup **REG_SZ**

Value: *IP Address*

Add this parameter to a RAS server's Registry to override the automatic assignment of the RAS server's backup WINS server to the RAS client.

This parameter appears in the Registry only during an active connection to a RAS server.

WIDNSNameServer **REG_MULTI_SZ**

Value: *IP Addresses*

Add this parameter to a RAS server's Registry to override the automatic assignment of the RAS server's DNS servers to the RAS client.

This parameter appears in the Registry only during an active connection to a RAS server.

AsyncMac Parameters

The Registry path for these entries is the following:

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AsyncMac`*`n`*`\Parameters`

MaxFrameSize **REG_DWORD**

Range: *576 - 1514*

Determines the maximum frame size. Use smaller frames for noisy links. A lower setting sends less data per frame, slowing performance. Do not change this parameter for previous versions of the Remote Access Service. The value is negotiated between the server and Windows NT clients.

Default: 1514.

TimeoutBase **REG_DWORD**

Range: *500 - 1000*

Determines the amount of time that elapses on a NetBIOS gateway before a connection is disconnected. If you are experiencing an abnormal number of time-out errors using the NetBIOS gateway (more than 10 time-outs per 100 kilobytes received), increase the **TimeoutBase** value from 500 to 1000 if your computer has a security device or your computer's modems have hardware compression or error control enabled.

With **TimeoutBase** increased to 1000, network functionality may on very rare occasions act abnormally. For example, you might have to type network commands more than once, or functionality may periodically slow down.

Default: 500.

NdisWan Parameter

The Registry path for this entry is the following:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
\NdisWan\Parameters
```

NetworkAddress="*xxxxxx*" **REG_SZ**

Value: *Network address*

Add this parameter to reassign the first 4 bytes of the 6-byte IEEE address. For example, if you reset the address to "03-1F-2C-81-92-34", only the first 4 bytes are looked at. The last 2 bytes are reserved to uniquely identify the port. Reset this parameter in the **NdisWan\Parameters** key with the datatype REG_SZ.

NwlnkRip Parameters

The Registry path for these entries is the following:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
\NwlnkRip\Parameters
```

NetbiosRouting **REG_DWORD**

Range: *0, 2, 4, or 6*

Controls the forwarding of IPX NetBIOS broadcast packets to and from the LAN. The RAS server can forward NetBIOS broadcast packets (IPX type-20) between RAS clients and the local network.

Set to 2, this parameter enables forwarding of NetBIOS broadcast packets from the remote client to the LAN.

Set to 4, this parameter enables forwarding of NetBIOS broadcast packets from the LAN to the remote client.

Set to 6, this parameter enables two-way forwarding of NetBIOS packets between remote clients and the LAN.

You may also need to set the **DisableDialinNetbios** registry entry, depending on your IPX NetBIOS application configuration. See NwlnkIpx Parameters for more information.

Default: 2.

NwlnkIpx Parameters

The Registry path for these entries is the following:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
\NwlnkIpx\Parameters
```

DisableDialinNetbios **REG_DWORD**

Range: *0 - 3*

Controls the forwarding of IPX type 20 packets between the remote RAS client, the LAN (by means of the RAS IPX router) and the RAS server running an IPX NetBIOS application (internal net). This parameter controls only dial-in lines on RAS servers.

Set to 0, IPX type 20 packets will broadcast from the RAS server to remote clients and from the remote clients to the RAS server then through the IPX router for broadcast on the LAN (if the router is configured to forward IPX NetBIOS packets.

Set to 1 (default), IPX type 20 packets will broadcast only from remote clients to the internal net and to the RAS IPX router. This setting disables broadcasts from the internal net to the remote clients.

Set to 2, IPX type 20 packets will broadcast from the internal net to the remote clients.

Set to 3, all IPX type 20 broadcasts are disabled.

You might also need to set the **NetbiosRouting** registry entry, depending on your IPX NetBIOS application configuration. See NwlnkRip Parameters for more information.

Default: 1.

RasMan Parameters

The Registry path for these entries is the following:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
\RasMan\Parameters
```

NumberOfRings **REG_DWORD**

Range: *1 - 20* (outside this range the default value is assumed)

Specifies the number of RING messages from the modem after which RAS will pick up the call. This only works with UNIMODEM devices.

Default: 1.

Logging **REG_DWORD**

Range: *0 - 1*

Sets logging of all communication from serial ports to the device connected to them during command mode. This parameter is useful for solving problems with serial devices and for testing new entries added to the Modem.inf or Pad.inf files.

Because some of the information will not be printable characters, you might want to view the Device.log file in a text editor that can display both character and hexadecimal output. Also, Device.log contains a carriage return and line feed at the end of each line. These bytes are provided by the program that creates the Device.log file and do not represent information communicated from or to the device.

Set to 1, communication from the serial port to the device connected to it will be logged in the file *systemroot*\system32\ras\device.log.

Logging is suspended after successful connection to the remote device and transmission of data. Logging resumes when a new connection is established and is appended to Device.log until the file size exceeds approximately 100K. Device.log is then cleared and logging resumes. Device.log is also cleared when any RAS component is started after all RAS components have been stopped.

Default: 0.

PPP Parameters

The Registry path for these entries is the following:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
\RasMan\PPP
```

MaxTerminate **REG_DWORD**

Range: *0 - unlimited*

Sets the number of Terminate-Request packets sent without receiving a Terminate-Ack before assuming that the peer is unable to respond.

Default: 2.

MaxConfigure **REG_DWORD**

Range: *0 - unlimited*

Sets the number of Configure-Request packets sent without receiving a valid Configure-Ack, Configure-Nak, or Configure-Reject before assuming that the peer is unable to respond.

Default: 10.

MaxFailure **REG_DWORD**

Range: *0 - unlimited*

Sets the number of Configure-Nak packets sent without sending a Configure-Ack before assuming that the configuration is not converging.

Default: 10.

MaxReject **REG_DWORD**

Range: *0 - unlimited*

Sets the number of Config-Rejects sent before assuming that the PPP negotiation will not converge.

Default: 5.

RestartTimer **REG_DWORD**

Range: *0 - unlimited*

Sets the time (in seconds) available for transmission of Configure-Request and Terminate-Request packets. Expiration of the Restart timer causes a time-out event, and retransmission of the corresponding Configure-Request or Terminate-Request packet.

Default: 3.

NegotiateTime **REG_DWORD**

Range: *0 - unlimited*

Sets the amount of time allowed (in seconds) for PPP negotiation to converge successfully before disconnecting the line. 0 means that the line will never be hung up.

Default: 150.

ForceEncryptedData **REG_DWORD**

Range: *0 - 1*

Used on RAS servers only. Requires the use of data encryption by remote clients. Clients must support the MS-CHAP protocol (introduced in Windows NT version 3.5) or the connection will be automatically dropped. Set to 1, the server requires data encryption. Set to 0, the server does not require data encryption.

Default: 0.

ForceEncryptedPassword **REG_DWORD**

Range: *0 - 2*

Used on RAS servers only. Sets the use of the Challenge-Handshake Authentication Protocol (CHAP) while authenticating clients. Set to 0, the server allows any encryption method, including clear text. Set to 1, the server allows any encryption

method, except clear text. Set to 2, the server requires MS-CHAP during authentication.

Default: 2.

Logging **REG_DWORD**

Range: *0 - 1*

Sets logging of PPP events. Set to 1, all PPP events will be logged in the file *systemroot*\system32\ras\ppp.log. This parameter is useful for solving problems with PPP connections.

Default: 0.

DisableSoftwareCompression **REG_DWORD**

Range: *0 - 1*

Enables or disables software compression. Set to 1, software compression is disabled. Set to 0, software compression is enabled.

Default: 0.

PPP Subkeys

The following entries are subkeys to the PPP key.

CBCP **REG_EXPAND_SZ**

Range: *DLL Path*

Specifies the location of the Callback Control Protocol (CBCP) DLL. CBCP negotiates callback information with the remote client. Always present.

CHAP **REG_EXPAND_SZ**

Range: *DLL Path*

Specifies the location of the Challenge-Handshake Authentication Protocol (CHAP) DLL. Always present.

COMPCP **REG_EXPAND_SZ**

Range: *DLL Path*

Specifies the location of the Compression Control Protocol (CCP) DLL. CCP negotiates compression with the remote client. Always present.

IPCP **REG_EXPAND_SZ**

Range: *DLL Path*

Specifies the location of the Internet Protocol Control Protocol (IPCP) DLL. Present if RAS is configured to use TCP/IP and TCP/IP is installed.

These parameters can be added to the **IPCP** subkey:

AcceptVJCompression **REG_DWORD**

Range: *0 - 1*

Add this parameter to prevent IPCP from accepting IPCP standard option 0x02, Van Jacobson header compression. If this parameter has not been added or is set to 1, RAS clients will accept VJ compression.

Default: not in registry

PriorityBasedOnSubNetwork **REG_DWORD**

Range: *0 - 1*

A computer can connect to the LAN using a network card and a RAS connection. If the RAS connection and the LAN network adapter card are assigned addresses with the same network number and the **Use Default Gateway On Remote Network** checkbox is selected, then all packets will be sent over the RAS connection, though the two addresses are in different subnetworks within the same network.

Set this parameter to 1 to send packets over the network card.

For example, if the network adapter card has IP address 10.1.1.1 (subnet mask 255.255.0.0) and the RAS connection is assigned the address 10.2.1.1, RAS will send all 10.x.x.x packets using the RAS connection. If the parameter is set, RAS will

send 10.2.x.x packets using the RAS connection and 10.1.x.x packets using the network adapter card.

Default: not in registry

RequestNameServerAddresses **REG_DWORD**

Range: *0 - 1*

Add this parameter on RAS clients to prevent IPCP from requesting the Microsoft extension options for WINS and DNS server address negotiation, i.e. IPCP options 0x81, 0x82, 0x83, 0x84. If this parameter has not been added or is set to 1, the client-side will request the addresses.

Default: not in registry

RequestVJCompression **REG_DWORD**

Range: *0 - 1*

Add this parameter on RAS clients to prevent IPCP from requesting IPCP standard option 0x02, Van Jacobson header compression. If this parameter has not been added or is set to 1, RAS clients will request VJ compression.

Default: not in registry

IPXCP **REG_EXPAND_SZ**

Range: *DLL Path*

Specifies the location of the Internetwork Packet Exchange Control Protocol (IPXCP) DLL. Present if RAS is configured to use IPX and the Client Service for NetWare or Gateway Service for NetWare is installed.

NBFCP **REG_EXPAND_SZ**

Range: *DLL Path*

Specifies the location of the NetBEUI Framing Control Protocol (NBFCP) DLL. Present if RAS is configured to use NetBEUI and NetBEUI is installed.

PAP **REG_EXPAND_SZ**

Range: *DLL Path*

Specifies the location of the Password Authentication Protocol (PAP) DLL. Always present.

Rdr Parameters

The Registry path for this entry is the following:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
\Rdr\Parameters
```

RawIoTimeLimit **REG_DWORD**

Range: *see below*

This parameter applies only to configurations using the NetBIOS gateway.

Sets the redirector to send data in 64 kilobyte blocks. When **RawIoTimeLimit** turned on, throughput increases by 10-15 percent. All other simultaneous data transfers are blocked when communicating at this speed.

This parameter is turned off for slow links and on for faster links, by default. For example, if you are communicating at 14,400 bps or slower, this feature is turned off. If you are communicating at faster speeds, such as through an ISDN line, this feature is turned on.

The following list shows what values turn raw I/O on and off for ISDN connections:

RawIoTimeLimit set to 9:

Raw I/O is enabled when connected through one 64K channel.
Raw I/O is enabled when connected through two 64K channels.

RawIoTimeLimit set to 5 (default):

Raw I/O is disabled when connected through one 64K channel.
Raw I/O is enabled when connected through two 64K channels.

RawIoTimeLimit set to 0:

Raw I/O is disabled when connected through one 64K channel.
Raw I/O is disabled when connected through two 64K channels.

RasArp Parameters

The Registry path for this entry is the following:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
\RasArp\Parameters
```

FilterBroadcasts **REG_DWORD**

Range: *0 - 1*

Add this parameter to cause RAS to transmit broadcast packets (for example, destination IP address 255.255.255.255) and subnet multicasts (for example, destination IP address 11.101.255.255). Set this parameter to 0 on clients if the computer is calling into third-party remote access routers that support broadcast/multicast forwarding. (Windows NT Remote Access servers do not forward broadcasts or multicasts.)

Default: 1.

Nbf Parameters

The Registry path for this entry is the following:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
\Nbf\Parameters
```

InitUIFrames **REG_DWORD**

Range: *0 - unlimited*

Add this parameter to set the number of NetBIOS names that can be added to the network simultaneously from a RAS client.

Default: 5.

Example Internet Session

With Windows NT Dial-Up Networking and TCP/IP, a modem or other WAN connection, and one of the many publicly available Internet browsers or tools, you can connect to an Internet server and browse the information and services available on the Internet.

A computer running Windows NT Server can also provide access to the Internet through an Internet service provider for up to 256 remote clients.

You connect to the Internet through an Internet service provider using Dial-Up Networking. Once connected, you can then use an Internet browser to search for information. This topic assumes you have installed and configured Windows NT, TCP/IP, Dial-Up Networking, and the Internet browser of your choice.

Start Dial-Up Networking from the My Computer group. Select the phonebook entry for the Internet service provider you will use and click **Dial**.

Dial-Up Networking dials the Internet service provider and log you on to the system. The actual sequence for logging on varies based on the requirements of the service provider you are calling. PPP connections will probably be entirely automatic. SLIP connections might require a terminal logon; the terminal logon may or may not permit you to automate the logon with scripts in the Switch.inf file. After successful connection and logon to the Internet service provider, you can minimize Dial-Up Networking.

You are then connected to the Internet and can use the Internet tools of your choice. When you have finished using the Internet, disconnect from your Internet service provider to prevent unnecessary charges.

Using Windows NT as an Internet Client

Dial-Up Networking makes connecting to the Internet easy. These components enable you to access the Internet:

- The TCP/IP protocol installed and enabled for the Dial-Up Networking Internet phonebook entry
- Dial-Up Networking installed on your computer and a user account with Remote Access Service (RAS) permissions if you are part of a corporate domain
- Modem or other WAN connection to an Internet service provider
- Account with an Internet service provider
- Internet tools such as browsing tools, FTP, or Telnet

TCP/IP and Dial-Up Networking

TCP/IP is the suite of protocols used for all Internet traffic. Windows NT TCP/IP is fully compatible for use on the Internet. Dial-Up Networking clients support both the PPP protocol and the SLIP protocol. These protocols are used by most Internet service providers, allowing Windows NT clients to connect to virtually all Internet service providers.

Modems and WAN Connections

Your connection to an Internet service provider will be through a modem and telephone line, an ISDN card and ISDN line, an X.25 network, or Point-to-Point Tunneling Protocol (PPTP).

If you are using a modem, you will want the fastest possible speed to reduce downloading time while on the Internet. Modems of 9600 baud or above are recommended. For more information about modems or other WAN connections, see WAN Options.

Obtaining an Internet Account with a Service Provider

There are Internet service providers around the world. Similar to other online services or bulletin boards, you dial into the service number and log into the remote system. Once connected, you have access to the Internet and any other services, such as electronic mail, provided by the service provider. Fees usually apply for all commercial Internet service providers.

Internet Tools

A multitude of tools are available to access the information and services on the Internet. The tools you select will depend on the information you want and how it is stored on the Internet.

Windows NT TCP/IP provides two standard tools for accessing Internet servers, FTP and TELNET. FTP is a command-line utility that permits you to connect to FTP servers and transfer files. TELNET is a graphical application that lets you log in to remote computers and issue commands as if you were at the computer's keyboard.

Many other tools are available through the Internet or commercially. Technology on the Internet has advanced since the FTP and TELNET standards were created. To fully explore the Internet and some of the advanced features available, you will need to obtain one or more Internet browsers. Two popular FTP sites for obtaining public-domain Internet browsers (and other Windows Sockets applications) are **sunsite.unc.edu** and **ftp.cica.indiana.edu**.

Installing Windows NT Software for Internet Access

This section explains installing TCP/IP and Dial-Up Networking (RAS) and configuring them for Internet access. You must install TCP/IP to access the Internet. You must install Dial-Up Networking if the computer that provides access to the Internet is not on your local area network. (Note Dial-Up Networking is probably installed on this computer since the file you are reading is only installed with Dial-Up Networking.)

After TCP/IP and Dial-Up Networking installation and configuration, use the Windows NT Explorer to review the shared directories available on your computer. Shared resources on your computer may be available to other remote computers, depending on your internet service provider. Stop sharing, or change the sharing configuration of any resources you do not want remote computers to use.

TCP/IP

TCP/IP is the set of protocols used on all computers using the Internet. To install TCP/IP use the Network option in Control Panel. On the **Protocols** tab, click **Add** and then select **TCP/IP Protocol**. Follow the instruction on screen to complete TCP/IP installation.

Once TCP/IP is installed, you may need to configure the following parameters to operate correctly on the Internet.

IP Address

If your network uses dynamic host configuration protocol (DHCP), you must determine if your DHCP server provides valid IP addresses and subnet masks for use outside your local network. If it does not, you must disable DHCP configuration and use a specific IP address and subnet mask.

Default Gateway

If you are connecting to an Internet server through RAS, the default gateway configured through RAS will be used.

DNS

The Domain Name Service (DNS) configuration on your computer may be for use on your local area network only. You may need to add DNS addresses to efficiently access the Internet.

HOSTS or LMHOSTS file

You can improve efficiency of connections to frequently accessed servers on the Internet by adding entries to your HOST or LMHOSTS file. Windows NT consults these local files for name resolution before consulting a DNS server on the Internet.

Dial-Up Networking

Dial-Up Networking is the software that allows you to use a remote Internet service provider. To install RAS, use the Network option in Control Panel. On the **Services** tab, click **Add** and then select **Remote Access Service**. Follow the instructions on the screen to complete Dial-Up Networking installation. See Installing Dial-Up Networking for detailed instructions on installing Dial-Up Networking.

You may need to configure the following parameters during Dial-Up Networking installation or after installation using the Network option in Control Panel. You must also configure individual Dial-Up Networking entries as described in Configuring Remote Access Entries for Internet Use.

Port Configuration

The port you use to connect to an Internet service provider must be configured for **Dial Out** or **Dial Out And Receive Calls**.

Network Configuration

The **TCP/IP** check box must be selected in the **Dial Out Protocols** box in the **Network Configuration** dialog box.

Installing Internet Tools

The Internet is a vast collection of information with many methods to access the information. This topic briefly describes some Internet tools and provides the process for installing them on Windows NT. Consult the Internet or your local library or bookstore for comprehensive discussions of the tools available for using the Internet.

History of Internet Tools

The Internet has been evolving since the early 1970s. Early servers on the Internet conformed to original Internet protocols, such as the file transfer protocol (FTP) or virtual terminal protocol (VTP, now called TELNET). These protocols generally allow you to copy files and/or issue commands or start programs through a character-based interface or, more recently, through a graphical user interface (such as Windows or XWindows).

As the volume of information on the Internet increased, other tools were created that allowed users to search for information on multiple servers. Archie is a common Internet standard that compiles indexes of the information on internet servers. You can then use one of several interfaces that let you query the Archie databases. Other indexing tools are also in use on the Internet.

Recently, Internet technology has grown beyond the simple file transfers on character-based FTP or TELNET servers. Newer servers on the Internet now have graphical interfaces and present information and services to Internet users using hypertext documents. Gopher servers and World Wide Web (WWW) servers now automatically provide formatted text, sounds, and animation to Internet users. You must use the proper browser (such as Cello or Mosaic) to use these Internet servers. Fortunately these browsers usually support the older standards, such as FTP, so you can use the newer browsers to access multiple servers and data types.

Finding Internet Tools

Windows NT TCP/IP provides FTP and TELNET. FTP is a character-based utility that permits you to connect to FTP servers and transfer files. TELNET is graphical application that lets you log in to remote computers and issue commands as if you were at the computer's keyboard. Multiple variations of FTP, TELNET, and other programs based on earlier Internet standards are also available on the Internet or commercially.

You will need to obtain one or more Internet browsers to access the hypertext documents available on newer Internet servers. In general these browsers have been developed at universities or educational institutions and are in the public domain, meaning they are freely distributed. Two popular FTP sites for obtaining public-domain Internet browsers (and other Windows Sockets applications) are **sunsite.unc.edu** and **ftp.cica.indiana.edu**.

Installing Internet Tools

Once you have a connection to an Internet service provider, you can use the **ftp** program provided with Windows NT TCP/IP to connect to an FTP server and download files, including Internet tools. The same tool may exist for different operating systems or processors. Ensure you obtain the correct version of the tool.

The files will probably have been compressed using the shareware program **pkzip**. You use the shareware program **pkunzip** to expand the .ZIP files on your local hard drive. The shareware compression tools are often available on local bulletin board or FTP servers in an uncompressed format.

After you have completed uncompressing the files for a particular program, you should read any available readme files for specific information about installing and configuring the program and comply with those instructions. Most public domain software designed for Windows 3.1 or Windows for Workgroups will work on Windows NT without modification.

You should now be able to start the Internet tools from the Windows NT desktop.

For an example of using an Internet tool with Windows NT, see Example Internet Session.

Configuring Remote Access Entries for Internet Use

You must create an entry in Dial-Up Networking to call an Internet service provider. This topic explains how to configure individual Dial-Up Networking entries to work with an Internet service provider. After creating an entry, you must configure the **Network** settings and the **Security** settings for the entry to work with the Internet service you are calling.

Creating an entry to connect to the Internet

1. In the **Dial-Up Networking** dialog box, click **New**.
2. Follow the instructions on your screen. Or, select the check box to edit the phonebook directly, click **Finish**, and continue with the following steps.
3. On the **Basic** tab, type a name for your entry (for example, **Internet)**, type the phone number to your Internet service provider, and select a modem to use.
4. On the **Server** tab, select your server type, **PPP** or **SLIP**.
5. In the **Networking protocols** box, select **TCP/IP**.

   If PPP is selected, make sure the NetBEUI and IPX check boxes are cleared.

   If SLIP is selected, you will automatically use TCP/IP.
6. Make sure the **Enable PPP LCP extensions** check box is selected. This enables newer PPP features and should be cleared only if you are unable to establish a connection while this setting is enabled.
7. Click **TCP/IP Settings**.
8. If your Internet service provider has assigned an IP address for your use, enter that number in the **Specify an IP address** box. Or, if no number was assigned or you know the server assigns IP addresses, click **Server assigned IP address**.
9. If your Internet service provider has assigned a DNS and/or WINS server IP address for your use, enter that number in the **Specify name server addresses** box. Or, if no numbers were assigned or you know the server assigns name server addresses, click **Server assigned name server addresses**.
10. Make sure the **Use default gateway on remote network** check box is selected.
11. If your Internet service provider uses header compression, select the **Use IP header compression** check box.
12. Click **OK** and then click **Dial**.

Note: Depending on your Internet service provider, you may need to make some modifications to your security settings. When you connect to the Internet service provider, some form of logon or authentication will occur. Your Internet service provider should tell you the logon sequence for their servers. You can use the **Security** tab to configure RAS for logging in to the Internet service provider.

To configure an entry for authentication on the remote server

1. In the **Dial-Up Networking** dialog box, click **More.**
2. Click **Edit entry and modem properties**.
3. On the **Security** tab, select the authentication method specified by your Internet service provider.

   Many Internet service providers require you to use clear text. If in doubt, select **Accept any authentication including clear text**.
4. After you have selected the security settings, click **OK**.

Note: If you click **Accept any authentication including clear text**, you must also know the sequence of logon for your service provider, and any required commands.

If your Internet service provider has a well defined logon sequence, you can create a script in the Switch.inf file that provides the required commands automatically at logon. Once you have created a scripting section in the *systemroot*\System32\RAS\Switch.inf file, you can select it on the **Script** tab. See Using Other Device Command Files (.INF) for more information about creating logon scripts.

Using Windows NT Server to Provide Internet Access

In conjunction with a router and Internet service provider, Windows NT Server acts as a gateway to the Internet for remote clients. Up to 256 clients can dial into the RAS server using standard telephone lines, ISDN lines, X.25, or PPTP. The clients then use any PPP-compliant software or Windows NT computer, together with Internet browsing tools, to access the Internet.

The Internet Connection

The Internet connection to your site will typically be made through a leased line to a router located on your network. Thus data travels over the Internet, over a leased line to a router, through the router, over your local network, to the RAS server and then to remote clients.

Typical Requirements for Creating Internet Access

These are the typical requirements for a system that will provide Internet access using Windows NT Server.

- Leased line from Internet service provider to router on local network (provided by communications company)
- Router on local network
- Local area network. For security this may be isolated from your primary network or you may have other security measures, often called *firewalls*.
- Computer running Windows NT Server with TCP/IP and RAS installed
- Multiport serial adapter on RAS server for multiple remote client connections
- Specialized communications hardware (ISDN or X.25 adapters)
- Valid Internet IP address assigned through a DHCP server on the local area network or statically through the RAS server
- Domain Name Service (DNS) server IP address. The DNS server may reside on the local area network or on the Internet.

See Installing and Configuring Windows NT Software to Provide Internet Access for information.

Installing and Configuring Windows NT Software to Provide Internet Access

You must install TCP/IP and RAS to provide Internet access. (Note that RAS is probably installed on this computer since the Help file you are reading is only installed with RAS.)

TCP/IP

TCP/IP is the underlying suite of protocols used on all computers using the Internet. To install TCP/IP use the Network option in Control Panel. See the Windows NT Server *Networking Supplement* for detailed information on TCP/IP.

Once TCP/IP is installed, you may need to configure the following parameters to provide access to the Internet.

IP Address

If your network uses dynamic host configuration protocol (DHCP), you must determine if your DHCP server provides valid IP addresses and subnet masks for use outside your local network. If it does not, you must disable DHCP configuration and configure RAS with a static pool of valid IP addresses.

Default Gateway

You must specify the IP address of the router on your network with access to the Internet.

DNS

You can configure TCP/IP to use a Domain Name Service (DNS) server on your local network or you can use a DNS server on the Internet. A DNS server on your local network may provide faster name resolution for RAS clients.

HOSTS or LMHOSTS file

You can improve efficiency of connections to frequently accessed servers on the Internet by adding entries to both the RAS server and the RAS clients' HOST or LMHOSTS file. Windows NT consults these local files for name resolution before consulting a DNS server.

Dial-Up Networking (RAS)

Dial-Up Networking is the software that allows remote clients to use the RAS server as an Internet service provider. To install Dial-Up Networking, double-click the Dial-Up Networking option in My Computer. Follow the instructions on screen to complete RAS installation. See Installing Dial-Up Networking for detailed instructions on installing Dial-Up Networking.

You may need to configure the following parameters during RAS installation or after installation using the Network option in Control Panel. Remote clients must also configure individual RAS entries as described in Configuring Remote Access Entries for Internet Use.

Port Configuration

The port(s) you will use to provide Internet service must be configured for Receive Calls or Dial Out and Receive Calls. Since you will most likely be using Windows NT Server to provide simultaneous access to multiple remote clients, you will probably have multiple COM ports (on a multiport adapter) to configure. You can configure the settings on one port and use the **Clone** button in the **Remote Access Setup** dialog box to duplicate identical settings for all remaining ports.

RAS Network Configuration

The **TCP/IP** check box must be selected in the **Server Settings** group in the **Network Configuration** dialog box. You must also select an encryption setting that reflects the capabilities of your remote clients while meeting your security requirements. See help in the **Network Configuration** dialog box for a description of each encryption setting.

RAS TCP/IP Configuration

TCP/IP client must be able to access the entire network since the router to the Internet will be on your network. Note that this network may be isolated from your primary network for security reasons. If your TCP/IP network uses DHCP you must ensure the DHCP server provides IP addresses that are valid on the Internet. Otherwise you must provide a static address pool with IP addresses that are valid on the Internet. You can also allow remote clients to provide their own IP address. This is useful if the clients use applications over the RAS connection that expect the user at a specific address.

PPP and Remote Access

The Point-to-Point Protocol (PPP) is a set of standard protocols that allows remote access software from different vendors to interoperate. Windows NT Dial-Up Networking can dial into remote networks through any industry-standard PPP server. PPP also enables a computer running Windows NT Server RAS to receive calls from, and provide network access to, other vendors' remote access software that complies with the PPP standards.

The PPP standards also permit advanced features, not available with older standard (such as SLIP). PPP supports encrypted authentication and most PPP implementations will allow you to automate the entire logon sequence. Older standard often provide little security and require terminal mode logons.

PPP also supports multiple LAN protocols. With Dial-Up Networking you can use TCP/IP, IPX, or NetBEUI as the network protocol for both remote clients and the RAS server.

PPP is expected to become the primary standard for most remote access computing.

See Also

PPP Operation and Protocols

PPP RFCs Supported

Using PPP for Internet Connections

Using PPP for Internet Connections

PPP connections are the default for Windows NT.

Windows NT Dial-Up Networking requires no special configuration to support inbound PPP calls. If Dial-Up Networking is configured properly, PPP connections are automatically negotiated.

If you are using Windows NT to dial a remote PPP server the default settings are usually ideal, and no configuration is necessary. However, you can configure the LAN protocols you will use for each Dial-Up Networking entry that dials a PPP server.

To configure PPP for dial out connections

1. In Dial-Up Networking, select a phonebook entry and then click **More.**
2. Click **Edit entry and modem properties** or **Clone entry and modem properties**.
3. On the **Server** tab, select **PPP** as your server type.
4. In the **Network protocols** box, click **TCP/IP**.
5. To configure your TCP/IP settings, click **TCP/IP Settings.**
6. On the **Server** tab, clear the **Enable PPP LCP extensions** check box. This serves as a troubleshooting measure only if you experience consistent problems with PPP connections.
7. After you have selected the LAN protocols for PPP, click **OK**.

   The entry is ready to dial a PPP server.

PPP Operation and Protocols

PPP connections must adhere to standard established in PPP RFCs. This is an overview of how PPP operates and the protocols used in a PPP connection.

PPP Dial up Sequence

After initial connection to a remote PPP server, the following negotiations occur to establish a PPP connection:

- **Negotiate Link Control Protocols (LCP).** LCP is used to establish and configure link and framing parameters such as maximum frame size.
- **Negotiate Authentication Protocols.** Authentication protocols are used to determine what level security validation the remote access server can perform, and what the server requires. The level of security that can be negotiated ranges from clear text password authentication to encrypted authentication, to callback security.
- **Negotiate Network Control Protocols (NCP).** NCPs are used to establish and configure different network protocol parameters for IP, IPX and NetBEUI. This negotiation includes negotiating protocol header compression, and compression control protocol.

The resulting connection remains active until the line is disconnected for any of the following reasons: user explicitly hangs up the line, line drops due to idle timeout, administrator hangs up the line, or an unrecoverable link error occurs.

PPP Framing

PPP framing defines how data is encapsulated before transmission on the wide area network. The PPP standard framing format ensures any vendors' remote access software can communicate and recognize data packets from any remote access software that adheres to the PPP standards.

PPP uses HDLC framing for serial, ISDN and X.25. Windows NT uses HDLC framing for serial, ISDN and X.25 data transfer.

Network Control Protocols

Network control protocols establish and configure different network protocol parameters for IP, IPX, and NetBEUI.

Internet Protocol Control Protocol (IPCP)	IPCP is used for configuring, enabling, and disabling IP Protocol modules at both ends of the link.
Internet Packet Exchange Control Protocol (IPXCP)	IPXCP is used for configuring, enabling and disabling IPX protocol modules on both ends of the connection. IPXCP is widely implemented by PPP vendors. The IPX WAN protocol is Novell's alternative to IPXCP. IPX WAN is not compatible with IPXCP. Over time, IPX WAN and IPXCP may converge to provide one standard for IPX network configuration over wide area networks. Windows NT supports IPX CP, which is implemented by the vast majority of remote access software today. Windows NT does not support IPX WAN
NetBIOS Frames Control Protocol (NBF CP)	NBF CP is used for configuring, enabling and disabling NetBEUI protocol modules on both ends of the connection. NBF CP is a Microsoft-proposed protocol for NetBEUI configuration. NBF

	CP is in draft status with the Internet Engineering Task Force (IETF).

Authentication Protocols

Negotiation of authentication protocols occurs immediately after link quality determination and before network layer negotiation.

Password Authentication Protocol (PAP)	PAP uses clear text passwords and is the least sophisticated authentication protocol. It is typically negotiated if the remote workstation and server cannot negotiate a more secure form of validation. The Windows NT RAS server can be set to prevent clear text passwords, enabling a high level of security.
Challenge-Handshake Authentication Protocol (CHAP)	CHAP uses a challenge-response with an encrypted response. CHAP allows different types of encryption algorithms to be used. Microsoft RAS uses DES encryption when both the client and the server are using Windows NT RAS. The RAS client can also negotiate MD5 encryption when connecting to other vendors' remote access servers. The Windows NT RAS server only provides DES encryption and will not negotiate MD5 with other vendors' remote access client software. MD5 is an encryption scheme used by various PPP vendors for encrypted authentication. Windows NT will always negotiate encrypted authentication when communicating with other Windows NT computers. When connecting to 3rd party remote access servers or client software, RAS may negotiate clear text authentication if the 3rd party product does not support encrypted authentication.

PPP RFCs Supported

Remote Access protocol standards are defined in *Requests for Comments* (RFCs), which are published by the Internet Engineering Task Force and other working groups. The RFCs supported in this version of Windows NT RAS are:

- RFC 1549 PPP in HDLC Framing
- RFC 1552 The PPP Internetwork Packet Exchange Control Protocol (IPXCP)
- RFC 1334 PPP Authentication Protocols
- RFC 1332 The PPP Internet Protocol Control Protocol (IPCP)
- RFC 1661 Link Control Protocol (LCP)
- RFC 1717 PPP Multilink Protocol

Troubleshooting PPP Connections

Can't Connect to PPP Server

If you cannot connect to a server using PPP, or the remote computer terminates your connection, the server may not support LCP extensions. Try clearing the **Enable PPP LCP extensions** check box.

To stop requesting LCP extensions

1. Disconnect from the remote PPP server.
2. In Dial-Up Networking, click **More** and then click **Edit entry and modem properties**.
3. On the **Server** tab, clear the **Enable PPP LCP extensions** check box.
4. Click **OK**.

TCP/IP Utilities Do Not Work

If you successfully connect to a remote PPP server but TCP/IP utilities do not work, the problem may be IP header compression. Try to reconnect after turning off IP header compression.

To turn off IP header compression

1. Disconnect from the remote PPP server.
2. In Dial-Up Networking, click **More** and then click **Edit entry and modem properties**.
3. On the **Server** tab, click **TCP/IP Settings**.
4. In the **PPP TCP/IP Settings** dialog box, clear the **Use IP header compression** check box.
5. Click **OK**.

Using Other Device Command Files (.INF)

RAS uses Switch.inf, Modem.inf, and Pad.inf to automate interactive log ins with servers and to initialize modems and X.25 PADS. These files all use the same commands and syntax to communicate with devices or computers automatically.

The files contain examples and sequences of commands (scripts) for common or supported devices. If the device you will use is not listed in the file, you can create your own scripts in the files using the other scripts as an example and adding the correct commands for your specific device.

Since the syntax and common commands for all files is the same, these MODEM.INF help topics below apply to the other .INF files.

Overview of Modem Script File

Modifying MODEM.INF

Syntax for Modem.inf

The following files are in the *systemroot*\System32\RAS directory.

Modem.inf

Commands in this file are sent to your modem automatically. You need not modify this file unless your modem does not work and is not listed. See Overview of Modem Script File for more information.

Switch.inf

Commands in this file are used when connecting through a security host or a remote server that requires an interactive log in (for example, a UNIX server). You create a script by typing the name of the device within brackets then add one or more commands following the device name. After creating the script you activate the script in each Remote Access entry that will use the script. You can use the scripts before you dial (for example, modem pools) or after you dial (for example, security hosts or actual logon to a remote server). See Automating Remote Logons Using SWITCH.INF Scripts for more information.

Pad.inf

Commands in this file are used when connecting through an X.25 PAD. Most supported PADS have scripts provided in PAD.INF. If necessary, you create a script by typing the name of the device within brackets then add one or more commands following the device name. After creating the script you activate the script on the **Script** tab for each Remote Access entry that will use the script. For more information, see the *Networking Supplement.*

Using Windows NT to Connect to MSN

You can only use the Microsoft Network (MSN) as your Internet service provider if you have already created an MSN account using Windows 95.

When you connect to the Internet through Windows NT using MSN, proprietary online services such as mail or bulletin boards are not available.

To connect to MSN

1. In the **Dial-Up Networking** dialog box, click **New**.
2. Follow the instructions on the screen. Or, select the check box to edit the phonebook directly, click **Finish**, and continue with the following steps.
3. On the **Basic** tab, type a name for your entry (for example, **MSN**).
4. Enter the phone number for the local MSN service that allows Internet access.
5. Select a modem and use the default modem configurations.
6. On the **Server** tab, in the **Dial-Up Server Type** box, select **PPP**.

   In the **Protocols** box, select only the **TCP/IP** protocol.

   Clear the **Enable PPP LCP extensions** check box.
7. On the **Security** tab, click **Accept any authentication including clear text** and then click **OK**.
8. Click **Dial**.
9. In the **Authentication** dialog box, supply your MSN user name by typing **MSN/***username.*
10. Type your MSN password and click **OK**.

Connecting to Remote Servers

The three most common remote connections are to:

- Microsoft RAS Servers. (These include LAN Manager 2.1, Windows for Workgroups 3.11 with server extention, Windows NT 3.1 or later, and Windows 95)
- Non-Microsoft Point-to-Point Protocol (PPP) servers.
- Serial Line Internet Protocol (SLIP) Servers.

Connecting to a Microsoft RAS server is a simple process that uses the credentials you specified when you logged on to Windows NT. If you use Windows NT RAS to connect to computers that are not running Windows NT RAS, the remote computer may require a specific sequence of commands and responses through a terminal window to successfully log you on to the remote system.

Microsoft RAS Servers

Connecting to a Microsoft RAS server is a simple process that uses the credentials specified when you logged on to Windows NT. If you use Windows NT RAS to connect to computers that are not running Windows NT RAS, the remote computer might require a specific sequence of commands and responses through a terminal window to successfully log you on to the remote system.

If the client is a Windows NT computer and the remote server is any Microsoft RAS server, logon is completely automated using Windows NT security.

See Also

Connecting to Remote Servers

PPP Servers

SLIP Servers

PPP Servers

Point-to-point protocol (PPP) is a newer protocol used to negotiate connections between remote computers. Remote server and client software that supports PPP authentication protocols automatically negotiate network and authentication settings. The following steps are necessary to connect to a PPP server:

- In Dial-Up Networking, edit an entry and choose the **Server** tab. In the **Dial-up server type** box, select PPP. This is the default selection.
- If the server you are calling requires a text-based logon exchange, choose the **Script** tab and select the **Pop up a terminal window** option. Now, during the connect sequence, you will see a terminal dialog that allows you to perform the text-based logon exchange.

The PPP standard provides for fully automated authentication using encrypted or clear-text authentication protocols. Some PPP providers do not implement the PPP authentication protocols; instead they require a text-based exchange prior to starting PPP.

To automate the text-based exchange, use a SWITCH.INF script instead of the clear-text logon dialog. For more information, see the Automating Remote Logons Using SWITCH.INF Scripts, Activating SWITCH.INF Scripts, and Troubleshooting Scripts Using DEVICE.LOG topics.

See Also

Connecting to Remote Servers

Microsoft RAS Servers

SLIP Servers

SLIP Servers

Serial Line Internet Protocol (SLIP) is an older protocol that does not support authentation as part of the protocol. SLIP connections typically rely on text-based logon sessions. Encryption and automatic network parameter negotiations are not supported. The following steps are important when you are connecting to a SLIP server:

- In Dial-Up Networking, edit an entry and choose the **Server** tab. In the **Dial-up server type** box, select SLIP.
- If the server you are calling requires a text-based logon exchange, choose the **Script** tab and select the **Pop up a terminal window** option. Now, during the connect sequence, you will see a terminal dialog that allows you to perform the text-based logon exchange.

To automate the text-based exchange, use a SWITCH.INF script instead of the clear-text logon dialog. For more information, see the Automating Remote Logons Using SWITCH.INF Scripts, Activating SWITCH.INF Scripts, and Troubleshooting Scripts Using DEVICE.LOG topics.

See Also

Connecting to Remote Servers

Microsoft RAS Servers

PPP Servers

Using RAS Terminal for Remote Logons

For a PPP or SLIP server, if the remote computer you dial in to requires that you log on with a terminal screen, you must configure the Script settings for that RAS entry to use a *RAS Terminal logon*. With such a logon, after RAS connects to the remote system, a character-based window displays the logon sequence from the remote computer. You use this window to interact with the remote computer for logging on. Alternatively, you can automate this manual logon as described in the section, Automating Remote Logons Using SWITCH.INF Scripts,.

Some commercial networks will present a large menu of available services before you log on. On old, established SLIP servers, you might go through an extensive sequence of commands that updates files, collects data about you, or configures your SLIP connection during your logon process. On a new PPP server, you might be prompted for only your username and password before you are given a connection.

Note: If the remote computer is a Microsoft RAS server, you do not need to use a terminal logon. Instead, logon is completely automated for you.

To configure a Windows NT RAS entry to use RAS Terminal after dialing

1 In Dial-Up Networking, select the entry to which you want to connect.

2 Click **More** and choose **Edit entry and modem settings**.

3 In the **Script** tab, choose the **Pop up a terminal window** option.

4 Click **OK** and then click **Dial**.

After you dial and connect to this entry, the After Dial Terminal window appears, and you will see prompts from the remote computer. You then log on to the remote computer using the After Dial Terminal window. After you have completed all interactions with the remote computer, click **Done.**

If the logon sequence does not vary, you can write a script that automatically passes information to the remote computer during the logon sequence, enabling completely automatic connections.

For more information, see the Automating Remote Logons Using SWITCH.INF Scripts, Activating SWITCH.INF Scripts, and Troubleshooting Scripts Using DEVICE.LOG topics.

Automating Remote Logons Using SWITCH.INF Scripts

To automate the logon process, you can use the SWITCH.INF file (or PAD.INF on X.25 networks) instead of the manual RAS Terminal window described in the Using RAS Terminal for Remote Logons topic.

Automated scripts are especially useful when a constant connection to a remote computer is needed: If the RAS entry is configured to use a script, and if a remote connection fails, RAS automatically redials the number and reestablishes the connection. Scripts also save time if you frequently log on to a remote system and do not want to manually log on each time.

The SWITCH.INF file provides a generic script that will probably work with little or no modification try it first If that does not work, then copy and modify the generic script to match the logon sequence of the remote computer you want to connect to.

Note: The script language described in this chapter was also designed to communicate with other devices, including modems. If you are unfamiliar with modem scripts, scripting can be difficult to understand. The following section explains how to create scripts, although you will probably find it easiest to copy, then modify, one of the generic sample scripts.

See Also

Creating Scripts for RAS

Activating SWITCH.INF Scripts

Troubleshooting Scripts Using DEVICE.LOG

Creating Scripts for RAS

The SWITCH.INF file, located in the *systemroot*\SYSTEM32\RAS folder, is like a set of small batch files (scripts) contained in one file. The SWITCH.INF file contains a different script for each intermediary device or online service that the RAS user will call.

A SWITCH.INF script has six elements: a section header, comment lines, commands, responses, response keywords, and macros.

See Also

Activating SWITCH.INF Scripts

Troubleshooting Scripts Using DEVICE.LOG

Stepping Through an Example Script

Getting Through Large Blocks of Text and Two-Second Gaps

Commands and Carriage Returns

Section Headers

Section headers divide the SWITCH.INF file into individual scripts. A section header marks the beginning of a script for a certain remote computer and must not exceed 31 characters. The text of a section header will appear in RAS when you activate the script. The section header is enclosed in square brackets. For example:

```
[Route 66 Logon]
```

See Also

Creating Scripts for RAS

Comment Lines

Comment lines must have a semicolon (;) in column one and can appear anywhere in the file. Comment lines contain information for those who maintain the SWITCH.INF file. For example:

```
; This script was created by MariaG on September 29, 1996
```

See Also

Creating Scripts for RAS

Commands

Each line in a script is a command from your local computer to the remote computer or a response from the remote computer to your local computer. Each command or response is a stream of data or text. For example, the following command sends a username (MariaG) and a carriage return (the macro **<cr>**) to the remote computer.

COMMAND=MariaG<cr>

The commands and responses must be in the exact order the remote device expects them. Branching statements, such as GOTO or IF, are not supported.

The required sequence of commands and responses for a specific remote device should be in the documentation for the device or, if you are connecting to a commercial service, from the support staff of that service. If the exact sequence is not available, activate the generic script provided with RAS and modify it to match the logon sequence of the remote computer as described in the Troubleshooting Scripts Using DEVICE.LOG topic.

The COMMAND= statement can be used in two additional ways:

```
COMMAND=

NoResponse
```

This is the default behavior and causes an approximate two-second delay. This can be useful when the intermediate device requires a delay.

```
COMMAND= string
```

Note: *string* is not followed by a carriage return (<**cr**>). This is useful when a device requires slow input. Instead of receiving the whole command string, the device requires characters to be sent one-by-one.

The following is an example in which the intermediary device is so slow that it is able to receive and process only one character of the command PPP at a time:

```
COMMAND=P

NoResponse


COMMAND=P

NoResponse


COMMAND=P

NoResponse
```

See Also

Creating Scripts for RAS

Response

A response is sent from the remote device or computer. To write an automatic script, you must know the responses you will receive from the remote device. If a gap of two or more seconds occurs between characters, the received text is sent as a response. This gap is the only cue that a response is over. For more information, see the topic Getting Through Large Blocks of Text and Two-Second Gaps..

See Also

Creating Scripts for RAS

Response Keywords

The keyword in a response line specifies what to do with the responses you receive from the remote computer:

OK=*remote computer response<macro>*
The script continues to the next line if the response or macro is encountered.

LOOP=*remote computer response<macro>*
The script returns to the previous line if the response or macro is encountered.

CONNECT=*remote computer response <macro>*
Used at the end of a successful modem script. Not generally useful for the SWITCH.INF file.

ERROR= *remote computer response <macro>*
Causes RAS to display a generic error message if the response is encountered. Useful for notifying the RAS user when the remote computer reports a specific error.

ERROR_DIAGNOSTICS= *remote computer response* <**diagnostics**>
Causes RAS to display the specific cause for an error returned by the device. Not all devices report specific errors. Use **ERROR=** if your device does not return specific errors that can be identified with Microsoft RAS diagnostics.

NoResponse
Used when no response will come from the remote device.

RAS on the local computer always expects a response from the remote device and will wait until a response is received unless a **NoResponse** statement follows the **COMMAND=** line. If there is no statement for a response following a **COMMAND=** line, the **COMMAND=** line will execute and stop the script at that point.

See Also

Creating Scripts for RAS

Macros

Macros are enclosed in angle brackets (<>) and perform a variety of special functions:

<cr>
Inserts a carriage return.

<lf>
Inserts a line feed.

<match> “*string*”
Reports a match if the string enclosed in quotation marks is found in the device response. Each character in the string is matched according to upper and lower case. For example, <match> “Smith” matches Jane Smith and John Smith III, but not SMITH.

<?>
Inserts a wildcard character, for example, CO<?><?>2 matches COOL2 or COAT2, but not COOL3.

<hXX> (XX are hexadecimal digits)
Allows any hexadecimal character to appear in a string—including the zero byte, <h00>.

<ignore>
Ignores the rest of a response from the macro on.

<diagnostics>
Passes specific error information from a device to RAS. This enables RAS to display the specific error to RAS users. Otherwise, a nonspecific error message appears.

See Also

Authentication Macros

Creating Scripts for RAS

Authentication Macros

The following macros enable your username and password logon credentials to be automatically passed to the remote computer.

<username>

The username entered in the RAS Authentication window is sent to the remote computer. This is not supported with SLIP connections.

<password>

The password entered in the RAS Authentication window is sent to the remote computer. This is not supported with SLIP connections.

Your logon credentials will fail (and the Retry Authentication dialog box will appear) if both of the following occur:

- You call into a system that has an intermediary security device. (This situation would generally not apply if you are using RAS to call an Internet provider.)
- After the security device has logged you on successfully, you try to log on to a Windows NT RAS server.

The dialog box appears because the RAS Authentication dialog box username and password boxes are used by the two new username and password macros as well as by Windows NT RAS servers.

For example, if the logon information for an intermediary security device that is plugged in between the Windows NT RAS server and its modem is username: "BB318" and password: "34554377", but on the Windows NT RAS server it is username: "BB318" and password: "treehouse", then your logon to the intermediary device will succeed, but your logon to the Windows NT RAS server will fail.

Logon will fail because the security device password of "34554377" is different from the Windows NT domain password. Windows NT will prompt you with the Retry Authentication dialog box to obtain your proper Windows NT logon credentials, in this case the password.

To eliminate the Retry Authentication dialog box

- Ask your administrator to make your username and password identical on both systems. (Because this solution defeats the purpose of the security device, it is not recommended.)
- Do not use the shared dialog box for the intermediary device logon credentials: Enter the username and password in clear text into the SWITCH.INF file according to the [Generic login for YourLoginHere] script provided in SWITCH.INF. To keep your clear-text password confidential you must use Windows NT file system (NTFS) file permissions to prevent other users from accessing this file.

Stepping Through an Example Script

This topic describes each part of the generic script provided in the SWITCH.INF file included with RAS.

Every script must start with a command to the remote computer, followed by one or more response lines. This initial command might be simply to wait for the remote computer to initialize and send its logon banner. The default initial command is to wait two seconds for the logon banner. It would look like this in the SWITCH.INF file:

COMMAND=

If the response, (the logon banner from the remote computer) is the following:

```
Welcome to Gibraltar Net. Please enter your login:
```

then the corresponding response line in the SWITCH.INF file should be:

OK=<match>“Please enter your login:”

This line indicates that everything is correct if the remote computer sends the string “Please enter your login:”. You respond by sending a command with the characters in your username and the carriage return.

COMMAND=MariaG<cr>

If the response from the remote computer is the following:

```
Please enter your password:
```

then the corresponding response line in the SWITCH.INF file should be:

OK=<match>“Please enter your password:”

To send your password, you would send the command:

COMMAND=mUs3naB<cr>

On many PPP computers, this script would automatically log you on.

See Also

Automating Log On to SLIP Computers

Creating Scripts for RAS

Automating Log On to SLIP Computers

If your SLIP provider assigns you the same IP address every time you call, you can fully automate your SLIP connection by entering that address in the **SLIP TCP/IP Settings** dialog box.

If you are assigned a different IP address every time you call, then even though you can automate much of the logon sequence, you must manually enter your IP address in the SLIP terminal window.

Getting Through Large Blocks of Text and Two-Second Gaps

If the remote computer has a two-second gap in the data stream response to your computer, RAS assumes that the gap is the end of the response. These gaps can occur anywhere—even between words—and can only be detected using DEVICE.LOG. For more information, see the Troubleshooting Scripts Using DEVICE.LOG topic.

If you write a script that seems to fail for no reason, consult DEVICE.LOG to see if a response ends in the middle of a word. If it does, your script must account for the two- second gap. A simple way to do this is to include the following command:

COMMAND=<cr>

You can skip to the end of large blocks of text that contain multiple gaps by using the **LOOP=** keyword and by matching text at the end of a block. For example,

COMMAND=<cr>
OK=<match>"Enter the service to start:"
LOOP=<ignore>

In this example, RAS sends a null command (waits two seconds). RAS then waits for the message "Enter the service to start:". If this is a long block of text, RAS does not find the string, so RAS then moves to the **LOOP** command. The **LOOP** command causes RAS to return to the line above, and RAS waits for the words "Enter the service to start:" in the second response. In this manner, you can loop though long blocks of text until you reach the text of the desired prompt.

See Also

Creating Scripts for RAS

Commands and Carriage Returns

Usually, you must include **<cr>,** which indicates a carriage return, at the end of a command. The carriage return causes the remote computer to process the command immediately. If you do not include **<cr>**, the remote computer might not recognize the command.

In other situations, **<cr>** cannot be used because the remote computer accepts the command without a carriage return and requires time to process the command. This situation mainly applies when you are sending a series of commands without expecting a response.

See Also

Creating Scripts for RAS

Activating SWITCH.INF Scripts

After you have created a script in SWITCH.INF, you can configure a RAS entry to execute the script.

To activate a script in Windows NT

1 In Dial-Up Networking, select the entry to which you want to connect.
2 Click **More** and choose **Edit entry and modem settings**.
3 In the **Script** tab, select the **Run this script** option and select the name of the script. The section header in SWITCH.INF appears as the name of the script.

   You can also edit your script by clicking **Edit scripts**.
4 Click **OK** and then click **Dial**.

When you dial this entry, the selected script will execute and complete all communication with the remote device before or after RAS dials the remote host.

See Also

Creating Scripts for RAS

Troubleshooting Scripts Using DEVICE.LOG

Troubleshooting Scripts Using DEVICE.LOG

Windows NT enables you to log all information passed between RAS, the modem, and the remote device, including errors reported by the remote device. This allows you to find errors that prevent your scripts from working.

The DEVICE.LOG file is created by enabling logging in the registry. After you enable logging, the DEVICE.LOG file is in the *systemroot*\SYSTEM32\RAS folder.

To create the DEVICE.LOG file

1 Hang up any connections, and then exit from Dial-Up Networking.

2 Start the Registry Editor by running the REGEDT32.EXE program.

3 Go to HKEY_LOCAL_MACHINE, and then access the following key:

```
\SYSTEM\CurrentControlSet\Services\RasMan\Parameters
```

4 Change the value of the Logging parameter to 1. When changed, the parameter should look like this:

```
Logging:REG_DWORD:0x1
```

5 Close the Registry Editor.

Logging begins when you restart Remote Access or start the Remote Access Server service (if your computer is receiving calls). You do not need to shutdown and restart Windows NT.

After you dial a number and connect, a script will start. If an error is encountered during script execution, execution halts. You should exit RAS, and then determine the problem by using any text editor to view DEVICE.LOG. The following topic is an example of an incomplete script that failed when a connection was attempted and the DEVICE.LOG file that was created.

Note: The traces from all calls will be appended to DEVICE.LOG as long as RAS or the Remote Access Server service are not stopped and restarted. So, if you need to save a DEVICE.LOG file with useful information for later review or troubleshooting, make a copy of the file, giving the file another name before you restart RAS or the Remote Access Server service.

See Also

Example of an Incomplete SWITCH.INF Script

Sample DEVICE.LOG

Creating Scripts for RAS

Activating SWITCH.INF Scripts

Example of an Incomplete SWITCH.INF Script

The following script is incomplete for the service to which the user tried to connect. This script was used with DEVICE.LOG to discover that the remote computer expected additional commands from the script. See the sample DEVICE.LOG for the complete output that was generated.

```
[Gibraltar Net Login for MariaG]
; FIRST COMMAND TO INITIALIZE REMOTE COMPUTER
COMMAND=

; Skip to login prompt. That is, loop through blocks of text
; separated by 2-second gaps until the login prompt is encountered.
OK=<match>"Login:"
LOOP=<ignore>

; Provide username to remote computer
COMMAND=MariaG<cr>

; Since no 2-second gap is present, immediately match "Password:"
OK=<match>"Password:"

; Provide password to remote computer
COMMAND=mUs3naB
```

See Also

Sample DEVICE.LOG

Sample DEVICE.LOG

This is the DEVICE.LOG file created by using the sample generic script. Note that DEVICE.LOG comment lines in all uppercase letters are writer comments added after the file was created to help you understand the contents of the file.

```
Remote Access Service Device Log  08/23/1996  13:52:21
---------------------------------------------------------------
; THIS SECTION IS THE COMMUNICATION BETWEEN RAS AND THE MODEM
Port:COM1 Command to Device:AT&F&C1&D2 W2\G0\J0\V1 S0=0 S2=128 S7=55

Port:COM1 Echo from Device :AT&F&C1&D2 W2\G0\J0\V1 S0=0 S2=128 S7=55

Port:COM1 Response from Device:
OK
Port:COM1 Command to Device:AT\Q3\N7%C0M1

Port:COM1 Echo from Device :AT\Q3\N7%C0M1

Port:COM1 Response from Device:
OK



; COMMAND TO DIAL REMOTE COMPUTER AND SUCCESSFUL CONNECTION

Port:COM1 Command to Device:ATDT1 206 555 5500

Port:COM1 Echo from Device :ATDT1 206 555 5500

Port:COM1 Response from Device:
CONNECT 14400/REL
Port:COM1 Connect BPS:19200
Port:COM1 Carrier BPS:14400


; INITIAL NULL COMMAND SENT TO DEVICE

Port:COM1 Command to Device:
Port:COM1 Response from Device:
_[2J_[H
Welcome to Gibraltar Net, a service of: Trey Computing,  Inc.

Problems logging in?  Call us at 555-5500 between 8:00am and 8:00pm Mon-Sat.

NOTE: Your software must support VT100 (or higher) terminal emulation!

Port:COM1 Response from Device:P


; THE LINE ABOVE INDICATES A TWO-SECOND GAP IN THE MIDDLE
; OF THE WORD "PLEASE" IF YOUR SCRIPT FAILED AND DEVICE.LOG ENDED
; AFTER THE RESPONSE ABOVE, YOU WOULD ACCOUNT FOR THIS
; TWO-SECOND GAP IN YOUR SCRIPT BY USING A NULL COMMAND= LINE OR THE
; OK=response AND LOOP=<match> COMBINATION.

Port:COM1 Response from Device:lease turn OFF your Caps Lock if it is on now.

Please enter your login name and password at the prompts below.
  - Log in as "guest" to take a look around the system.
  - Log in as "new" to create an account for yourself.

Login:
```

```
; SEND YOUR USERNAME AS A COMMAND
Port:COM1 Command to Device:MariaG
Port:COM1 Echo from Device :MariaG
Port:COM1 Response from Device:
Password:

; SEND YOUR PASSWORD AS A COMMAND
Port:COM1 Command to Device: mUs3naB
Port:COM1 Echo from Device : mUs3naB

; THE LOGIN SEQUENCE CONTINUES ON THE REMOTE COMPUTER
; BUT THE SCRIPT DOES NOT CONTINUE FROM HERE.
; THE AUTOMATED LOG IN WOULD FAIL AT THIS POINT.
Port:COM1 Response from Device:
```

This script would be complete for many remote computers, but the remote computer sent more responses and expected a command to start a service. To complete the script you must know the remainder of the responses from the remote computer. If you logged on manually using RAS Terminal and found the remainder of the logon sequence looked like this:

```
Gibraltar Net offers you several network services:

Service
------------------------------------------------------------------------
SHell
UPload
DOwnload
PAssword
PPP
SLIP

Please enter a service:
```

you would complete the script with these lines:

COMMAND=<cr>
OK=<match>“Please enter a service:”
LOOP=<ignore>

If you added the lines above to your script, restarted RAS and redialed, you would successfully connect.

If the generic script in RAS does not work, these guidelines should help you modify the generic script to work for your connections. First copy the generic script to the end of SWITCH.INF, then modify the copy to work with your connections.

See Also

Example of an Incomplete SWITCH.INF Script

Using Scripts with Other Microsoft RAS Clients

Microsoft RAS version 1.0 (which runs on LAN Manager) cannot invoke RAS Terminal or use scripts in .INF files.

Microsoft RAS version 1.1a (which runs on LAN Manager) supports PAD.INF only. Note that the syntax used in the PAD.INF file differs slightly from subsequent versions of Microsoft RAS.

Microsoft RAS for Windows for Workgroups version 3.11 and Windows NT version 3.1 or later support RAS Terminal and scripts in SWITCH.INF and PAD.INF.

Overview of Modems

This section contains information on unsupported modems and modifying your modem script file, Modem.inf, which stores information describing each modem type supported by the Remote Access Service. Do not modify this file except for the following reasons:

- To add sections for modems that are not already supported.
- To enhance existing entries, such as increasing the maximum modem speed to 57600 bits per second (bps).

For information about modifying Modem.inf for an unsupported modem, see Overview of Modem Script File.

For recommendations about getting the most out of compression, see Compression Recommendations.

Overview of Modem Setup

Dial-Up Networking supports many features that can take full advantage of your modem:

- Hardware flow control
- Modem error control
- Modem compression
- Ability to enter modem commands manually
- High speeds such as 14,400, 19,200, 28,800, 38,400, and in some cases even 57,600 bps

If possible, choose a supported modem from the Windows NT Hardware Compatibility List. Microsoft has tested these modems with the remote access software.

Note: To ensure compatibility, use the same kind of modem as the one connected to the remote access server, select the same initial speed, and enable the same features. If you don't choose the same model, at least choose a modem with the same CCITT standard as the server's modem.

For information about dialing in through an unsupported modem, see Overview of Modem Script File.

To change your modem or install a new one

1 Double-click the Network option in Control Panel.

2 On the **Services** tab, click **Remote Access Service** and then click **Properties**.

3 Click the **Help** button for more information.

See Also

Testing Your Modem

Setting Modem Features

Hardware Flow Control

Enables hardware handshaking. This feature allows the modem to tell Remote Access software when the line is congested or clear, so that the Remote Access software can temporarily stop transmitting data when necessary. This handshaking streamlines data transmission, prevents overrun errors, and thus improves overall data throughput.

Modem Error Control

Checks errors on blocks of data through cyclic redundancy checks (CRCs). Modem error control causes the modem to retransmit garbled data, ensuring that only error-free data passes through the modem. For more information, see MNP4 and V.42.

Modem Compression

Compresses the modem-to-modem data stream, reducing the number of bytes transmitted and therefore reducing the transmission time. The reduction achieved depends on the amount of redundancy in the transmitted data.

Note: Software compression is more effective than hardware compression because a much larger pattern buffer is available on the computer than on the modem. In addition, modem compression delays the first transmission while the modem's pattern buffer is filled at computer-to-modem speed. Software compression accomplishes this task at the much faster memory speed and transmits compressed data over the entire computer-to-computer link rather than just the modem-to-modem segment.

In general, you should not enable modem compression and software compression at the same time, because no benefit is gained from compressing precompressed data. In fact, it may actually increase the size of the transmitted data, depending on the algorithm used by the modem.

Enter modem commands manually

Lets you enter AT commands to the modem manually when dialing rather than executing the scripted commands. Enable this feature when testing modem strings for new entries in the modem script file (Modem.inf) and for unusual situations where interaction is required midway in the dial sequence.

In general, do not enable this feature when dialing with the telephone keypad, for example, when connecting through a switch controlled by a human operator.

Setting Modem Features

To set modem features

1. In **Dial-Up Networking**, select a phonebook entry, and then click **More.**
2. Click **Edit entry and modem properties** or **Clone entry and modem properties**.
3. On the **Basic** tab, select a modem in the **Dial using** box and then click **Configure**.
4. In the **Modem Configuration** dialog box, set the speed of the modem and select hardware features such as modem compression.

Note: Selecting a feature that is not supported by your modem has no effect on its performance.

To change your modem or install a new modem

- Double-click the Network option in Control Panel. On the **Services** tab, select **Remote Access Service** and then click **Properties**. Click the **Help** button in the dialog boxes for more information.

Compression Recommendations

Modem Compression

When modem compression is enabled, set the port speed to 38400 bps or 57600 bps. You must have a 16550 serial port or better and a 386/33 or faster processor, which can handle a high interrupt rate without generating overrun errors. Note that since throughput ultimately depends on the data compression ratio, running at a port speed of 57600 bps does not necessarily mean that throughput will approach 57600 bps.

For example, suppose you have a V.32bis modem with a modem-to-modem speed of 14400 bps. You are connecting with modem compression enabled and the port speed set to 57600 bps. But the transferred data is being compressed at a ratio of 2:1, which means your average throughput is actually 28800 bps. You can approach 57600 bps only if transferring highly compressible data (such as a file consisting of zeros or a black bitmap), which is unlikely.

In Modem.inf, maximum speed has been set to 38400 bps because typical hardware cannot handle higher port speeds without risking overruns. Customers who have the appropriate hardware can try to run at 57600 bps, but it will not necessarily result in higher throughput, as explained in the previous paragraph. Also, Microsoft has not tested any modems at 57600 bps.

Software Compression

The Remote Access Service also offers software data compression, so you won't have to turn on modem compression to benefit from a faster throughput. If you have a V.32bis modem, you can run at 14400 bps, enable software compression, and experience an average throughput of 28800 bps. Tests show that software compression results in better throughput than modem compression. Software compression also lowers the interrupt rate and diminishes the risk of overruns.

For best results, enable modem error control, turn off modem compression, and enable software compression.

Understanding Industry Standards

Most manufacturers use CCITT standards because all modems signal one another at different speeds. Some of these standards, primarily modulation, include some of the higher layers (such as negotiation) as well. Multispeed modems may use several of these standards, which include:

V.21

V.22

V.22bis

V.23

V.29

V.32

V.32bis

MNP4

MNP5

V.42

V.42bis

Be sure to choose modems that conform to industry standards, as shown in the following table:

Speed in bps	Standard
1200	V.22 or Bell 212A
2400	V.22bis
9600	V.32
14,400	V.32bis

Error Control and Data Compression

For any error correction or data compression protocol to work, modems on both ends of the connection must support it. Once two modems are connected, they automatically negotiate to determine the best mutual protocols.

Protocols

MNP4

MNP5

International Standards

V.42

V.42bis

Turning On Your Device.log

The Device.log file tracks information recorded about your modem. If you have any modem problems that you can't troubleshoot by following the instructions under Modem Idiosyncrasies, this file will help you or your system administrator troubleshoot the problem.

The Device.log file is in the \System32\RAS subdirectory of your Windows NT directory.

To create Device.log

1 Copy the contents of this procedure to the Clipboard so that you can refer to it after you've exited from RAS.

2 Hang up any connections, and exit from RAS.

3 Open the Registry by running Regedt32.

4 Go to HKEY_LOCAL_MACHINE, and access the following key:

```
\System\CurrentControlSet\Services\RasMan\Parameters
```

5 Change the value of the Logging parameter to 1. When changed, the parameter should look like this:

Logging:REG_DWORD:0x1

Note: Logging begins when you restart RAS or start the Remote Access Server service (if your computer is receiving calls). You do not need to shutdown and restart Windows NT.

Modem Idiosyncrasies

This section describes idiosyncrasies of modems supported by the Remote Access Service. For a list of supported modems, see the Windows NT Hardware Compatibility List (HCL).

To troubleshoot a supported modem

1 Make sure your cabling is correct. See Cabling Requirements.

2 If your cabling satisfies the requirements of the Remote Access Service, but you still cannot connect, check the modem's documentation to make sure you have correctly installed the modem.

3 If the modem has been installed correctly, use a terminal emulator program (such as Windows NT HyperTerminal) to see if you can issue commands to the modem. See Testing Your Modem.

4 If the modem still does not work with the Remote Access Service, contact your system administrator.

Note: If you have any modem problems, please report them to your system administrator. In your report, include the output of your Device.log file, which is located in the \System32\RAS subdirectory of your Windows NT directory. For information about creating a Device.log file, see Turning On Your Device.log

See Also

General Idiosyncrasies

Codex 326x Series Idiosyncrasies

DataRace Idiosyncrasies

Datatrek Idiosyncrasies

Hayes Idiosyncrasies

MicroCom Idiosyncrasies

MicroGate Idiosyncrasies

MultiTech Idiosyncrasies

Octocom Idiosyncrasies

PDI Idiosyncrasies

Practical Peripherals Idiosyncrasies

Racal-Milgo Idiosyncrasies

Supra Idiosyncrasies

Telebit Idiosyncrasies

UDS Motorola Idiosyncrasies

US Robotics Idiosyncrasies

VenTel Idiosyncrasies

Western Datacom Idiosyncrasies

General Idiosyncrasies

Modems that Remote Access supports do not necessarily work in all modes with other modems on the Windows NT Hardware Compatibility List (HCL).

Example

Some V.32bis modems do not work with port speeds of 14,400 bps although they communicate at a modem-to-modem speed of 14,400 bps. If your V.32bis modem does not work at an initial speed of 14,400 bps, change the speed to 19,200 bps. For information about changing initial modem speed, see Setting Modem Features.

Internal Modems

The Windows NT system cannot automatically detect certain internal modems, such as the Digicom Scout Plus. You must add the modem manually through the Windows NT Control Panel. You may also need to add a communications port for the modem to use, if one is not already available. You must add the port before you add the modem. Click here  to open **Ports**. Click here
 to open **Install New Modem**.

Callback

Modems supported as server modems may not support callback when used as client modems.

Manual Dialing

These modems have following idiosyncrasies with manual dialing.

Modem	Idiosyncrasy
Bocamodem M1440	Fails modem protocol negotiation.
Gateway 2000 Telepath Internal	Always disconnected by the server after negotiation.
Intel SatisFaxtion 100	Fails authenticatation.
PDI-1000	Doesn't support manual dialing.
Racal-Milgo 2412	Handset should never be replaced, even after connection.
Ven-Tel 9600 Plus II	Fails authenticatation.

Codex 326x Series Idiosyncrasies

If you are connecting through a Codex 3260, 3261, 3262, 3263, 3264, or 3265, turn off flow control under the following circumstances:

- If you're connecting at 2400 or 9600 bps.
- If the modem negotiates down to 9600 or 2400 bps from an initial speed of 19,200 or 38,400 bps.

If you are connecting with a Codex V.FAST (3260, 3261, 3262, 3263, 3264, or 3265) modem to a Remote Access server that also has a Codex V.FAST modem, make sure that hardware flow control is enabled. Otherwise, you will not connect, and the following message "The device has switched to an unsupported baud rate" appears.

DataRace Idiosyncrasies

RediModem V.32bis

Error control and flow control are forced on.

Datatrek Idiosyncrasies

Elite 624D

Advanced features are disabled.

Datatrek V.32

Supported as a client modem only.

Hayes Idiosyncrasies

V-Series 9600

The Hayes V-Series 9600 modem connects at 9600 bps only with another Hayes V-Series 9600 modem.

Before you install this modem on your computer, make sure that the Remote Access server also has a Hayes V-Series 9600 modem. Otherwise, connections will probably be made at 2400 bps.

Hayes Optima 14.4

If a US Robotics Sportster modem initiates a connection to a Hayes Optima 14.4, the two modems are not able to negotiate a connection. If a Hayes Optima 14.4 initiates a connection to a US Robotics Sportster 14.4 modem, the connection is successful.

MicroCom Idiosyncrasies

QX 4232bis

Advanced features are disabled.

Microgate Idiosyncrasies

MicroGate MG96

Error control and flow control is forced on.

MicroGate MG144

Error control and flow control is forced on.

MultiTech Idiosyncrasies

MultiModem 224

Flow control is forced on.

Octocom Idiosyncrasies

8324

Error control and flow control are forced on.

PDI Idiosyncrasies

PDI-1000

The PDI 1000 is supported as a client modem only.

PDI-1000/S Intelligent Data Adapter

The PDI-1000/S is a digital device that connects to a dial-out modem or modem pool through an IBX digital phone line. Although not a modem, a PDI performs like one when connected to a modem pool.

Note: If you're experiencing trouble connecting to the RAS server through a PDI-1000/S, do the following:

- Make sure your IBX provider configures the system to expect a PDI at a certain number. If the IBX is not configured for a PDI on that line, it will drop the line during a call. Dial-in and dial-out lines must be configured independently.
- In the **Modem Settings** dialog box, set the Initial speed (bps) field to correspond to the speed of the server's modem. To reset this field, see Setting Modem Features. If you don't know the speed of the server's modem, ask your system administrator.

Practical Peripherals Idiosyncrasies

Practical Peripherals 2400SA

Supported as a client modem only.

Practical Peripherals 2400MNP

Advanced features are disabled.

Racal-Milgo Idiosyncrasies

2412/2

Maximum DTE speed set to 2400

Supra Idiosyncrasies

Supra COM Card PCMCIA 144

Supported as a client modem only.

Telebit Idiosyncrasies

Telebit T1500

Supported as a client modem only.

Telebit T1600

Advanced features are disabled.

UDS Motorola Idiosyncrasies

UDS Motorola V.3225

Advanced features are disabled.

UDS Motorola V.3227

Maximum DTE speed is set to 9600.

UDS Motorola FasTalk V.32/42bis

Maximum DTE speed is 9600.

US Robotics Idiosyncrasies

HST

US Robotics HST modems use a proprietary protocol that cannot negotiate connection speeds greater than 2400 bps with modems that do not support this protocol.

Even if you have HST-compatible modems on both the remote client and server, Microsoft does not recommend connecting at 14,400 bps with these modems. The HST protocol is not a full-duplex 14,400 bps protocol. In other words, data transmitted in one direction travels at 14,400 bps while data traveling in the opposite direction travels at a much slower rate. This results a low throughput since the Remote Access Service depends on the same speed for transferring data in both directions.

All 14400bps modems

All US Robotics 14400bps modems must be set to 19200, not 14400 as the initial speed. This applies to the US Robotics Sportster modem, which is installed on some Gateway 2000 computers.

If a US Robotics Sportster modem initiates a connection to a Hayes Optima 14.4, the two modems are not able to negotiate a connection. If a Hayes Optima 14.4 initiates a connection to a US Robotics Sportster 14.4 modem, the connection is successful.

VenTel Idiosyncrasies

VenTel 14400

Because the VenTel 14400 fax modem does not detect when a client hangs up, it will tie up a line until the timeout period has expired. Therefore, you should not use this modem as a server modem unless you don't mind having the lines tied up for extended periods of time.

This modem works fine as a client.

Ven-Tel 9600 Plus II

Modem compression is forced on.

Western Datacom Idiosyncrasies

Worldcom V32bis

Supported as a client modem only.

Cabling Requirements

The Remote Access Service has more stringent cabling requirements than terminal communications programs. If your serial cable works with the Windows NT HyperTerminal program but not with RAS, please make sure that your cable provides all the signals listed in the following table.

The Remote Access Service requires the following pins on the RS-232 cable:

Rx	Receive
Tx	Transmit
CTS	Clear To Send
RTS	Ready To Send
DTR	Data Terminal Ready
DSR	Data Set Ready
DCD	Data Carrier Detected

Caution

All the pins listed above must be present. The Remote Access Service does not work if any of the seven pins is missing. If any is not present or not working, the Remote Access Service reports a hardware error.

Most ISA and EISA computers have one of the following serial port connectors:

- 25-pin male "D-shell" connectors
- 9-pin male connectors

Most off-the-shelf cables will work with your modems, but not all. Some cables do not have all the pins connected as shown in the tables under 25-Pin Cabling, 9-Pin Cabling, and NULL Modem Cabling. When buying cables, tell your dealer exactly what you need and give him the information in these tables to be sure you have the correct match.

Note: Do not use the 9-to-25-pin converters that come with most mouse hardware, because some of them do not carry modem signals.

See Also

25-Pin Cabling

9-Pin Cabling

NULL Modem Cabling

25-Pin Cabling

As the following table shows, pins 1 through 8 on the serial port connector are wired to their counterparts on the modem connector. Ribbon cables usually have all 25 pins wired straight across, but they can cause interference with TVs, radios, and VCRs. Shielded RS-232 cable normally corrects this problem.

25-pin serial port connector	25-pin modem connector	Signal
1	1	Chassis Ground
2	2	Transmit Data
3	3	Receive Data
4	4	Request to Send
5	5	Clear to Send
6	6	Data Set Ready
7	7	Signal Ground
8	8	Carrier Detect
20	20	Data Terminal Ready

9-Pin Cabling

The following table shows how to connect a 9-pin serial port connector on a computer to a 25-pin connector on a modem. Again, if you buy an off-the-shelf cable, be sure all pins are connected, as shown in the following table.

Note that some modems have the Data Set Ready (DSR) signal physically tied to the Data Carrier Detect (DCD) signal. Some 1200-bps modems and other 2400-bps modems have dip switches default to this setting as well. As a result, if such a modem loses power while listening for a call, the Remote Access server cannot detect the condition because the DSR will not change, as it does with other modems.

9-pin serial port connector	25-pin modem connector	Signal
1	8	Carrier Detect
2	3	Receive Data
3	2	Transmit Data
4	20	Data Terminal Ready
5	7	Signal Ground
6	6	Data Set Ready
7	4	Request to Send
8	5	Clear to Send
9	22	Ring Indicator (optional)

NULL Modem Cabling

If you are using a NULL modem to make a direct serial connection between two computers, your cable must be wired as shown in the following tables.

Note that off-the-shelf NULL modem cables may not be wired properly. Be sure to tell your dealer that your NULL modem cables must be wired as shown in the 25-pin NULL modem table.

9-Pin NULL Modem Cabling

Remote host serial port connector	Calling system serial port connector	Signal
3	2	Transmit Data
2	3	Receive Data
7	8	Request to Send
8	7	Clear to Send
6, 1	4	Data Set Ready and Carrier Detect
5	5	Signal Ground
4	6, 1	Data Terminal Ready

25-Pin NULL Modem Cabling

Remote host serial port connector	Calling system serial port connector	Signal
2	3	Transmit Data
3	2	Receive Data
4	5	Request to Send
5	4	Clear to Send
6, 8	20	Data Set Ready and Carrier Detect
7	7	Signal Ground
20	6, 8	Data Terminal Ready

Overview of Modem Script File

RAS now supports modems through the Universal Modem Driver (Unimodem) and continues to support modems described in this chapter for older legacy systems. To configure a previously installed unsupported modem to work with the Remote Access Service, add an entry for that modem in the Modem.inf file.

For more information on Unimodem, see the files Mdk.doc and Reg.doc at the following location: ftp://ftp.microsoft.com/developr/drg/modem/modemdev.exe.

Modemdev.exe is a self-extracting compressed file. Run it to obtain Mdk.doc and Reg.doc.

Note: The files are Windows 95 documents that are also relevant to Windows NT except for the following areas:

- Plug and Play (PnP)
- Voice INF structures
- VoiceView support
- Parallel port modems

The Modem.inf file

The Modem.inf file lists all modems supported by RAS, along with the command and response strings each modem needs for correct operation. When you select a modem during remote access installation, the Setup program associates the selected modem with the specified communication port. Remote access connection utilities read Modem.inf to obtain the command

strings for the modem associated with each communication port. You can find Modem.inf in the *systemroot*\System32\RAS directory.

General Structure

The Modem.inf file consists of two main parts:

- A global [Responses] section. Example Global Responses

  This section contains common result strings that a variety of modems return.
- Individual sections for each supported modem, such as [AT&T Comsphere 3820]. Example Modem Section

  Modem sections contain the following command strings:
- Initialization
- Dial
- Listen

To connect through an unsupported modem, you will need to modify the Modem.inf file. For detailed information, see Modifying Modem.inf.

See Also

Requirements for Advanced Modem Features

Syntax for Modem.inf

Example Global Responses

The following example shows a typical entry in the global responses section of a Modem.inf file.

```
[Responses]
OK=<cr><lf>OK<cr><lf>
OK=<hFF><cr><lf>OK<cr><lf>
LOOP=<cr><lf>RING<cr><lf>
LOOP=<cr><lf>RRING<cr><lf>
LOOP=<cr><lf>RINGING<cr><lf>
LOOP=<cr><lf>DIALING<cr><lf>
ERROR=<cr><lf>ERROR<cr><lf>
ERROR=<cr><lf>ABORTED<cr><lf>
ERROR_NO_CARRIER=<cr><lf>NO CARRIER<cr><lf>
ERROR_VOICE=<cr><lf>VOICE<cr><lf>
ERROR_NO_DIALTONE=<cr><lf>NO DIALTONE<cr><lf>
ERROR_NO_DIALTONE=<cr><lf>NO DIAL TONE<cr><lf>
ERROR_BUSY=<cr><lf>BUSY<cr><lf>
ERROR_NO_ANSWER=<cr><lf>NO ANSWER<cr><lf>
ERROR_NO_PROMPTTONE=<cr><lf>NO PROMPTTONE<cr><lf>
CONNECT_EC=\
<cr><lf>CARRIER <carrierbps><cr><lf><append>\
<cr><lf>PROTOCOL: V.42/LAPM<cr><lf>\
<cr><lf>COMPRESSION: V.42BIS<cr><lf>\
<cr><lf>CONNECT <connectbps><cr><lf>
```

LOOP

The only information contained by LOOP is that another response is coming. Remote Access then waits for that response before moving on. Any response keyword beginning with LOOP or LOOP_ acts this way.

ERROR

The modem reported an error as soon as a command was sent to the modem. This response often means that the command string sent to the modem is incorrect. Make sure your have the correct modem strings by testing your modem through Windows NT HyperTerminal to help find exactly which command causes the error. See Testing Your Modem.

Try using the AT command without any additional commands. If this returns an error, the modem has probably encountered a hardware problem. Try turning off the modem for about 20 seconds, restarting it, and seeing whether that solves the problem. If this doesn't solve the problem, contact your modem's manufacturer.

CONNECT

Indicates a connection has been established.

OK

The modem has received and successfully processed the command.

CONNECT_EC

Indicates a connection with modem error control or compression enabled.

Example Modem Section

The following example shows a typical modem section in the Modem.inf file.

```
[AT&T Comsphere 3820]
<speaker_on>=M1
<speaker_off>=M0
<hwflowcontrol_on>=\\Q3
<hwflowcontrol_off>=\\Q0
<compression_on>=%C1"H3
<compression_off>=%C0"H0
<protocol_on>=\\N5
<protocol_off>=\\N0
CALLBACKTIME=10
DEFAULTOFF=compression
MAXCARRIERBPS=14400
MAXCONNECTBPS=38400
COMMAND_INIT=AT&F&C1&D2 V1 X7 S0=0 S2=128 S7=55<cr>
COMMAND_INIT=AT<hwflowcontrol><compression><protocol><speaker><cr>
COMMAND_LISTEN=ATS0=1<cr>
COMMAND_DIAL=ATDT<phonenumber><cr>
```

CALLBACKTIME

The time in seconds that the server waits before calling the client back. This delay allows the client's modem to reset itself. Start with 10 seconds, and increase this number if there are problems.

DEFAULTOFF

A list of all the on/off macros that you want turned off by default, until Rasphone.exe turns them on.

MAXCARRIERBPS

The maximum speed the client's modem and the Remote Access server's modem exchange data (bps rate on the telephone line). This speed is always equal to or less than MAXCONNECTBPS.

MAXCONNECTBPS

The maximum speed a modem talks to the computer (DTE-to-DCE bps transfer rate). Set this value to the maximum serial port bps that the modem can support.

speaker

Turns the modem speaker on or off.

protocol

Turns the error control on or off.

compression

Turns modem compression on or off.

hwflowcontrol

Tells the modem whether to use hardware flow control between the COM port and modem.

cr

Inserts a carriage return.

\f

Inserts a line feed.

match

Reports a match if the string enclosed in quotation marks is found in the device response. For example, <match>"Smith" matches "Jane Smith" and "John Smith III".

?

Inserts a wildcard character. For example, CO<?><?>2 matches COOL2 or COAT2, but not COOL3.

phonenumber

Dials the phone number entered in the Dial-Up Networking Phonebook.

carrierbps

The speed at which the client's modem and the remote access server's modem exchange data (bps rate on the telephone line).

connectbps

The speed at which a modem talks to the computer (DTE-to-DCE bps transfer rate).

append

Breaks information into segments and received from the modem one segment at a time. The client expects delays between the segments and waits until all the information has arrived.

ignore

Ignores the rest of a response from the macro on. For example, <cr><lf>CONNECT<ignore> reads the following responses as the same: "crlfCONNECTV-1.1" and "crlfCONNECTV-2.3".

hXX (XX are hexidecimal digits.)

Allows any hexadecimal character to appear in a string including the zero byte, <h00>.

diagnostics

Diagnostic information returned from the PAD when an attempted connection through an X.25 network fails. The **diagnostics** macro collects and displays this information to help identify the problem. This reserved word appears in the Pad.inf file.

facilities

Facility parameters such as **/R** to specify reverse charging.

x25address

The X.121 address (the X.25 equivalent of a phone number) for the remote access server to be called.

x25pad

The type of X.25 packet assembler/disassembler (PAD) to be used. For dialup PADs, it's the name of the X.25 provider.

userdata

Additional connection information required by the X.25 host computer.

message

Raw information from a device, such as a modem. When an error occurs, this information is displayed to help troubleshoot the problem. This reserved word does not appear in any .INF file.

Modifying Modem.inf

To connect through a modem that is not supported by the Remote Access Service, you must modify your Modem.inf file.

To modify Modem.inf

1 Back up your existing Modem.inf file.

2 Copy an existing section to the end of the file and then rename the section header of the copy to the name of your modem.

Ensure that the section header does not exceed 31 characters. You will create a new entry by editing this copy.

3 Provide the following strings:

- Initialization string
- Dial string
- Listen string

Requirements for the initialization string:

- Recall factory settings.
- Track the presence of data-carrier-detect (DCD) (high when a carrier is detected).
- Hang up and disable auto-answer when data terminal ready (DTR) goes from ON to OFF (high to low).
- Return result codes.
- Return verbose codes.
- Enable character echo in command state.
- Wait about 55 seconds for a carrier.
- Disable the +++ escape sequence.

Requirements for the dial string:

- Go off hook and dial.

Requirements for the listen string:

- Answer after one ring.

For further information about command strings, see Commands.

4 Check your modem's documentation to see if the modem responses (result strings) are already included in the global section of Modem.inf. If they are, you don't need to make any changes for the responses. If they are not, you can create private responses in your modem's section. For further information about responses, see Responses.

Note: To avoid unexpected consequences, do not add responses to or delete any of them from the global response section in Modem.inf.

See Also

Requirements for Advanced Modem Features

Requirements for Advanced Modem Features

In creating a new modem section for an unsupported modem, be sure to set the following requirements in the Modem.inf file to enable the advanced modem features.

- Hardware (CTS/RTS) flow control ON.
- Hardware (CTS/RTS) flow control OFF.
- Error Control Protocol ON.

  Autoreliable negotiation starting with V.42 (LAP-M). Fall back to MNP4 or no error control. If your modem does not support V.42, start negotiating with MNP4.
- Error Control Protocol OFF.
- Compression ON.

  Autoreliable negotiation starting with V.42bis. Fall back to MNP5 or no compression. If your modem does not support V.42bis, start negotiating with MNP5.
- Compression OFF.

See Also

Setting Modem Features

Syntax for Modem.inf

A typical modem entry in the Modem.inf file contains the following components. The first four appear in the order given. Comment lines can appear anywhere.

- Section header
- Configuration parameters
- Substitution macros
- Commands
- Comment lines

See Also

Responses

Line Continuation

Assigning an Alias

Section Header

Identifies the specific device to which the section applies. In Modem.inf it is normally a name that identifies the modem make and model. A section header is a string of up to 32 characters between square brackets, and it occupies the first line in each section. For example, [AT&T Comsphere].

Configuration Parameters

Remote Access works with the modem through these parameters. They take the following form:

parameter_name=*value_string*

For example:

```
MAXCARRIERBPS=9600
CALLBACKTIME=8
```

Substitution Macros

Substitution macros are placeholders that are replaced by their values in command strings. Macros follow these rules:

- In the Modem.inf file, macros must come before the first command, and by convention, after the configuration parameters.
- Macro names must be enclosed in angle brackets (< >).

For example:

```
<reset>=&F

<speaker_on>=M1

<speaker_off>=M0
```

For details, see "Substitution Macros."

Commands

Commands are strings of characters sent to the modem. These strings can contain macros and take the following form:

command_keyword=value_string

For further information, see "Commands."

Comment Lines

Comment lines begin with a semicolon (;) and can appear anywhere in the file. Comment lines convey important information to those who maintain the .INF files. For example:

```
; Explanation of modem commands
; &F Reset modem to factory default settings
; &C1 DCD tracks presence of modem carrier
; &D2 Hangup & disable autoanswer when DTR goes from ON TO OFF
```

Substitution Macros

There are two types of substitution macros, as listed below.

Note that nested macros are not allowed. Two adjacent left brackets are always interpreted as a greater than sign, and two adjacent right brackets are always interpreted as a less than sign. Interpreting angle brackets this way allows greater than and less than symbols in a command string, when required.

Macro Type	Form
Unary	<*macro_name*>=*value_string*
Binary	<*macro_name*_ON>=*value_string*
	<*macro_name*_OFF>=*value_string*

Binary Macros

The command AT<reset><cr> would be sent as AT&F0D. Binary macro placeholders are replaced according to instructions from you. For example, if you disable the speaker, the command AT<speaker><cr> is sent as ATM00D. If you enable the speaker then it is sent as ATM10D.

Define binary macros, such as **speaker**, **protocol**, **compression**, and **hwflowcontrol**, as follows:

```
<speaker_on>=M1
<speaker_off>M0
```

As values, use them as shown in the following example:

```
COMMAND_INIT=AT<speaker><cr>
```

Macros in Responses

Some responses can also use macros. Most macros in response strings behave the same way as in commands. However, certain macros, such as **carrierbps** and **x25address**, capture information such as baud rate from the device response string.

The Remote Access Service uses **match**, **?**, **append**, **hXX**, and **ignore** in response strings to recognize responses from a modem or another device.

Reserved Words

The macros in the following list are reserved words, which means you cannot use them in Modem.inf when creating a new entry. Reserved words are case insensitive.

- carrierbps
- connectbps
- message
- phonenumber
- cr
- lf
- match
- ?
- append
- ignore
- hXX

The Pad.inf file uses the following as reserved words:

- diagnostics
- facilities
- x25address
- x25pad
- userdata

Note: Using reserved words as macro names could result in unpredictable behavior of the Remote Access software.

Modem Commands

The set of command keywords (or types) is:

- COMMAND_INIT
- COMMAND_DIAL
- COMMAND_LISTEN

Commands of a given type are executed in the order found in the Modem.inf file. By convention, commands of the same type are grouped together, as shown in the following example from Modem.inf:

```
COMMAND_INIT=AT&F&C1&D2 V1 S0=0 S2=128 S7=55 W0 \
S95=44<speaker><protocol><compression><hwflowcontrol><cr>

COMMAND_LISTEN=ATS0=1<cr>

COMMAND_DIAL=ATDT<phonenumber><cr>
```

Multiple Command Strings

Because most modems accept strings of about 50 characters, Remote Access supports multiple command strings, which let you break up long commands into shorter strings that the modem can accept.

Using multiple command strings, the first line in the previous example from Modem.inf could be rewritten as follows:

```
COMMAND_INIT=AT&F&C1&D2 V1 S0=0 S2=128 S7=55 W0 S95=44<cr>

COMMAND_INIT=AT<speaker><protocol><compression><hwflowcontrol><cr>
```

Notice that each string:

- Is a command in its own right.
- Begins with AT and ends with a carriage return (<cr>).
- Gets a response before going to the next string.

COMMAND_INIT

Initializes the modem.

COMMAND_DIAL

Dials the phone number and connects.

COMMAND_LISTEN

Sets the modem to autoanswer mode. Check your modem documentation for the code that makes the modem answer after the first ring.

Responses

A command-response set consists of one command followed by zero or more responses. Responses are strings that are expected to be received from the device, and can contain macros. Responses take the form:

keyword=value_string

The Modem.inf file contains two types of responses:

Type of response	Location
Global	In the [Responses] section.
Private	Immediately following the command line that is expected to produce the response, and before the next command line.

Global Responses

Responses used by most modems are in the global [Responses] section of Modem.inf. For an example, see Example Global Responses.

Private Responses

Individual modem sections can contain private response strings in Modem.inf. Remote Access checks for private responses first. If it doesn't find a response string to match the actual string returned by the modem, it continues checking in the global response section. There is one exception, however. If the first part of a string containing an <**append**> macro is matched in the private section, the global section will not be searched. Instead, Remote Access waits a few seconds for the rest of the string to arrive from the modem.

For an example, see Example Private Responses

Example Private Responses

The following example shows a section with private responses. Microsoft encourages you to use this method of inserting responses for any section you add.

```
COMMAND_LISTEN=ATS0=1<cr>

CONNECT=<cr><lf>CONNECT <carrierbps><cr><lf>

CONNECT_EC=<cr><lf>CONNECT <carrierbps>/MNP<cr><lf>

CONNECT_EC=<cr><lf>CONNECT <carrierbps>/MNP/COMPRESSED<cr><lf>

CONNECT_EC=<cr><lf>CONNECT <carrierbps>/MNP COMPRESSED<cr><lf>

CONNECT_EC=<cr><lf>CONNECT <carrierbps>/V42<cr><lf>

CONNECT_EC=<cr><lf>CONNECT <carrierbps>/V42BIS<cr><lf>
```

Line Continuation

A backslash character (\) signals a line continuation. This mark indicates commands or responses are continued on the next line, making files more legible.

For example:

```
CONNECT_V42=\

<cr><lf>CARRIER <carrierbps><cr><lf><append>\

<cr><lf>PROTOCOL: V.42/LAPM<cr><lf>\

<cr><lf>COMPRESSION: NONE<cr><lf>\

<cr><lf>CONNECT <connectbps><cr><lf>
```

Note that the backslash is interpreted as a line continuation except when preceded by another backslash. If your modem uses commands that include a backslash, be sure to use double backslashes (\\) when entering these commands.

For example, the AT&T Comsphere 3820 modem enables error control with the \N5 command. Be sure to enter \\N5 in the initialization string for this modem instead of \N5. Otherwise, Remote Access will report a hardware error when trying to dial.

Assigning an Alias

If a modem's command strings are identical to those already listed for another modem, the name of the latter modem can be used as an alias for the former.

For example:

[AT&T Comsphere 3810]

ALIAS=AT&T Comsphere 3820

In this example, the ATT&T Comsphere 3810 uses the command strings of the AT&T Comsphere 3820.

Note: An alias to an alias is not allowed. In other words, you cannot nest aliases. For example, to alias two modems to another modem, you must alias them directly:

[AT&T Comsphere 3811]

ALIAS=AT&T Comsphere 3820

But **not**:

[AT&T Comsphere 3811]

ALIAS=AT&T Comsphere 3810

Testing Your Modem

If you are having trouble connecting through your modem, test the modem's compatibility through Windows NT HyperTerminal.

To test a modem with Windows NT HyperTerminal

1. In the Accessories folder, click the HyperTerminal folder and select HyperTerminal.
2. In the **Connection Description** dialog box, type a name in the **Name** box and then click **OK**.
3. In the **Connect To** dialog box, click **Cancel.**

   Note that HyperTerminal tests the first modem listed in the **Connect Using** box.
4. In the HyperTerminal window, type **at**.

   Your modem should return *OK*, which is echoed on the screen. Some modems return *0*, depending on their result code settings.
5. If your modem will not work through HyperTerminal, call the manufacturer.

This error should not occur under normal circumstances. Restart your computer to make sure that all recent configuration changes have taken effect. If the error persists, consult the Windows NT event log for detailed warnings or errors.

A possible cause of this error is that the connection was rejected by the remote computer because the remote computer has exceeded its client license limit. Contact your system administrator to buy more client licenses or point you to a different remote computer.

Error Messages

600 An operation is pending.

601 The port handle is invalid.

602 The port is already open.

603 Caller's buffer is too small.

604 Wrong information specified.

605 Cannot set port information.

606 The port is not connected.

607 The event is invalid.

608 The device does not exist.

609 The device type does not exist.

610 The buffer is invalid.

611 The route is not available.

612 The route is not allocated.

613 Invalid compression specified.

614 Out of buffers.

615 The port was not found.

616 An asynchronous request is pending.

617 The port or device is already disconnecting.

618 The port is not open.

619 The port is disconnected.

620 There are no endpoints.

621 Cannot open the phone book file.

622 Cannot load the phone book file.

623 Cannot find the phone book entry.

624 Cannot write the phone book file.

625 Invalid information found in the phone book.

626 Cannot load a string.

627 Cannot find key.

628 The port was disconnected.

629 The port was disconnected by the remote machine.

630 The port was disconnected due to hardware failure.

631 The port was disconnected by the user.

632 The structure size is incorrect.

633 The port is already in use or is not configured for Remote Access dialout.

634 Cannot register your computer on the remote network.

635 Unknown error.

636 The wrong device is attached to the port.

637 The string could not be converted.

638 The request has timed out.

639 No asynchronous net available.

640 A NetBIOS error has occurred.

641 The server cannot allocate NetBIOS resources needed to support the client.

642 One of your NetBIOS names is already registered on the remote network.

643 A network adapter at the server failed.

644 You will not receive network message popups.

645 Internal authentication error.

646 The account is not permitted to log on at this time of day.

647 The account is disabled.

648 The password has expired.

649 The account does not have Remote Access permission.

650 The Remote Access server is not responding.

651 Your modem (or other connecting device) has reported an error.

652 Unrecognized response from the device.

653 A macro required by the device was not found in the device .INF file section.

654 A command or response in the device .INF file section refers to an undefined macro

655 The <message> macro was not found in the device .INF file section.

656 The <defaultoff> macro in the device .INF file section contains an undefined macro

657 The device .INF file could not be opened.

658 The device name in the device .INF or media .INI file is too long.

659 The media .INI file refers to an unknown device name.

660 The device .INF file contains no responses for the command.

661 The device .INF file is missing a command.

662 Attempted to set a macro not listed in device .INF file section.

663 The media .INI file refers to an unknown device type.

664 Cannot allocate memory.

665 The port is not configured for Remote Access.

666 Your modem (or other connecting device) is not functioning.

667 Cannot read the media .INI file.

668 The connection dropped.

669 The usage parameter in the media .INI file is invalid.

670 Cannot read the section name from the media .INI file.

671 Cannot read the device type from the media .INI file.

672 Cannot read the device name from the media .INI file.

673 Cannot read the usage from the media .INI file.

674 Cannot read the maximum connection BPS rate from the media .INI file.

675 Cannot read the maximum carrier BPS rate from the media .INI file.

676 The line is busy.

677 A person answered instead of a modem.

678 There is no answer.

679 Cannot detect carrier.

680 There is no dial tone.

681 General error reported by device.

682 ERROR WRITING SECTIONNAME

683 ERROR WRITING DEVICETYPE

684 ERROR WRITING DEVICENAME

685 ERROR WRITING MAXCONNECTBPS

686 ERROR WRITING MAXCARRIERBPS

687 ERROR WRITING USAGE

688 ERROR WRITING DEFAULTOFF

689 ERROR READING DEFAULTOFF

690 ERROR EMPTY INI FILE

691 Access denied because username and/or password is invalid on the domain.

692 Hardware failure in port or attached device.

693 ERROR NOT BINARY MACRO

694 ERROR DCB NOT FOUND

695 ERROR STATE MACHINES NOT STARTED

696 ERROR STATE MACHINES ALREADY STARTED

697 ERROR PARTIAL RESPONSE LOOPING

698 A response keyname in the device .INF file is not in the expected format.

699 The device response caused buffer overflow.

700 The expanded command in the device .INF file is too long.

701 The device moved to a BPS rate not supported by the COM driver.

702 Device response received when none expected.

703 ERROR INTERACTIVE MODE

704 ERROR BAD CALLBACK NUMBER

705 ERROR INVALID AUTH STATE

706 ERROR WRITING INITBPS

707 X.25 diagnostic indication.

708 The account has expired.

709 Error changing password on domain.

710 Serial overrun errors were detected while communicating with your modem.

711 RasMan initialization failure. Check the event log.

712 Biplex port is initializing. Wait a few seconds and redial.

713 No active ISDN lines are available.

714 Not enough ISDN channels are available to make the call.

715 Too many errors occurred because of poor phone line quality.

716 The Remote Access IP configuration is unusable.

717 No IP addresses are available in the static pool of Remote Access IP addresses.

718 PPP timeout.

719 PPP terminated by remote machine.

720 No PPP control protocols configured.

721 Remote PPP peer is not responding.

722 The PPP packet is invalid.

723 The phone number, including prefix and suffix, is too long.

724 The IPX protocol cannot dial-out on the port because the computer is an IPX router.

725 The IPX protocol cannot dial-in on the port because the IPX router is not installed..

726 The IPX protocol cannot be used for dial-out on more than one port at a time..

727 Cannot access TCPCFG.DLL.

728 Cannot find an IP adapter bound to Remote Access.

729 SLIP cannot be used unless the IP protocol is installed.

730 Computer registration is not complete.

731 The protocol is not configured.

732 The PPP negotiation is not converging.

733 The PPP control protocol for this network protocol is not available on the server.

734 The PPP link control protocol terminated..

735 The requested address was rejected by the server..

736 The remote computer terminated the control protocol.

737 Loopback detected..

738 The server did not assign an address.

739 The remote server cannot use the Windows NT encrypted password.

740 The TAPI devices configured for Remote Access failed to initialize or were not installed correctly.

741 The local computer does not support encryption.

742 The remote server does not support encryption.

743 The remote server requires encryption.

744 Cannot use the IPX net number assigned by the remote server. Check the event log.

752 A syntax error was encountered while processing a script.

600

This error should not occur under normal circumstances. Restart your computer to make sure that all recent configuration changes have taken effect. If the error persists, consult the Windows NT event log for detailed warnings or errors.

601

This error should not occur under normal circumstances. Restart your computer to make sure that all recent configuration changes have taken effect. If the error persists, consult the Windows NT event log for detailed warnings or errors.

602

Another application is using the port. Close the application and redial.

603

This error should not occur under normal circumstances. Restart your computer to make sure that all recent configuration changes have taken effect. If the error persists, consult the Windows NT event log for detailed warnings or errors.

604

The Remote Access Phone Book file and the current Remote Access configuration are probably inconsistent. If you have changed your communications equipment (such as your serial port or modem), be sure to reconfigure Remote Access. See Reconfiguring Dial-Up Networking.

605

The Remote Access Phone Book file and the current Remote Access configuration are probably inconsistent. If you have changed your communications equipment (such as your serial port or modem), be sure to reconfigure Remote Access. See Reconfiguring Dial-Up Networking.

If the error persists, remove and recreate the affected Phone Book entry or, reinstall the Remote Access Service.

The Remote Access Phone Book (RASPHONE.PBK) is in the SYSTEM32\RAS subdirectory of your Windows NT directory.

606

This error should not occur under normal circumstances. Restart your computer to make sure that all recent configuration changes have taken effect. If the error persists, consult the Windows NT event log for detailed warnings or errors.

607

This error should not occur under normal circumstances. Restart your computer to make sure that all recent configuration changes have taken effect. If the error persists, consult the Windows NT event log for detailed warnings or errors.

608

The Remote Access Phone Book file and the current Remote Access configuration are probably inconsistent. If you have changed your communications equipment (such as your serial port or modem), be sure to reconfigure Remote Access. See Reconfiguring Dial-Up Networking.

If the error persists, remove and recreate the affected Phone Book entry or, reinstall the Remote Access Service.

The Remote Access Phone Book (RASPHONE.PBK) is in the SYSTEM32\RAS subdirectory of your Windows NT directory.

609

The Remote Access Phone Book file and the current Remote Access configuration are probably inconsistent. If you have changed your communications equipment (such as your serial port or modem), be sure to reconfigure Remote Access. See Reconfiguring Dial-Up Networking.

If the error persists, remove and recreate the affected Phone Book entry or, reinstall the Remote Access Service.

The Remote Access Phone Book (RASPHONE.PBK) is in the SYSTEM32\RAS subdirectory of your Windows NT directory.

610

This error should not occur under normal circumstances. Restart your computer to make sure that all recent configuration changes have taken effect. If the error persists, consult the Windows NT event log for detailed warnings or errors.

611

Most likely, your network configuration is wrong. Restart your computer to make sure that all recent configuration changes have taken effect. If error persists, consult the Windows NT event log for detailed warnings or errors.

612

Most likely, your network configuration is wrong. Restart your computer to make sure that all recent configuration changes have taken effect. If error persists, consult the Windows NT event log for detailed warnings or errors.

613

This error should not occur under normal circumstances. Restart your computer to make sure that all recent configuration changes have taken effect. If the error persists, consult the Windows NT event log for detailed warnings or errors.

614

This error should not occur under normal circumstances. Restart your computer to make sure that all recent configuration changes have taken effect. If the error persists, consult the Windows NT event log for detailed warnings or errors.

615

The Remote Access Phone Book file and the current Remote Access configuration are probably inconsistent. If you have changed your communications equipment (such as your serial port or modem), be sure to reconfigure Remote Access. See Reconfiguring Dial-Up Networking.

If the error persists, remove and recreate the affected Phone Book entry or, reinstall the Remote Access Service.

The Remote Access Phone Book (RASPHONE.PBK) is in the SYSTEM32\RAS subdirectory of your Windows NT directory.

616

This error should not occur under normal circumstances. Restart your computer to make sure that all recent configuration changes have taken effect. If the error persists, consult the Windows NT event log for detailed warnings or errors.

617

Wait for Remote Access to finish disconnecting the entry or close the Remote Access Service.

618

This error should not occur under normal circumstances. Restart your computer to make sure that all recent configuration changes have taken effect. If the error persists, consult the Windows NT event log for detailed warnings or errors.

619

This error should not occur under normal circumstances. Restart your computer to make sure that all recent configuration changes have taken effect. If the error persists, consult the Windows NT event log for detailed warnings or errors.

620

Most likely, your network configuration is wrong. Restart your computer to make sure that all recent configuration changes have taken effect. If error persists, consult the Windows NT event log for detailed warnings or errors.

621

The Remote Access Service uses the RASPHONE.PBK file in the \SYSTEM32\RAS subdirectory of your Windows NT directory. Make sure the file is on this path, and restart Remote Access.

622

The Remote Access Service uses the RASPHONE.PBK file in the \SYSTEM32\RAS subdirectory of your Windows NT directory. Make sure the file is on this path, and restart Remote Access.

623

Remote Access has located the Phone Book but cannot find the specified entry. This error should not occur unless you are writing to Remote Access APIs, and have specified an incorrect entry name. The Remote Access Service uses the file RASPHONE.PBK, located in the \SYSTEM32\RAS subdirectory of your Windows NT directory.

624

The Remote Access Service uses the RASPHONE.PBK file in the \SYSTEM32\RAS subdirectory of your Windows NT directory. Make sure your disk is not full and that you have write access to this file.

625

The Remote Access Service uses the file RASPHONE.PBK, located in the \SYSTEM32\RAS subdirectory of your Windows NT directory. Delete this file, and restart Remote Access.

626

This error should not occur under normal circumstances. Restart your computer to make sure that all recent configuration changes have taken effect. If the error persists, consult the Windows NT event log for detailed warnings or errors.

627

One of the Remote Access configuration files probably contains invalid information. The easiest way to resolve this problem is to reinstall Remote Access.

If you are using a modem that is not supported by Remote Access, switch to a supported modem, or see Overview of Modem Script File for information about modifying the modem script file for your modem.

The Remote Access script files (PAD.INF, MODEM.INF, and SWITCH.INF) are in the \SYSTEM32\RAS subdirectory of your Windows NT directory.

628

Redial the entry. If you continue to get this message, reduce the modem's initial speed, and turn off the advanced modem features. See Setting Modem Features. If the problem persists, contact your system administrator.

629

The link has been disconnected for one of the following reasons:

- An unrecoverable phone line error.
- A noisy line.
- Disconnection by the system administrator.
- A conflict in configuration parameters between the client and the remote computer.

To re-establish the link, verify that the authentication, encryption, and DNS parameters defined in the Dial-Up Networking phonebook entry match those that are configured on the remote computer. If the remote computer cannot authenticate the client, the connection will be terminated. Also, try lowering your modem speed. See Setting Modem Features.

You can enable automatic redialing through the User Preferences **Dialing** tab. See Redial Settings

630

The link has been disconnected for one of the following reasons:

- An unrecoverable error occurred in your modem (or other communication device).
- An unrecoverable error occurred on your communications port.
- Your modem cable has come unplugged.

Possible actions to diagnose and correct the problem:

- Make sure your modem is on and your cable is securely attached.
- Make sure your modem is functioning properly. For instructions on testing your modem through Windows NT Terminal, see Testing Your Modem.

631

You have disconnected the line through an action on your computer. Redial.

632

This error should not occur under normal circumstances. Restart your computer to make sure that all recent configuration changes have taken effect. If the error persists, consult the Windows NT event log for detailed warnings or errors.

633

If the port is already in use by another connection, hang up the connection on this port, or edit the entry to use another communication port.

If the port is not already in use, reconfigure your Remote Access port for dial out. Ensure that the adapter/modem has been installed and the port has been added using the Control Panel **Network** option. See Reconfiguring Dial-Up Networking.

634

The Remote Access server was unable to register your computer's name on the network. Contact your system administrator.

635

This error should not occur under normal circumstances. Restart your computer to make sure that all recent configuration changes have taken effect. If the error persists, consult the Windows NT event log for detailed warnings or errors.

636

Your hardware configuration and the Remote Access setup are probably inconsistent with each other. If you have changed your communications equipment (such as serial port or modem), be sure to reconfigure Remote Access accordingly. See Reconfiguring Dial-Up Networking.

This error occurs when a section header(an entry within square brackets:[]) in the MODEM.INF file is longer than 32 characters. Ensure that the section header in MODEM.INF is 32 characters or less before attempting any other corrective action.

637

This error should not occur under normal circumstances. Restart your computer to make sure that all recent configuration changes have taken effect. If the error persists, consult the Windows NT event log for detailed warnings or errors.

638

This error should not occur under normal circumstances. Restart your computer to make sure that all recent configuration changes have taken effect. If the error persists, consult the Windows NT event log for detailed warnings or errors.

639

Most likely, your network configuration is wrong. Restart your computer to make sure that all recent configuration changes have taken effect. If error persists, consult the Windows NT event log for detailed warnings or errors.

Please record the Fail Code (a NetBIOS error code), and make it available to your technical support staff if you call for help.

640

Your modem may not have negotiated the connection correctly, or the line may be noisy. Set the modem to a lower initial speed (bps), and dial again. See Setting Modem Features and Modem Idiosyncrasies. Please record the Fail Code (a NetBIOS error code), and make it available to your technical support staff if you call for help.

641

Ask your system administrator to increase the resource capacity of the Remote Access server, or through the Services Control Panel stop nonessential services on your computer, such as messaging and network DDE.

642

Networking architecture requires each computer on the network to be registered with a unique name. This rule applies to both the LAN and remote workstations.

To see if your computer has a unique name on the network, do the following:

- Make sure your computer name is different from all other computer names on the network.

  To change your computer name, start the **Network** Control Panel, and select a new computer name.

  If the name is not your computer name, another computer may have registered a computer name matching your domain name, or you are running a NetBIOS application that has added a conflicting name.
- If the problem persists after changing the name, contact your system administrator

Note

- Because unique names are required, you cannot have both a Remote Access and a direct connection (such as Ethernet connector) to the same network. If you are evaluating Remote Access in such a situation, you need to unplug the network connector before attempting to connect through Remote Access.

643

Report this error to your system administrator.

644

Another computer already connected to the network is using your messaging name. Messages addressed to you will be sent to that computer. If you want to receive messages at your remote workstation, you must remember to log off your office computer before you next dial in to the network.

Note

- This error does not affect messaging through Microsoft Mail.

645

This error should not occur under normal circumstances. Restart your computer to make sure that all recent configuration changes have taken effect. If the error persists, consult the Windows NT event log for detailed warnings or errors.

Please record the Fail Code (a NetBIOS error code), and make it available to your technical support staff if you call for help.

646

Your account has been configured for limited access to the network. If you need to access the network at a different time of day than what's presently configured, ask your system administrator to change the configuration.

647

Ask your system administrator to enable your account.

If you are connecting through the Remote Access Phone Book, you will automatically be prompted to change your password.

If you are connecting through the **RASDIAL** command, you can change your password by doing the following:

1 Press CTRL+ALT+DEL.

2 Select Change Password, and follow the instructions on the screen.

649

You have a valid account on the domain you selected, but your account does not have permission to access the network remotely. Ask your system administrator to give you dial-in permission.

If you have an account with dial-in permission on another domain, do the following to use your account on that domain:

1 Edit the Phone Book entry and clear the **Authenticate using current user name and password** check box.

2 Dial.

3 Specify the appropriate user name, password, and domain.

650

One of the following may have caused this error:

- The Remote Access server is not running. Contact your system administrator to make sure the server is running.
- The line may be too noisy. Lower the modem's initial speed (bps), and dial again. See Setting Modem Features.
- Your modem may have failed to negotiate correctly with the Remote Access server's modem at the selected speed. Lower the modem's initial speed (bps), and dial again.

651

Your modem (or other connecting device) has reported an error. If you are using a supported modem, turn the modem off and then back on. Close and restart the Remote Access Service, and then redial.

If your modem is not supported by Remote Access, contact your modem's manufacturer. For a list of supported modems, see the Windows NT Hardware Compatibility List.

Make sure you have correctly configured your modem for Remote Access. To check your configuration, see Reconfiguring Dial-Up Networking.

652

Your modem (or other connecting device) has returned a message that is not listed in one or more of your Remote Access script files (PAD.INF, MODEM.INF, or SWITCH.INF).

If you are connecting through a supported modem, turn the modem off and back on. Then redial. If the problem persists, try connecting at a lower initial speed. See Setting Modem Features.

If you are connecting through an unsupported modem, make sure that the indicated response is included in the appropriate script file. See Overview of Modem Script File.

The Remote Access script files are located in the \SYSTEM32\RAS subdirectory of your Windows NT directory.

653

One of the Remote Access configuration files probably contains invalid information. The easiest way to resolve this problem is to reinstall Remote Access.

If you are using a modem that is not supported by Remote Access, switch to a supported modem, or see Overview of Modem Script File for information about modifying the modem script file for your modem.

The Remote Access script files (PAD.INF, MODEM.INF, and SWITCH.INF) are in the \SYSTEM32\RAS subdirectory of your Windows NT directory.

654

One of the Remote Access configuration files probably contains invalid information. The easiest way to resolve this problem is to reinstall Remote Access.

If you are using a modem that is not supported by Remote Access, switch to a supported modem, or see Overview of Modem Script File for information about modifying the modem script file for your modem.

The Remote Access script files (PAD.INF, MODEM.INF, and SWITCH.INF) are in the \SYSTEM32\RAS subdirectory of your Windows NT directory.

655

One of the Remote Access configuration files probably contains invalid information. The easiest way to resolve this problem is to reinstall Remote Access.

If you are using a modem that is not supported by Remote Access, switch to a supported modem, or see Overview of Modem Script File for information about modifying the modem script file for your modem.

The Remote Access script files (PAD.INF, MODEM.INF, and SWITCH.INF) are in the \SYSTEM32\RAS subdirectory of your Windows NT directory.

656

One of the Remote Access configuration files probably contains invalid information. The easiest way to resolve this problem is to reinstall Remote Access.

If you are using a modem that is not supported by Remote Access, switch to a supported modem, or see Overview of Modem Script File for information about modifying the modem script file for your modem.

The Remote Access script files (PAD.INF, MODEM.INF, and SWITCH.INF) are in the \SYSTEM32\RAS subdirectory of your Windows NT directory.

657

One of the Remote Access configuration files probably contains invalid information. The easiest way to resolve this problem is to reinstall Remote Access.

If you are using a modem that is not supported by Remote Access, switch to a supported modem, or see Overview of Modem Script File for information about modifying the modem script file for your modem.

The Remote Access script files (PAD.INF, MODEM.INF, and SWITCH.INF) are in the \SYSTEM32\RAS subdirectory of your Windows NT directory.

658

One of the Remote Access configuration files probably contains invalid information. The easiest way to resolve this problem is to reinstall Remote Access.

If you are using a modem that is not supported by Remote Access, switch to a supported modem, or see Overview of Modem Script File for information about modifying the modem script file for your modem.

The Remote Access script files (PAD.INF, MODEM.INF, and SWITCH.INF) are in the \SYSTEM32\RAS subdirectory of your Windows NT directory.

659

One of the Remote Access configuration files probably contains invalid information. The easiest way to resolve this problem is to reinstall Remote Access.

If you are using a modem that is not supported by Remote Access, switch to a supported modem, or see Overview of Modem Script File for information about modifying the modem script file for your modem.

The Remote Access script files (PAD.INF, MODEM.INF, and SWITCH.INF) are in the \SYSTEM32\RAS subdirectory of your Windows NT directory.

660

One of the Remote Access configuration files probably contains invalid information. The easiest way to resolve this problem is to reinstall Remote Access.

If you are using a modem that is not supported by Remote Access, switch to a supported modem, or see Overview of Modem Script File for information about modifying the modem script file for your modem.

The Remote Access script files (PAD.INF, MODEM.INF, and SWITCH.INF) are in the \SYSTEM32\RAS subdirectory of your Windows NT directory.

661

One of the Remote Access configuration files probably contains invalid information. The easiest way to resolve this problem is to reinstall Remote Access.

If you are using a modem that is not supported by Remote Access, switch to a supported modem, or see Overview of Modem Script File for information about modifying the modem script file for your modem.

The Remote Access script files (PAD.INF, MODEM.INF, and SWITCH.INF) are in the \SYSTEM32\RAS subdirectory of your Windows NT directory.

662

One of the Remote Access configuration files probably contains invalid information. The easiest way to resolve this problem is to reinstall Remote Access.

If you are using a modem that is not supported by Remote Access, switch to a supported modem, or see Overview of Modem Script File for information about modifying the modem script file for your modem.

The Remote Access script files (PAD.INF, MODEM.INF, and SWITCH.INF) are in the \SYSTEM32\RAS subdirectory of your Windows NT directory.

663

One of the Remote Access configuration files probably contains invalid information. The easiest way to resolve this problem is to reinstall Remote Access.

If you are using a modem that is not supported by Remote Access, switch to a supported modem, or see Overview of Modem Script File for information about modifying the modem script file for your modem.

The Remote Access script files (PAD.INF, MODEM.INF, and SWITCH.INF) are in the \SYSTEM32\RAS subdirectory of your Windows NT directory.

664

The system has run out of memory. Close some applications, and redial.

665

If the port is already being used for another connection, hang up that connection, or edit this entry to use another communications port.

If the port is not already in use, reconfigure your Remote Access port for dialing out. For instructions, see Reconfiguring Dial-Up Networking.

666

Your modem (or other connecting device) is not responding for one of the following reasons:

- The modem has been turned off.
- The modem is not securely connected to your computer. Make sure your cable is securely fastened to both the modem and the computer.
- The serial cable does not have the correct specifications required by Remote Access. See Cabling Requirements.
- The modem has experienced a hardware glitch. Turn off the modem, wait for 20 seconds, and then restart the modem.

667

One of the Remote Access configuration files probably contains invalid information. The easiest way to resolve this problem is to reinstall Remote Access.

If you are using a modem that is not supported by Remote Access, switch to a supported modem, or see Overview of Modem Script File for information about modifying the modem script file for your modem.

The Remote Access script files (PAD.INF, MODEM.INF, and SWITCH.INF) are in the \SYSTEM32\RAS subdirectory of your Windows NT directory.

668

Redial the entry. If you continue to get this message, reduce the modem's initial speed, and turn off the advanced modem features. See Setting Modem Features. If the problem persists, contact your system administrator.

If you're dialing manually, make sure you're connected before you click **Done**.

669

One of the Remote Access configuration files probably contains invalid information. The easiest way to resolve this problem is to reinstall Remote Access.

If you are using a modem that is not supported by Remote Access, switch to a supported modem, or see Overview of Modem Script File for information about modifying the modem script file for your modem.

The Remote Access script files (PAD.INF, MODEM.INF, and SWITCH.INF) are in the \SYSTEM32\RAS subdirectory of your Windows NT directory.

670

One of the Remote Access configuration files probably contains invalid information. The easiest way to resolve this problem is to reinstall Remote Access.

If you are using a modem that is not supported by Remote Access, switch to a supported modem, or see Overview of Modem Script File for information about modifying the modem script file for your modem.

The Remote Access script files (PAD.INF, MODEM.INF, and SWITCH.INF) are in the \SYSTEM32\RAS subdirectory of your Windows NT directory.

671

One of the Remote Access configuration files probably contains invalid information. The easiest way to resolve this problem is to reinstall Remote Access.

If you are using a modem that is not supported by Remote Access, switch to a supported modem, or see Overview of Modem Script File for information about modifying the modem script file for your modem.

The Remote Access script files (PAD.INF, MODEM.INF, and SWITCH.INF) are in the \SYSTEM32\RAS subdirectory of your Windows NT directory.

672

One of the Remote Access configuration files probably contains invalid information. The easiest way to resolve this problem is to reinstall Remote Access.

If you are using a modem that is not supported by Remote Access, switch to a supported modem, or see Overview of Modem Script File for information about modifying the modem script file for your modem.

The Remote Access script files (PAD.INF, MODEM.INF, and SWITCH.INF) are in the \SYSTEM32\RAS subdirectory of your Windows NT directory.

673

One of the Remote Access configuration files probably contains invalid information. The easiest way to resolve this problem is to reinstall Remote Access.

If you are using a modem that is not supported by Remote Access, switch to a supported modem, or see Overview of Modem Script File for information about modifying the modem script file for your modem.

The Remote Access script files (PAD.INF, MODEM.INF, and SWITCH.INF) are in the \SYSTEM32\RAS subdirectory of your Windows NT directory.

674

One of the Remote Access configuration files probably contains invalid information. The easiest way to resolve this problem is to reinstall Remote Access.

If you are using a modem that is not supported by Remote Access, switch to a supported modem, or see Overview of Modem Script File for information about modifying the modem script file for your modem.

The Remote Access script files (PAD.INF, MODEM.INF, and SWITCH.INF) are in the \SYSTEM32\RAS subdirectory of your Windows NT directory.

675

One of the Remote Access configuration files probably contains invalid information. The easiest way to resolve this problem is to reinstall Remote Access.

If you are using a modem that is not supported by Remote Access, switch to a supported modem, or see Overview of Modem Script File for information about modifying the modem script file for your modem.

The Remote Access script files (PAD.INF, MODEM.INF, and SWITCH.INF) are in the \SYSTEM32\RAS subdirectory of your Windows NT directory.

676

Redial the number. Automate redialing through the User Preferences **Dialing** tab. See Redial Settings

677

A modem did not pick up the phone. Please check the number and dial again.

678

A modem did not pick up the phone. Please check the number and dial again.

679

A modem did not pick up the phone. Please check the number and dial again. Automate redialing through the User Preferences **Dialing** tab. See Redial Settings

Note

- Many modems return this error if the remote modem does not pick up the phone.

680

Make sure the phone line is plugged into the correct socket in the modem. Also, make sure you've added any special access numbers, such as the prefix 9 followed by a comma, to connect to an outside line. For example: 9,555-8181

681

One of the Remote Access configuration files probably contains invalid information. The easiest way to resolve this problem is to reinstall Remote Access.

If you are using a modem that is not supported by Remote Access, switch to a supported modem, or see Overview of Modem Script File for information about modifying the modem script file for your modem.

The Remote Access script files (PAD.INF, MODEM.INF, and SWITCH.INF) are in the \SYSTEM32\RAS subdirectory of your Windows NT directory.

682

This error should not occur under normal circumstances. Restart your computer to make sure that all recent configuration changes have taken effect. If the error persists, consult the Windows NT event log for detailed warnings or errors.

683

This error should not occur under normal circumstances. Restart your computer to make sure that all recent configuration changes have taken effect. If the error persists, consult the Windows NT event log for detailed warnings or errors.

684

This error should not occur under normal circumstances. Restart your computer to make sure that all recent configuration changes have taken effect. If the error persists, consult the Windows NT event log for detailed warnings or errors.

685

This error should not occur under normal circumstances. Restart your computer to make sure that all recent configuration changes have taken effect. If the error persists, consult the Windows NT event log for detailed warnings or errors.

686

This error should not occur under normal circumstances. Restart your computer to make sure that all recent configuration changes have taken effect. If the error persists, consult the Windows NT event log for detailed warnings or errors.

687

This error should not occur under normal circumstances. Restart your computer to make sure that all recent configuration changes have taken effect. If the error persists, consult the Windows NT event log for detailed warnings or errors.

688

This error should not occur under normal circumstances. Restart your computer to make sure that all recent configuration changes have taken effect. If the error persists, consult the Windows NT event log for detailed warnings or errors.

689

This error should not occur under normal circumstances. Restart your computer to make sure that all recent configuration changes have taken effect. If the error persists, consult the Windows NT event log for detailed warnings or errors.

690

This error should not occur under normal circumstances. Restart your computer to make sure that all recent configuration changes have taken effect. If the error persists, consult the Windows NT event log for detailed warnings or errors.

691

Type your user name, password, and domain. If you are unsure of this information, ask your system administrator.

If you do not specify a domain, the Remote Access server attempts to verify your user name and password on the domain of which it is a member.

692

Your modem (or other connecting device) is not responding for one of the following reasons:

- The modem has been turned off.
- The modem is not securely connected to your computer. Make sure your cable is securely fastened to both the modem and the computer.
- The serial cable does not have the correct specifications required by Remote Access. See Cabling Requirements.
- The modem has experienced a hardware glitch. Turn off the modem, wait for 20 seconds, and then restart it.

693

One of the Remote Access configuration files probably contains invalid information. The easiest way to resolve this problem is to reinstall Remote Access.

If you are using a modem that is not supported by Remote Access, switch to a supported modem, or see Overview of Modem Script File for information about modifying the modem script file for your modem.

The Remote Access script files (PAD.INF, MODEM.INF, and SWITCH.INF) are in the \SYSTEM32\RAS subdirectory of your Windows NT directory.

694

This error should not occur under normal circumstances. Restart your computer to make sure that all recent configuration changes have taken effect. If the error persists, consult the Windows NT event log for detailed warnings or errors.

695

This error should not occur under normal circumstances. Restart your computer to make sure that all recent configuration changes have taken effect. If the error persists, consult the Windows NT event log for detailed warnings or errors.

696

This error should not occur under normal circumstances. Restart your computer to make sure that all recent configuration changes have taken effect. If the error persists, consult the Windows NT event log for detailed warnings or errors.

697

This error should not occur under normal circumstances. Restart your computer to make sure that all recent configuration changes have taken effect. If the error persists, consult the Windows NT event log for detailed warnings or errors.

698

One of the Remote Access configuration files probably contains invalid information. The easiest way to resolve this problem is to reinstall Remote Access.

If you are using a modem that is not supported by Remote Access, switch to a supported modem, or see Overview of Modem Script File for information about modifying the modem script file for your modem.

The Remote Access script files (PAD.INF, MODEM.INF, and SWITCH.INF) are in the \SYSTEM32\RAS subdirectory of your Windows NT directory.

699

This error should not occur under normal circumstances. Restart your computer to make sure that all recent configuration changes have taken effect. If the error persists, consult the Windows NT event log for detailed warnings or errors.

700

The limit for commands in the script file is 256 characters. Break up the command into multiple commands. See Commands.

701

Your modem tried to connect at a speed that the serial port cannot interpret. Reset your initial speed to the next lowest standard bps rate: 38400, 19200, 9600, 2400.

702

One of the Remote Access configuration files probably contains invalid information. The easiest way to resolve this problem is to reinstall Remote Access.

If you are using a modem that is not supported by Remote Access, switch to a supported modem, or see Overview of Modem Script File for information about modifying the modem script file for your modem.

The Remote Access script files (PAD.INF, MODEM.INF, and SWITCH.INF) are in the \SYSTEM32\RAS subdirectory of your Windows NT directory.

703

You can connect to entries that require Terminal mode only through the Remote Access Phone Book. This feature is not supported by RASDIAL or the Remote Access APIs.

704

This error should not occur under normal circumstances. Restart your computer to make sure that all recent configuration changes have taken effect. If the error persists, consult the Windows NT event log for detailed warnings or errors.

705

This error should not occur under normal circumstances. Restart your computer to make sure that all recent configuration changes have taken effect. If the error persists, consult the Windows NT event log for detailed warnings or errors.

706

This error should not occur under normal circumstances. Restart your computer to make sure that all recent configuration changes have taken effect. If the error persists, consult the Windows NT event log for detailed warnings or errors.

707

Your X.25 connection has returned an error. Ask your X.25 provider to interpret the diagnostic information provided.

708

Ask your system administrator to reactivate your account.

709

Try changing your password again. If you still get this message, report it to your system administrator.

710

Lower the modem's initial speed (bits per second), and redial. For instructions about lowering the initial speed, see "Setting Modem Features" in online Help.

711

This error should not occur under normal circumstances. Restart your computer to make sure that all recent configuration changes have taken effect. If the error persists, consult the Windows NT event log for detailed warnings or errors.

712

This error can occur on a port configured for dialing out and receiving calls (biplex port). It happens when you dial out at the same time the server is initializing the port for receiving calls. Remote Access solves this problem for you by redialing in a few seconds.

713

Make sure that your ISDN line is plugged in correctly, make sure that the terminating resistors are installed correctly (see the documentation for your ISDN card), and then redial. If you still get this error, contact your ISDN card vendor Customer Service or your ISDN telephone company.

714

All of the available ISDN channels are busy. Hang up one call and redial.

715

Too many asynchronous errors occurred on your phone line during authentication. Try again. If the problem persists, lower your baud rate and disable any modem features that may be set. See "Setting Modem Features" and "Modem Idiosyncrasies" in the Phone Book online help.

716

This error indicates a problem with the Remote Access TCP/IP configuration. User should reboot to ensure all configuration changes have taken effect.

717

Try a specific IP address that will not cause a conflict on the remote network.

718

A PPP conversation was started, but was terminated because the remote computer did not respond within an appropriate time. This can be caused by poor line quality or by a problem at the server.

719

A PPP conversation was started, but was terminated at the request of the remote machine. Most likely an error occurred on the server.

720

Either there are no PPP network control protocols configured for the entry or the corresponding network protocol is not installed. This error may occur when the type of network protocols is changed during the product upgrade process. Correct the entry by checking the desired protocols in the PPP section of the **Network Protocol Settings phonebook entry** dialog box. If you intentionally cleared all protocols to force a downlevel RAS connection, this error indicates the NetBEUI protocol used for down-level connections is not installed.

721

PPP was attempted but the remote computers did not respond. This error occurs when the server does not support PPP, such as a down-level Remote Access server or a SLIP server.

The NetBEUI protocol must be installed to communicate with down-level Remote Access servers. The SLIP protocol must be selected for the entry and the TCP/IP protocol installed to communicate with SLIP servers. For more information, see Network Protocol Settings.

This error may also occur if the server requires a terminal-style log on before starting PPP. If the server requires a terminal-style log on, you can choose to use a terminal window in the Dial-Up Networking **Script** tab.

If terminal log on solves the problem, you can automate the terminal login for future connections by activating an After-dialing script by selecting one in the Dial-Up Networking **Script** tab.

722

A PPP packet was received that was not in a valid format.

723

The maximum length of the phone number, including prefix and suffix, is 128 characters.

724

This is a beta limitation that will be removed for final release.

725

This indicates an inconsistency in the Remote Access IPX configuration. Reboot to ensure all configuration changes have taken effect.

726

Only one port can be used to dial out using the IPX protocol.

727

The TCPCFG.DLL is a required TCP/IP component. Ensure TCP/IP is installed correctly.

728

This error indicates a problem with the Remote Access TCP/IP configuration. Reboot to ensure all configuration changes have taken effect.

729

Install TCP/IP using Control Panel.

730

A request for information on the status of computer registration was made before the information was available.

731

Specific information was requested on a PPP control protocol that is not configured.

732

The negotiation of PPP parameters did not succeed because the local and remote computers could not agree on a common set of parameters.

733

The server supports PPP but does not support the client network protocol.

734

A PPP link control protocol conversation was started, but was terminated at the request of the remote computer. Most likely an error occurred on the server.

735

The client is configured to request a specific IP address. The server is not configured to permit clients requesting specific IP addresses or the specific IP address may already be in use by another client.

736

A PPP network control protocol conversation was started, but was terminated at the request of the remote computer. Most likely an error occurred on the server.

737

The local and remote computers involved in the PPP conversation are the same computer. This usually means a device (for example, a modem) on the link is echoing characters back. Try resetting these devices.

For other vendor's servers, it may indicate that the remote computer is attempting a teletypewriter (TTY) login before connecting. Configure this entry for a post-connect Terminal.

738

The server was unable to assign an IP address to the client from the pool of addresses allocated. Try a specific IP address on the client that will not cause a conflict on the remote network.

739

This error will occur only when making a PPP connection to non-Microsoft Windows NT servers. The standard PPP authentication protocols, used for interoperating with third-party servers, require the password to be available in clear-text form, but Windows NT stores only the encrypted form for security.

740

The TAPI devices configured for Remote Access failed to initialize or were not installed correctly. Remove Remote Access and the TAPI devices then reinstall Remote Access and the TAPI devices.

741

The **Require Data Encryption** check box is selected but the RAS driver does not have encryption capability. Clear the check box to use unencrypted connections.

742

The **Require Data Encryption** check box is selected but the RAS server does not support data encryption. Clear the check box to use unencrypted connections or contact your system administrator.

743

The **remote RAS server requires data encryption** check box is selected but the local RAS client does not have encryption capability.

744

The IPX network number assigned to the client by the RAS server for the WAN interface is already in use on the client's LAN. Disconnect the client from the LAN, wait 3 minutes, and try again.

752

The dial-up script associated with a phonebook entry contains a syntax error.

In Dial-Up Networking, edit the phonebook entry. In the **Script** tab, click **Edit scripts.**

Overview of RAS Automatic Dialing

RAS AutoDial maps and maintains network addresses to RAS phonebook entries, allowing them to be automatically dialed when referenced—whether from an application or from the command line. A network address can be an Internet host name, an IP address, or a NetBIOS server name.

AutoDial also learns about every connection made over a RAS link for possible automatic reconnection later.

There are two possible scenarios when AutoDial attempts to make a connection:

- If you are disconnected from a network, AutoDial attempts to create a network connection whenever an application references a remote address.
- If you are connected to a network, AutoDial attempts to create a network connection for only those addresses that it has previously learned. Incorrectly typed server or Internet host names will not cause an AutoDial attempt.

See Also

Turning off AutoDial

Troubleshooting AutoDial

Turning off AutoDial

Although AutoDial is automatically enabled when you start your computer, you can turn it off if desired. (For example, you might have multiple Internet providers on a computer at one location and want to use different providers at different times).

To turn off AutoDial

1 In Dial-Up Networking, select an entry to dial from the Phonebook list.

2 Click **More** and select **User preferences**.

3 In the **Dialing** tab, clear each location listed in the **Enable auto-dial by location** list.

You can turn on AutoDial by reselecting a location in the **Enable auto-dial by location** list.

See Also

Overview of RAS Automatic Dialing

Troubleshooting AutoDial

Troubleshooting AutoDial

Known Problems for this Release

- AutoDial does not yet work over IPX connections. AutoDial works only with the TCP/IP and NetBEUI protocols. In Dial-Up Networking, select the entry for each RAS connection over which you expect to AutoDial. Then click **More** and select **Edit Entry and Modem Settings**. In the **Server** tab, clear the **IPX/SPX compatible** check box.
- If you need to disable your network card, you cannot simulate being disconnected from the network by simply unplugging the cable from the network adapter card. Instead, create a new hardware profile with your network adapter card disabled:
- In the System icon in Control Panel, in the **Hardware Profiles** tab, make a copy of your original installation. Then, in the Devices icon, select your network card and click **HW Profiles**. Select the new hardware profile and disable your network card. When you reboot, you can choose this no-network profile.
- This is useful if you have a portable computer with a PCMCIA network card installed all the time and you want to connect to the network from a remote location.

- If the following three conditions exist, make sure your DNS server does not resolve Internet hostnames:
- a DNS server on your network
- your network is not directly connected to the Internet
- you want to AutoDial Internet addresses

Most Internet utilities (ftp, www browsers, etc.) do not ask DNS for exact matches, and it is possible for the DNS server to successfully resolve an address to one within your local domain. For example, try typing a similar command at the Command Prompt while connected to your network:

```
C:> ping ftp.microsoft.com

Bad IP address ftp.microsoft.com
```

If the **ping** command resolves the name to an IP address, you must disable DNS on your computer for AutoDial to automatically dial Internet addresses when connected to your network.

- AutoDial requires at least one TAPI dialing location. AutoDial can automatically dial different RAS phonebook entries for the same address, depending on the current TAPI dialing location.

For example, suppose two TAPI dialing locations are created (Home and Office), and suppose you run the command **ftp ftp.microsoft.com**. AutoDial automatically dials the RAS phonebook entry INTERNET1 when your current TAPI dialing location is set to Home, and it automatically dials the RAS phonebook entry INTERNET2 when your current TAPI dialing location is set to Office.

To create TAPI dialing locations, use the Telephony icon in Control Panel.

- When the Explorer is initializing, it might reference remote paths in your desktop shortcut icons or targets which, in turn, will cause an AutoDial attempt. If AutoDial tries to create a connection when you log on to your computer, either delete remote paths from your Desktop shortcut icons or targets, or change them to reference a local file.
- If commands in your Explorer Start/Run list access remote paths, selection of one causes an AutoDial attempt. Currently, you cannot selectively delete items in this list. But to work around this issue, remove the HKCU\Software\Windows\CurrentVersion\Explorer\RunMRU key in the Registry, log out, and log back on again. Your Explorer Start/Run list should now be empty.
- The Registry configuration for AutoDial has changed. It is recommended that you delete the Autodial registry key in:

```
HKEY_CURRENT_USER\Software\Microsoft\RAS
```

AutoDial will then relearn your addresses.

AutoDial Status

If you have problems, run the following command from the Command Prompt to give basic AutoDial status:

C:> rasautou -s

Status ouptput has two parts: network adapter card bindings and a list of learned AutoDial addresses. At least one network adapter card binding must be reported as working for AutoDial to realize you are connected to the network. For AutoDial to automatically create a network connection while you are connected to a network, the address must be in the list of learned AutoDial addresses. Here is an example listing network adapter card bindings and a list of learned addresses:

```
Checking netcard bindings...

NetworkConnected: network (\Device\Nbf_IEEPRO1, 0) is up

Enumerating AutoDial addresses...

There are 3 Autodial addresses:

ftp.microsoft.com
```

```
198.105.232.1
SCRATCH
```

See Also

Turning off AutoDial

Overview of RAS Automatic Dialing

Overview of Multilink Dialing

Multilink combines multiple physical links into a logical "bundle." This aggregate link increases your bandwidth.

RAS performs PPP Multilink dialing over multiple ISDN, X.25, or modem lines. The feature is available only if multiple WAN adapters are available on the computer.

To use Multilink, both the clients and servers must have Multilink enabled.

Note: If a client uses a multinked phonebook entry to dial a server that is configured to call that user back for security reasons (*enforced callback*), then only one of the multilinked devices will be called back. This is because only one number can be stored in a user account. Therefore, only one device will connect and all other devices will fail to complete the connection, and the client loses multilink functionality.

A situation that will work is if the multilinked phonebook entry is ISDN with two channels that have the same phone number.

Enabling Multilink

To enable Multilink on a RAS client

1 In Dial-Up Networking select an entry to dial from the Phonebook list.

2 Click **More** and select **Edit entry and modem properties**.

3 In the **Basic** tab, in the **Dial using** box, select multiple lines.

4 Click **Configure** to choose which modems or adapters to use for the connection and then click **OK**.

To enable Multilink on a RAS server

1 In Control Panel, click the Network icon.

2 In the **Services** tab, select **Remote Access Service** in the Network Services box and click **Configure**.

3 In the **Remote Access Setup** dialog box, click **Network**.

4 In the **Network Configuration** dialog box, select **Enable Multilink** and click **OK**.

Monitoring Connections and Status Reporting

The Dial-Up Networking Monitor (located in the Control Panel) provides the status of a call, and allows you to see

- the speed at which you connected
- the duration of the connection
- the names of users connected to a RAS server
- protocols used during the connection
- which devices are part of a connection

You also use the Dial-Up Networking Monitor to hang-up active connections. If you have Multilink connections, you can hang up a specific device if you want to use it for another call.

By default, the Dial-Up Networking Monitor appears on the taskbar as you dial out. Use the **Preferences** tab to change the view and configure it to appear as window. The Dial-Up Networking Monitor displays lights to indicate traffic over dial-up lines: A button flashes blue when sending or receiving data, and a button flashes red when an error occurs.

Also, when Dial-Up Networking Monitor is viewed as a window, you can configure it to show rows of lights for multiple devices. To do this, in the **Preferences** tab, click **Lights**.

For specific information on the dialog box properties, click the question mark.

Overview of X.25

An X.25 network transmits data with a packet-switching protocol. This protocol relies on an elaborate worldwide network of packet-forwarding nodes that can participate in delivering an X.25 packet to its designated address.

See Also

Installing X.25

Setting X.25 Parameters

X.25 Troubleshooting

Installing X.25

1 Install the X.25 PAD or smart card and start your computer. See your X.25 manufacturer's documentation for instructions on installing the card.
2 Reconfigure the Remote Access Service for X.25. See Reconfiguring Dial-Up Networking

See Also

Setting X.25 Parameters

X.25 Troubleshooting

Setting X.25 Parameters

1 In Dial-Up Networking, select a phonebook entry and then click **More** and choose **Edit entry and modem properties**.

2. In the **X.25** tab, select your X.25 provider and type the X.25 address of the remote server.

3. You can enter additional information in the **User Data** and **Facilities** boxes.

See Also

Overview of X.25

X.25 Troubleshooting

Overview of ISDN

Integrated services digital network (ISDN) offers a much faster communication speed than the telephone line. The phone line communicates typically at 9600 bits per second (bps), whereas ISDN communicates at speeds of 64 or 128 Kb per second. Businesses that need this kind of speed usually have a large telecommuting work force or need to do extensive administrative tasks remotely such as installing software on off-site workstations.

See Also

Installing Your ISDN Card

Setting ISDN Features

ISDN Troubleshooting

Installing Your ISDN Card

1 Install an integrated services digital network (ISDN) card, and start your computer.

If you install more than one ISDN card, you must restart your computer after you have installed the ISDN drivers. Otherwise, all available ISDN ports may not show up when you configure Remote Access for ISDN.

If you remove and then reinstall RAS on a computer that was previously configured with RAS and ISDN, you will not be able to add the ISDN ports in RAS setup. You must reconfigure the ISDN driver before reinstalling and reconfiguring RAS with ISDN ports.

Note: Older DigiBoard cards don't work on some computers. If you don't have the latest PCIMAC-ISA DigiBoard card, serial number A14308 or greater, contact DigiBoard for a replacement.

2 Reconfigure the Remote Access Service for ISDN. See Reconfiguring Dial-Up Networking

See Also

Setting ISDN Features

Setting ISDN Features

To configure ISDN parameters

1 In **Dial-Up Networking**, select a phonebook entry, and then click **More.**

2 Click **Edit entry and modem properties** or **Clone entry and modem properties**.

3 On the **Basic** tab, select a device in the **Dial using** box and then click **Configure**.

4 In the **ISDN Configuration** dialog box, set the line type and other hardware features.

To configure the ISDN adapter or install a new ISDN adapter, choose the Network icon in Control Panel. In the **Adapters** tab, select the adapter and then click **Add** or **Properties**. Click the Help button in the dialog boxes for more information.

See Also

Adding/Editing/Cloning an Entry

Overview of ISDN

PPTP Overview

A RAS server is usually connected to a PSTN, ISDN, or X.25 network, allowing remote users to access a server through these networks. RAS now allows remote users access through the Internet by using the new Point-to-Point Tunneling Protocol (PPTP).

PPTP is a new networking technology that supports multiprotocol virtual private networks (VPNs), enabling remote users to access corporate networks securely across the Internet by dialing into an Internet Service Provider (ISP) or by connecting directly to the Internet. PPTP offers the following advantages:

Lower Transmission Costs PPTP uses the Internet as a connection instead of a long-distance telephone number or 800 service. This can greatly reduce transmission costs.

Lower Hardware Costs PPTP enables modems and ISDN cards to be separated from the RAS server. Instead, they can be located at a modem pool or at a communications server (resulting in less hardware for an administrator to purchase and manage).

Lower Administrative Overhead With PPTP, network administrators centrally manage and secure their remote access networks at the RAS server. They need to manage only user accounts instead of supporting complex hardware configurations.

Enhanced Security Above all, the PPTP connection over the Internet is encrypted and secure, and it works with any protocol (including, IP, IPX, and NetBEUI).

See Also

Applications for PPTP

Applications for PPTP

PPTP provides a way to route PPP packets over an IP network. Since PPTP allows multiprotocol encapsulation, you can send any type of packet over the network. For example you can send IPX packets over the Internet.

PPTP treats your existing corporate network as a PSTN, ISDN, or X.25 network. This virtual WAN is supported through public carriers, such as the Internet.

Compare PPTP to the other WAN protocols: When you use PSTN, ISDN, or X.25, a remote access client establishes a PPP connection with a RAS server over a switched network. After the connection is established, PPP packets are sent over the switched connection to the RAS servers to be routed to the destination LAN.

In contrast, when you use PPTP instead of using a switched connection to send packets over the WAN, a transport protocol such as TCP/IP is used to send the PPP packets to the RAS server over the virtual WAN.

The end benefit for both the user and the corporation is a savings in transmission costs by using the Internet rather than long distance dial-up connections.

The following topics describe how PPTP can be used: for outsourcing a dial-up network, for client connections directly through the Internet , and for client connections through an ISP.

See Also

PPTP in Outsourced Dial-Up Networks

Secure Access to Corporate Networks over the Internet (Virtual Private Networks)

PPTP in Outsourced Dial-Up Networks

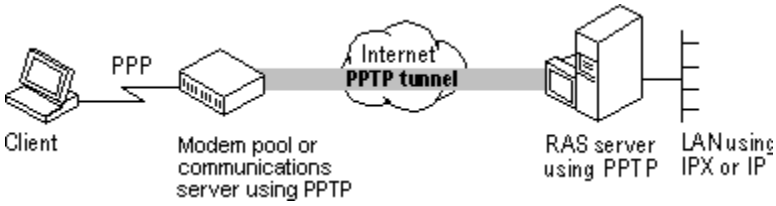
Communications hardware available for supporting dial-up needs can be complicated and not well integrated. For a large enterprise, putting together a Windows NT RAS server requires modems, serial controllers, and many cables. Furthermore, many solutions do not provide a single integrated way to efficiently support V.34 and ISDN dial-up lines.

Many corporations would like to outsource dial-up access to their corporate backbone networks in a manner that is cost effective, hassle free, protocol independent, secure, and that requires no changes to the existing network addressing. Virtual WAN support using PPTP is one way a service provider can meet the needs of corporations.

By separating modem pools from a RAS server, PPTP allows you to outsource dial-up services or geographically separate the RAS server from the hardware within a corporation. For example, a telephone company can manage modems and telephone lines so that user account management can be centralized at the RAS server. An end user would then make a local call to the telephone company which connects to a Windows NT RAS sever using a WAN link. The client then has access to the corporate network.

This type of solution leverages existing proven PPP authentication, encryption, and compression technologies.

See the following figure for an example: The RAS client does not need to have a PPTP driver; the client simply makes a PPP connection to the modem pool or communications server. Note that the communication server or modem pool must implement PPTP for communication with the RAS server.



See Also

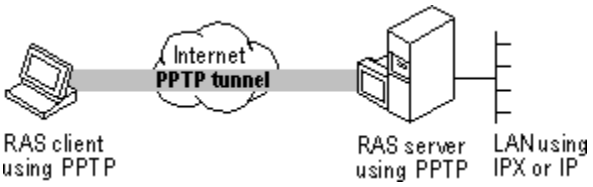
Secure Access to Corporate Networks over the Internet (Virtual Private Networks)

Secure Access to Corporate Networks over the Internet (Virtual Private Networks)

A RAS client that has a PPTP driver as its WAN driver can access resources on a remote LAN by connecting to a Windows NT RAS server through the Internet. There are two ways to do this: By connecting directly to the Internet or by dialing an ISP as shown in the following examples.

In the first, a client directly connected on the Internet dials the number for the RAS server. The PPTP driver on the client makes a tunnel through the Internet and connects to the PPTP enabled adapter on the RAS server. After authentication, the client can access the corporate network, as shown in the following figure.

Note: Connecting directly to the Internet means direct IP access without going through an ISP. (For example, some hotels allow you to use an Ethernet cable to gain a direct connection to the Internet.)



In the second example, the same functionality is achieved by calling an ISP instead of being directly connected to the Internet. The client first makes a call to the ISP. After that connection is established, the client makes another call to the RAS sever that establishes the PPTP tunnel.

See Also

PPTP in Outsourced Dial-Up Networks

Security Considerations

Data sent across the PPTP tunnel is encapsulated in PPP packets. Because RAS supports encryption, the data will be encrypted. RAS supports bulk data encryption using RSA RC4 and a 40-bit session key that is negotiated at PPP connect time between the RAS client and the Windows NT RAS server.

PPTP uses the Password Authentication Protocol and the Challenge Handshake Authentication Protocol encryption algorithms.

In addition to supporting encrypted PPP links across the Internet, a PPTP-based solution also enables the Internet to become a network backbone for carrying IPX and NetBEUI remote-access traffic. PPTP can transfer IPX traffic because it encapsulates and encrypts PPP packets so that they can ride TCP/IP. Thus, a solution does not depend only on TCP/IP LANs.

See Also

Installing PPTP

Protecting a RAS Server from Internet Attacks

Installing PPTP

You must have the PPTP protocol installed on the RAS server—and on the client or communications server—for PPTP tunneling to succeed.

To install the PPTP protocol

1. In Control Panel, double-click the Network icon, then click the **Protocols** tab.
2. Click **Add** and select **Point to Point Tunneling Protocol**.

   When prompted for the path to the distribution files, provide the path and click **OK**.
3. Enter the number of connections you want available to PPTP (i.e. Virtual Private Networks).

   RAS setup will start and add the PPTP protocol to RAS. Choose the port on which you want to install the PPTP protocol and click **OK**.
4. You must restart your computer for the PPTP configuration to take effect.

See Also

Security Considerations

Protecting a RAS Server from Internet Attacks

Protecting a RAS Server from Internet Attacks

If you select PPTP filtering, you effectively disable the selected network adapter for all other protocols. Only PPTP packets will be allowed in.

You might want to do this when you have a multihomed computer with one network adapter (with PPTP filtering enabled) connected to the Internet and another network adapter connected to the internal corporate network. Clients outside the corporate network can use PPTP to connect to the computer from across the Internet and gain secure access to the corporate network. Thus, the only traffic that can access the corporate network is PPTP packets from clients who have been authenticated using RAS authentication.

Note: The RAS client can either be connected to the Internet directly or to a service provider. It is not necessary to be connected to both to use PPTP.

To enable PPTP filtering

1 In Control Panel, double-click the Network icon, then click the **Protocols** tab.

2 Select **TCP/IP Protocol**, and click **Properties**.

3 On the **IP Address** tab, click **Advanced**.

4 In the **Adapter** box, select the network adapter for which you want to specify PPTP filtering. The PPTP filtering settings in this dialog box are defined only for the selected network adapter.

5 To enable PPTP filtering, select **Enable PPTP Filtering**.

The settings take effect after you restart the computer.

For more information about advanced TCP/IP configuration, see the topic "To Configure Advanced TCP/IP Options" in the TCP/IP online Help file.

See Also

Installing PPTP

Security Considerations