Additional Notes About Networks in Windows NT

Table of Contents

This document contains information about networks not available in the Microsoft®Windows NT® Server *Networking Supplement* or in Help, as well as information on changes that occurred after publication.

Additional information is available in the Setup.txt, Readme.wri, and Printer.wri files. Setup.txt contains important pre-installation information. Readme.wri contains general information about Windows NT, including information on specific hardware and software applications. Printer.wri contains information related to printing, including information on specific printers.

Using WordPad to View This Document

 If you enlarge the WordPad window to its maximum size, this document will be easier to read. To do so, click the Maximize button in the upper-right corner of the window. Or open the Control menu in the upper-left corner of the WordPad window (press ALT+SPACEBAR), and then click **Maximize**.

To move through the document, press PAGE UP or PAGE DOWN. Or click the arrows at the top and bottom of the scroll bar along the right side of the WordPad window.

To have the words wrap to the screen size or the ruler
1. From the **View** menu, click **Options**.
2. Click either **Wrap to window** or **Wrap to ruler**, and then click **OK**.

To print the document
1. From the **File** menu, click **Print**.
2. Select the printer, and then click **OK**.

Before you call for support on a networking/protocol issue:

Gather the following information:
• Version of Windows NT on affected computers
• Service Packs and hotfixes applied

- Exact error messages displayed on screen and in Event Viewer
- Protocols used on affected computers (in order of lana# preferred)
- Network adapter and driver
- Client/server operating system and protocols if other than Windows NT

If the issue is specific to an area below, make sure you have available the following information:

TCP/IP specific
- Output of "IPCONFIG /ALL" including, but not limited to:
- Host name
- Node type
- IP address
- Subnet mask
- Default gateway
- WINS server
- DHCP server
- Output of ROUTE PRINT command

DHCP/WINS
- Must have administrator access to DHCP Manager and WINS Manager
- Map of push/pull relationships
- Scope ranges (exclusions, reservations, etc.)

IPX specific
- Output from "IPXROUTE CONFIG," including:
- Frame type
- IPX network number
- Internal network number
- Manual or automatic frame detection
- Is direct hosting in use by Windows for Workgroups clients?

CSNW/GSNW
- Preferred server or default NDS tree and context
- NetWare server version
- User account used for gateway (username, group permissions on NetWare server)
- Is packet burst mode enabled or disabled?

FPNW
- Respond to Find_Nearest_Server request enabled?
- Allow new users to log in enabled?
- FPNW server name
- Home directory root path
- Maintain NetWare compatible login enabled for user accounts?
- Domain structure

Routing/MPR
- Is MPR being used?
- Output of "ROUTE PRINT" (for TCP/IP)
- Output of "IPXROUTE SERVERS" (for IPX)
- Output of "IPXROUTE TABLE" (for IPX)
- Are type 20 packets being passed (for IPX)?

Before you call for support on a Dial-Up Networking

issue

First gather the following information:

- Version of Windows NT
- Service packs and hotfixes applied
- Modem make/model
- Does the modem work in HyperTerminal?
- Exact errors displayed on screen and in Event Viewer for Dial-Up Networking client and RAS server
- Protocols in use for Dial-Up Networking
- If TCP/IP protocol, get the relevant IP, DNS, WINS, DHCP information
- Dialin client operating system/software
- Server operating system/software
- If using a multiserial adapter, does the problem exist using a standard serial port?

Before you call for support on a Services for Macintosh issue

First gather the following information:

- Version of Windows NT
- Service Packs and hotfixes applied
- Version of Macintosh client
- How is the Macintosh client connected to the network?
- Are any devices seeding the network?
- Windows NT authentication package in use?
- Size of Windows NT volume being mounted
- If printing related problem, is target printer PostScript or other?

TCP/IP

Removing TCP/IP

If you remove the TCP/IP protocol, the Internet Information Server component (or Peer Web Services component on Windows NT Workstation) cannot be removed using **Add/Remove Programs** in Control Panel. To work around the problem and remove IIS (or Peer Web Services), reinstall the TCP/IP protocol, then remove IIS (or Peer Web Services).

DHCP

Previously the DHCP server ignored the broadcast flag in the discovers/requests and answered always broadcasting. This remained the default behavior. However by setting the (new) **IgnoreBroadcastFlag** registry variable, this behavior can be changed. If **IgnoreBroadcastFlag** is non-existent or if it is set to > 0, we will broadcast. If set to 0, we will unicast if the broadcast bit in the discover packet is 0.

Text changes

The following sections are from the "Managing DHCP Servers" chapter in the Networking Guide for Windows NT Server version 4.0 Resource Kit.

DHCP Offer

Once a DHCP server has received the Discover packet, and determined that it can accommodate the client's request, it responds with a DHCP Offer message. The DHCP Offer frame is 342 bytes total. The first 14 bytes constitute the Ethernet header portion of the packet.

The first distinguishing characteristic is the destination address, which is the Ethernet broadcast address of 255.255.255.255. The server responds to the client with a broadcast which is an Ethernet Type 0800 frame (IP).

Note: By default, Microsoft DHCP server broadcasts the initial (not renewal) DHCP Offer packet to the DHCP client. This default behavior can be changed for Microsoft DHCP server running under Windows NT Server version 4.0. To change this default behavior, you must add the **IgnoreBroadcastFlag** parameter with DWORD Value=0 to the Registry and restart the Microsoft DHCP server service. This parameter should be added under the following key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DhcpServer\Parameters\

Changing the default behavior reduces broadcast traffic. However, this can be done only when the Microsoft DHCP server and DHCP client are on a homogeneous Ethernet network or the same subnet of a Token Ring network. You should not change the default broadcast behavior of a Microsoft DHCP server when the server and client are on different Token Ring subnets or are separated by a router or bridge that does MAC level address translation for example, Ethernet to-or-from Token Ring.

DHCP ACK
Once a DHCP server has received the Request packet, it responds with a DHCP ACK message. The DHCP ACK frame is 342 bytes total. The first 14 bytes constitute the Ethernet header portion of the packet. The first distinguishing characteristic is the destination address, which is the Ethernet broadcast address of 255.255.255.255. The server responds to the client with a broadcast. It is a Ethernet Type 0800 frame (IP).

Note: By default, Microsoft DHCP server broadcasts the initial (not renewal) DHCP ACK packet to the DHCP client. This default behavior can be changed for Microsoft DHCP server running under Windows NT Server version 4.0. To change this default behavior, you must add the IgnoreBroadcastFlag parameter with DWORD Value=0 to the Registry and restart the Microsoft DHCP server service. This parameter should be added under the following key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DhcpServer\Parameters\

Changing the default behavior of Microsoft DHCP server will reduce broadcast traffic generated by the Microsoft DHCP server. However, this can be done only when the Microsoft DHCP server and DHCP client are on a homogeneous Ethernet network or the same subnet of a Token Ring network. You should not change the default broadcast behavior of a Microsoft DHCP server when the server and client are on different Token Ring subnets or are separated by a router or bridge that does MAC level address translation for example, Ethernet to-or-from Token Ring.

DNS
A new DNS registry parameter has been added to enable the Microsoft DNS server to interoperate with non-Microsoft DNS servers that use an older, slower version of the DNS BIND.

The Registry path for this entry is the following:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters
      BindSecondaries
      Data type = **REG_DWORD**
      Range = *0 or 1*
      Default = 1

If this parameter is set to a non-zero value, the MS DNS sends zone transfers to non-Microsoft DNS secondaries with one resource record per message. Non-Microsoft DNS servers using BIND versions prior to 4.9.4 cannot receive the transfer unless it is in this single resource record per message format.

If this parameter is zero, the Microsoft DNS server places as many resource records as possible in each message to achieve maximum compression and speed of transfer. Microsoft DNS servers and non-Microsoft DNS servers that use BIND version 4.9.4 or higher can receive transfers in this format.

Note
Transfers between Microsoft DNS servers will always be done with using the faster, high compression method, regardless of how the BindSecondaries flag is set.

Editing DNS Configuration Files
Be sure to stop DNS before manually editing configuration files. If the server is running when you edit the files, stop and then restart the server. Otherwise, you could experience problems.

DNS Manager
You must be an administrator of the machine in order to see records in the DNS Manager. Otherwise, only statistics can be viewed.

In this version, there is no way of resetting the statistics in DNS Manager without stopping and restarting the DNS Server service. A utility to do this will be in the Windows NT version 4.0 Resource Kit. It is also available from the Windows NT section of the Microsoft web site; www.microsoft.com. The name of the file is dnsstat.exe.

The first time change is in the DNS Manager, the boot information will be moved to the registry. The original boot information will be copied to *systemroot*\system32\dns\backup\boot.bak. The boot file will be modified and includes information on returning to your original state before any changes were made in the DNS Manager.

The **Create Associated PTR Record** check box in the **New Host** and **New Resource Record** dialog boxes are not yet functional. If you select the check box and then click **Done** or **OK**, the associated PTR record is not created.

DNS Names in DNS Manager
The use of DNS names in creating resource records in the DNS Manager differs from the naming convention used in the database files. This difference is primarily to avoid confusion by users relatively new to DNS who are not accustomed to terminating DNS names with a period (.) to indicate a fully qualified DNS name (FQDN).

1) The domain names at which records are located (for example, hostname for A, alias for CNAME, domain for SOA or NS, and so forth) must always be entered by going to (or creating) the desired domain and entering (if necessary) a single part non-dotted DNS name.

2) Domain names which are data in a record (for example, NS nameserver, CNAME cannonical name, SOA primary name server and responsible party, MX mail server, and so forth.) must be given as the full DNS name.

Example: You are adding at CNAME record to the ms.com zone. The alias will be www.nt.ms.com for the actual server jamesg1.ms.com.
   -- click Open on the ms.com zone
   -- click Open (or add domain) the nt subdomain
   -- add the ecord
      -- select CNAME
      -- in "Alias Name" field type "www"
      -- in "For Host DNS Name" type "jamesg1.ms.com"
      -- click OK

Note
For the record data, the entire DNS name is required "jamesg1.ms.com". If you enter a single

part name "jamesg1" for the RR data, the FQDN you will receive will be "jamesg1.", not "jamesg1.ms.com." which would be the result in the database file.

Record Data in DNS Manager
The DNS Manager does not automatically refresh its record data. The reason for this is efficiency -- domains with large numbers of records are expensive to refresh, similar to the work of a zone transfer. Hence, when adding or updating records, the data displayed is the administrative tool's last record of the data. After all your changes have been made to a zone, it is wise to refresh the data for the zone and to verify that the record data is as desired.

Also, if the DNS server has been restarted, you should select that server and perform a refresh. This prevents the DNS Manager from sending obsolete data to the server.

Writing Records Back to the Data File
The server stores records in memory. As soon as a change is made using the DNS Manager, that change will be reflected in the data the DNS Manager sends on the wire. However, that data is not immediately written back to the zone's data file until one of the following occurs: shutdown, periodic cleanup, or prompting by the user.

After making all desired changes to a zone, users are encouraged to select the server and click **Update server data files**. This forces write back of all server data to the database files, and initiates (through SOA NOTIFY) zone transfer requests from the secondary servers.

Changing Server to be Root Authoritative
The DNS server is shipped configured as a caching server for the Internet. (The cache file points at Internet root DNS servers and no zones are configured.)

If the server will be used on a private intranet, the server can be configured to be root authoritative (to have a root zone):
 -- Because the root usually contains cache file data (or cached data) for locating the root servers, before creating a primary root zone, you are advised to open the cache and delete records (usually NS) at the root. If a cached SOA record exists at the root, the administrative tool may not allow deleting it. Simply stop and restart the DNS server to remove it.
-- When creating the root zone, the zone name will be period (.). Be sure and select a an appropriate file name (the default is poorly chosen).
-- After zone creation completes, select the server and refresh, and the "cache" icon should disappear as the server is now root authoritative.

WINS

WINS Server Sends Mysterious Multicast Packets
The WINS service sends packets that are addressed to IP address 224.0.1.24 hardware address 01005E000118.

This is a multicast packet sent so that if some other WINS is set for auto-replication, it will pick up the packet and add the sending WINS as a partner. WINS periodically sends information about itself using these packets. If you do not want these packets to be sent, set UseSelfFndPnrs in the registry under Wins\Parameters to DWORD 0 and also set McastIntvl to some huge value (DWORD FFFFFFFF. For instance, by default the interval is 2400 i.e. 40 mts).

WINS parameters
The following are new WINS registry parameters.
The Registry path for these entries is the following:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Wins\Parameters

BurstHandling
Type = **REG_DWORD**
Value: *0* or *1*
Default = 0

This parameter is used to temporarily achieve a steady state in the WINS server when the WINS server is either started with a clean database or many WINS clients come on-line for the first time. Either situation causes a large amount of name registration and name refresh traffic to occur. The WINS server currently stores a maximum of 25000 name registration and refresh queries in it's queue before dropping queries. By using this parameter the WINS server can be configured to send success responses to the clients whose requests are dropped. These responses will have TTLs that will slow down the refresh rate of those WINS clients and regulate the burst of WINS client traffic. This will result in a steady state being reached much more quickly.

To turn on this parameter, change the value to 1.

\ConsistencyCheck subkey
This is an optional subkey that should be created if you want WINS to periodically perform database consistency checks. The following option values can be created under this key.

MaxRecsAtATime
Type = **REG_DWORD**
Range = 1000 to total number of records
Default = 30000

Specifies the maximum number of records that will be replicated in one consistency check cycle. WINS does consistency checks on the records of each owner WINS server (the WINS server from which the record was replicated). After checking a owner WINS server, the local WINS server continues to the next owner WINS server, or stops. This is determined by the **MaxRecsAtATime** value.

UseRplPnrs
Type = **REG_DWORD** or non-zero value
Range = 0 or not-zero
Default = 0

If set to zero, WINS will contact the owner WINS server.
If set to a non-zero value, WINS sill contact only it's pull partners to perform consistency checks. Specifies the time interval between WINS server database consistency checks. If set to non-zero, WINS randomly picks a WINS from a list of pull partners unless the owner WINS server also happens to be a pull partner. In that case, the owner WINS is contacted.

TimeInterval
Type = **REG_DWORD**
Range = 6 hours -
Default = 24 hours

Specifies the time interval between WINS server database consistency checks.

SpTime
Type = **REG_SZ**
Default = 2:00:00 (2 am).

Specifies the specific time at which the first WINS server database consistency check will occur. The time is specified in hh:mm:ss format. Thereafter, the WINS database is periodically checked for consistency by using the time interval specified in the **TimeInterval** parameter.

Database Conversion Procedure
When the WINS, DHCP, and RPL service starts for the first time after an upgrade to Windows NT version 4.0, it will detect that the database needs to be converted. It will then start a conversion process, JETCONV.EXE. (If JETCONV.EXE has already been started by another

service, another JETCONV process is not started.) Before conversion, you are notified that the conversion process is about to start and is asked for confirmation. If you click **OK**, the WINS, DHCP, and RPL service terminates and the conversion begins. JETCONV converts the databases of all the installed services (WINS, DHCP, and RPL) to the new Windows NT version 4.0 database format.

Once the databases are converted successfully by JETCONV, the service is automatically restarted.

Notes:

▪ Before upgrading to Windows NT Server version 4.0, the Windows NT version 3.51 databases of the WINS, DHCP, and RPL services should be brought to a consistent state. This can be done by terminating the services, either via service control panel or via the net stop service command. This is recommended because it prevents the JETCONV conversion from failing due to an inconsistent Windows NT version 3.51 database.

▪ The conversion requires approximately the same amount of free disk space as the size of the original database and log files. You should have at least 5 MB free for the log files for each database.

▪ The conversion process preserves the original database and log files in a folder named 351db under the same folder where original database and log files were (For example, for DHCP *systemroot*\system32\dhcp\351db\). The administrator can later remove these files to reclaim the disk space.

The database conversion can take anywhere from a minute to an hour, depending on the size of the database. You must not try to restart the services while the databases are being converted. To check the status of the conversion, watch the Application Event Log of the JETCONV process in the Event Viewer.

In case this automatic procedure of converting databases fails for some reason (as can be determined from the event logs), the database that could not be converted can be converted manually using systemroot\system32\upg351db.exe. At the command line, type upg351db -? for instructions.

▪ You cannot convert the new database back to the previous database format.

▪ The converted database will not work with Windows NT version 3.51 or earlier services.

▪ The new database engine uses log files that have the prefix J50.

Dial-Up Networking

Windows NT Remote Access Service (RAS) 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, used to monitor connections and devices, is located in Control Panel.
▪ Remote Access Admin, used to monitor remote users connecting to a RAS server, is located in the **Administrative Tools** folder on the **Start** menu.

Dial-Up Networking Notes

· If a Dial-Up Networking client connects to a RAS server that is using older RAS framing (a Windows NT version 3.1 or Windows for Workgroups version 3.11 RAS server), the client will report 0 percent software compression for throughput. Although compression is actually taking place, it is not being measured correctly in this release.

· In Dial-Up Networking, Null Modem support is now called Dial-Up Networking Serial Cable between 2 PCs. The functionality is the same as Null Modem.

To use a cable to connect two computers, in the Network icon in Control Panel, in the **Services** tab select **Remote Access Service** and click **Properties**. Click **Add,** and then click **Install Modem**. In the **Install New Modem** dialog box, in the **Manufacturers** box select **Standard Modem Types,** select **Dial-Up Networking Serial Cable between 2 PCs** in the **Models** box, and then click **OK**.

· In Dial-Up Networking, in the **Script** tab, the **Pop up a terminal window** option works only for serial ports. For instance, if you select this option and then dial over an ISDN line, you will not see the after dial Terminal dialog.

· In Dial-Up Networking, identical phone numbers for multiple devices may be set in one step. To do this, in the **Edit Phonebook Entry** dialog box, in the **Basic** tab, select **Multiple Lines** in the **Dial using** box and click **Configure**. In the **Multiple Line Configuration** dialog box, hold the SHIFT key to select multiple devices and click **Phone numbers**. The new phone numbers you add will be applied to all the selected devices.

· In chapter 4 "Routing in Windows NT" in the *Networking Supplement*, the following parameters in the section "Registry Parameters for IP RIP" have an incorrect range. The upper end of the range should be 86400 seconds, not 884400 seconds.

> **MaxTriggeredUpdateFrequency**
> Data type = **REG_DWORD**
> Range = *1 second - 86400 seconds (24 hours)*
> Default = 5 seconds
> The minimum number of seconds that must elapse between triggered updates.

> **UpdateFrequency**
> Data type = **REG_DWORD**
> Range = *15 seconds - 86400 seconds (24 hours)*
> Default = 30 seconds
> The number of seconds between periodic updates which contain the entire routing table.

· The following is a new PPP parameter for appendix A "RAS Registry Values" in the *Networking Supplement.*
The Registry path for this entry is the following:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\PPP
> **DefaultCallbackDelay**
> Data type = **REG_DWORD**
> Range = *0 – 255 seconds*
> Default: 12 (if the parameter is not in the Registry)
> Used on RAS clients to tell the RAS server's modem how many seconds to wait before calling back.

· If a Dial-Up Networking client is multihomed (it is using IP on the LAN interface and the Dial-Up Networking link), the client may not be able to communicate with all computers on the LAN. In this case, the client can use the **route** command to add routes for the networks it cannot reach. For example:

If the computer has the following IP configuration on the LAN interface

     IP ADDRESS: 10.1.1.1
     MASK: 255.255.0.0
     DEFAULT GATEWAY: 10.1.1.254

and the Dial-Up Networking link has the following IP configuration

     IP ADDRESS: 20.1.2.3
     MASK: 255.255.0.0
     DEFAULT GATEWAY: 20.1.2.3

then the Dial-Up Networking client will not be able to communicate with computers with an IP address of 10.2.1.1, since by default the IP router will send packets over the Dial-Up Networking link. To fix this, add the following route. **Note**: This is a persistent route and only needs to be added once.

route add -p 10.0.0.0 MASK 255.0.0.0 10.1.1.254

Dial-Up Networking and PPTP

PPTP Clients

· To access PPTP servers using an Internet Service Provider (ISP) that does not support PPTP, first dial your ISP for Internet access. Then, make a second call to the PPTP server using the PPTP server's IP address as the phone number.

· If your computer does not have a modem or ISDN line, you can implement ISDN and modem pooling by using PPTP to dial a communications server on the network which then dials out and connects you to a RAS server on the PSTN or ISDN network.
In Dial-Up Networking, specify the phone number for the entry in the following way:
     12.12.12.12 (206)1234567
where 12.12.12.12 is the IP address of the communications server and (206)1234567 is the phone number you want to call.
Note: There must be a space between the IP address and the phone number.

PPTP Servers

· To use PPTP to call back a user through a PPTP communications server, on the RAS server start Remote Access Admin. In the **Users** menu, click **Permissions**. Select a user and then choose the **Preset To** callback option. In the **Preset To** box type:
     12.12.12.12 (206)1234567
where 12.12.12.12 is the IP address of the communications server and (206)1234567 is the phone number you want to call.
Note: There must be a space between the IP address and the phone number.

· The following are new PPTP parameters for appendix A "RAS Registry Values" in the *Networking Supplement.* If you need this functionality, you must add these values to the Registry because they are not created by default.
The Registry path for these entries is the following:
HKEY_LOCAL_MACHINE\SYSTEM\Services\RASPPTPE\Parameters\Configuration

     AuthenticateIncomingCalls
     DataType = **REG_DWORD**
     Range = *0 - 1*
     Default = 0
     Set this parameter to 1 to force the PPTP protocol to accept calls only from IP addresses listed in the **PeerClientIPAddresses** registry value. If **AuthenticateIncomingCalls** is set to 1 and there are no addresses in **PeerClientIPAddresses**, then no clients will be able to connect.

PeerClientIPAddresses
DataType = **REG_MULTI_SZ**
Range = the format is a valid IP address xx.xx.xx.xx
This parameter is a list of the IP addresses of pptp clients from which this server
will accept PPTP calls. This list is only relevant if the **uthenticateIncomingCalls**
parameter is set to 1.

▪ If you are configuring a Windows NT Server computer to use PPTP as a dial-up server on the
Internet, you must complete the following steps.

1) When you install PPTP, a default route gets installed for each LAN adapter.
For instance, if you have two LAN adapters, one for Internet access and one for
the corporate LAN, you will have default routes for both. To correct this situation,
disable the default route on the corporate LAN adapter by adding the following
registry key:

HKEY_LOCAL_MACHINE\SYSTEM\Services\<*adapter name*>\Parameters\Tcpip
DontAddDefaultGateway
Data type = **REG_DWORD**
Range = *0 – 1*
Default: 1

Note: You must add this registry value for each adapter that is not connected to
the Internet.

2) You must use the **route** command to configure persistent static routes to
point toward the corporate network. For instance, if you have a set of IP
addresses from 123.45.x.x to 123.47.x.x use the following commands:
route add -p 123.45.0.0 MASK 255.555.0.0 <*default gateway*>
route add -p 123.46.0.0 MASK 255.555.0.0 <*default gateway*>
route add -p 123.47.0.0 MASK 255.555.0.0 <*default gateway*>

Dial-Up Networking and Autodial

Text Corrections
▪ In chapter 6 "Installing and Configuring Remote Access Service" in the *Networking
Supplement*, the first paragraph in the section "Known Problems for this Release" under "RAS
Automatic Dialing" is incorrect. Autodial does work over IPX connections.

"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, click to clear the **IPX/SPX compatible** check box."

▪ In chapter 6 "Installing and Configuring Remote Access Service" in the *Networking
Supplement*, the last paragraph in the section "Known Problems for this Release" under "RAS
Automatic Dialing" is incorrect. Please disregard the following text:

"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 disabled without a Dial out port
▪ If you install Dial-Up Networking on a Windows NT Server computer that does not have one
or more ports configured for dialing out, Remote Access Autodial Manager will be installed in a
disabled state. If you later change one or more ports to the **Dial Out** option, Remote Access

Autodial Manager will still be disabled. You must manually select the Autodial service in the Control Panel Services icon and enable it.

Setting addresses that will never cause an Autodial attempt
▪ You can specify a list of addresses that will never cause an Autodial attempt even if Autodial is enabled for the current dialing location. The first time the Autodial service runs, the following registry key is created:
HKEY_CURRENT_USER\Software\Microsoft\RAS Autodial\Control\DisabledAddresses.
Once this value is created, it will not be changed by the Autodial system service, and you can modify the list however you wish. All addresses in the list are case-insensitive.

Disabling cached passwords
▪ Dial-Up Networking caches passwords which can accumulate over time if you have many different phonebook entries. This might result in a slight delay after you type your credentials in the **Connecting To...** dialog box. You can clear cashed passwords for all Dial-Up Networking phonebook entries and prevent cached passwords from being saved in the future by adding the following Registry key to:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\Parameters
> **DisableSavePassword**
> Data type = **REG_DWORD**
> Range = *0 – 1*
> Default: 0

Set the value to 1 to clear cached passwords and prevent cached passwords from being saved.

Disabling Autodial for performance improvement
▪ If a dial out port is configured on a Windows NT Server computer, the Autodial system service automatically enables client-side redial on link failure and Autodial services for the dial out port. If Autodial is not required on the dial out port, you can gain a small performance improvement by disabling it.
To disable Autodial, in Dial-Up Networking, click **More** and select **User preferences**.   In the **Enable auto-dial by location** box, clear the box for each dialing location.

The **Redial on link failure** option will still work even if Autodial is disabled. (There is no performance degradation for enabling redial on link failure.)

Autodial requests when logging in
▪ If an icon in the Start menu is a shortcut to a remote network server or UNC path, the Explorer attempts to load the icon when you logon. If Autodial is enabled, this reference causes an Autodial attempt. You can determine which icons have references to a remote server by using the following command in the \system32 folder:
 findstr /s /m /i /c:"*string*" *.lnk
where *string* is the name of the remote server for which you are getting Autodial requests during logon.

You can change your icon to reference a local icon file instead of a remote icon file. In the Start menu, click **Settings\Taskbar** and in the **Start Menu Programs** tab click **Advanced**. In the Explorer, select the application and right click. Click **Properties** and in the **Shortcut** tab click **Change Icon**. In the **Change Icon** dialog box, type a local path to an icon file (for example %SystemRoot%\system32\shell32.dll).

The Explorer will also cache shortcuts to remote documents in the Start\Documents menu. You can easily clear this menu by clicking **Settings\Taskbar** and in the **Start Menu Programs** tab click **Clear**.

Explorer shortcuts and Autodial
▪ If you are not connected to the network and have a shortcut on the desktop that references a remote file, double-clicking on that shortcut will cause an Autodial attempt but will not start the application after the Dial-Up Networking connection has been made.

This is because the Explorer times-out operations on remote objects after 7.5 seconds and it may take 30 seconds or more to connect if you are using a modem.
After the Dial-Up Networking connection is established, double-click on the shortcut again to start the application.

Invoking Autodial multiple times from the same application using the same DNS or IP address
▪ If you are connected to a local LAN and run an application that references a DNS or IP address that is unreachable, Autodial will only start the first time this address is determined to be unreachable. Subsequent tries using the same DNS or IP address within the same application will not invoke Autodial. Autodial will start if the application is restarted or a different address is used.

Windows 95 Clients
A Windows 95 RNA client must enable compression if it is dialing into a Windows NT version 4.0 RAS server that forces encryption. Otherwise, the RAS server will disconnect the line.

ShivaRemote for Windows Dial-In Clients
If a ShivaRemote for Windows Dial-In client dials into a Windows NT version 4.0 RAS server using NetBEUI, the client will report a NetBIOS error and not connect to the server using NetBEUI. The client can connect using IP or IPX.

Connection Problems between Windows NT version 3.51 Clients and Windows NT version 4.0 Servers
If a Windows NT version 3.51 RAS client dials into a Windows NT version 4.0 RAS server and fails with error 742, the client should clear the **Require data encryption** checkbox in the **Security** tab in Dial-Up Networking and retry the connection. Windows NT version 3.51 clients can eliminate this problem by obtaining the Windows NT version 3.51 Service Pack 5.

If a Windows NT version 4.0 RAS server disconnects a Windows NT version 3.51 RAS client, check to see if the following RemoteAccess event is logged in the Event Viewer:
"The server machine is configured to require data encryption. The machine for user Domain\Username connected on port COMX does not support encryption. The line has been disconnected."

If you see this message, on the Windows NT version 4.0 RAS server, click the Network icon in Control Panel. In the **Services** tab, select **Remote Access Service** and click **Properties**. Click **Network,** and clear the **Force data encryption** checkbox.

Upgrading from Windows NT version 3.5x to Windows NT version 4.0
▪ If Windows NT RAS is upgraded to version 4.0, then the modems that are already installed and configured are treated as modem.inf modems, as indicated in the **Remote Access Setup** dialog box as **Type Modem (modem.inf)**. Any new modems installed after an upgrade or on a new Windows NT installation are added as **Type Modem (unimodem)**. To add a new modem port to RAS configuration, the modem must first be added by clicking **Add** and then clicking **Install Modem.**

▪ If you use Security Dynamics or Digital Pathways 3rd-party security .DLL and are upgrading from Windows NT version 3.5x RAS to Windows NT version 4.0 RAS, you must get new versions of the .DLLs from Security Dynamics and Digital Pathways.

▪ If you have a Digi ISDN BRI adapter, after you upgrade to Windows NT version 4.0, in the Remote Access Service configuration in the Network icon, you might not see the Digi ISDN port. To fix this problem, complete the following steps after the upgrade is complete and before you do any RAS configuration:

- In Control Panel, click Network.
- In the **Adapters** tab, select the Digi ISDN adapter and click **Properties**.
- In the Digi ISDN adapter configuration dialog box, click **OK.**

This ensures that your computer keeps a permanent record of all Digi ISDN lines.

▪ Upgrading to Windows NT version 4.0 does not migrate existing redial settings from the Windows NT version 3.51 phonebook. To correct this, in Dial-Up Networking click **More** and select **User preferences**. In the **Dialing** tab, check the **Redial on link failure** box.

▪ If you are using Windows NT Server Multi-Protocol Routing and have added the DisableOtherSrcPackets registry entry, you must readd the parameter after you upgrade to Windows NT version 4.0.

TAPI/Unimodem Support

Windows NT version 4.0 includes support for the Windows Telephony API (TAPI) and the universal modem driver (Unimodem). The following two files (Mdk.doc and Reg.doc) 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

Windows 95 Modem Development Kit (MDK) (Mdk.doc)
This Windows 95 Modem Development Kit (MDK) provides the tools, sample INF files, and information you need to build and test Windows 95 format INF files for AT (data) and AT+V (voice) command modems. Windows 95 INF files are required for modems to be used by programs which call the Windows Telephony API (TAPI) to make data/fax/voice calls, including the Windows applications HyperTerminal, Dial-up Networking, Phone Dialer, The Microsoft Network as well as other Win32 communications applications written for Windows 95 or Windows NT.

Windows 95 Modem Registry Reference (Reg.doc)
Windows 95 and Windows NT use modem INF files to install modems so they can be used by applications, through the universal modem driver (Unimodem). A modem INF generally consists of some standard device INF entries, and many specific entries that provide Unimodem with information about the modem. This document is a complete list of the registry entries that can be added to the registry through the modem INF file.

These documents are located on 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.

Microsoft Money for Windows 95, version 4.0 or 4.0a
Under Windows NT, the Microsoft Money 95 application experiences problems with online banking and online stock quotes. This will be fixed in a future release of Money 95. Before you can dial out in Money95 using TAPI services on a computer running Windows NT Workstation, replace the Xsnpc.dll file in the system folder of MSMONEY with the Windows NT version 4.0 release of the Microsoft FAST Xs npc dll file dated March 29, 1996.
This file can be found at www.microsoft.com and will be included in the next release of Money 95.

Devices That Must be Manually Installed

The following devices must be manually installed—do not choose to have Windows NT automatically detect them.

- E-Tech Pocket Fax/Modem
- Multi-tech Multimodem (various models)
- Penril modems (various models)

Also, the Modems option in Control Panel closes when you attempt to query these devices.

Modems That Depend on Windows 95 Drivers
Some modems are configured differently than the traditional serial port modem or internal bus modem with an embedded serial port. They depend on special drivers written for Windows 95 or previous versions of Windows. Until these manufacturers provide comparable device drivers for Windows NT version 4.0, these modems do not work.

The two most common types are parallel port modems, and "Windows modems". The later are modems which move traditional modem hardware and firmware functions into Windows device drivers. Examples include the US Robotics Sportster WinModem, the IBM MWAVE modem, and the Intel Teladdin modem.

Users should consult the Hardware Compatibility List for the list of currently supported devices.

Modem Features Not Used in Windows NT version 4.0
Windows NT version 4.0 does not include built-in Group 3 FAX functionality, but support will be provided in a future release and by other software vendors.

Windows NT version 4.0 does not support the common voice modem functions which are supported by Unimodem/V in Windows 95. These may be supported in a future release. The Unimodem/V version in Windows 95 should not be used to upgrade to voice support in Windows NT version 4.0; they are incompatible.

Windows NT version 4.0 does not support VoiceView functionality or the Windows 95 file transfer application.

Modem Mis-detection
Windows NT version 4.0 attempts to recognize modems automatically. However, if it does not recognize a particular modem, the modem will be treated as a "standard modem." As a result, some of the features of the modem may be unusable. To work around this issue:

If the modem vendor provided an updated INF file on a disk, manually remove the previous entry, and retry modem installation using the **Have disk** option.

If there is no updated modem INF available, manually install the same modem or a similar modem by the same manufacturer.

If Internet access is available, an updated INF may be available from the manufacturer, or from www.microsoft.com. Copy the INF into the *systemroot*\inf folder, and retry the installation.

Removing and Reinstalling Modems
When you remove and re-install a modem, the modem response strings are not updated. This is a problem only if you have updated or modified the Modem.inf file.

Plug and Play ISA Modems
There are modems designed to plug into a PC ISA bus, which implement the Plug and Play ISA (PnP ISA) specification. Windows NT version 4.0 does not contain complete Windows 95 Plug and Play support. For additional information about the PnP ISA support provided in Windows

NT, see "Plug and Play ISA Device Installation and PNPISA.SYS" in the Readme.wri file. It contains descriptions about how to:

>Install the PNPISA Enabler software (PNPISA.SYS) if needed.
>Disable PNPISA.SYS
>Install PnP ISA devices
>Configure PnP ISA devices
>Remove PnP ISA devices

The sections that follow address modem-specific PnP ISA issues.

Duplicate Enumeration
If a PnP modem has already been installed and modem control panel autodetection is run again, perhaps to install additional modems, a duplicate modem of the same or different name may appear using the same com port of the modem control panel. In most cases this is not a problem. Both modem instances will function and either modem may be deleted. This is a known issue and will be fixed in a future release.

Multiple PnP ID Cards
Multiple PnP modems can be installed assuming computer resources are available.

Work Arounds and Known Issues
In the PNPISA Enabler, the first input/output range and IRQ listed in the **Resources** tab of the **Advanced Port Settings** dialog box may not be correct. This is merely the first available resource range which is suggested by the PnP card. If necessary, clear the **Use Automatic Settings** option and try various configuration ranges.

Complex multifunction cards which contain a modem, joystick and sound card are available in the marketplace. It may be difficult to install functionality for all devices within some of these cards. For example only the modem and joystick might be enabled, but the sound card portion left unusable due to existing resource conflicts or lack of driver support. Cancel installation for devices within these multifunction cards which cannot be used.

Some Sierra modems have two PnP IDs and will be enumerated twice by PNPISA.SYS. The first PnP detection event is usually the modem and can be installed correctly. The second PnP detection event may be for an audio dma channel which might not be needed or supported by Windows NT. This event can be dismissed or canceled to conserve computer resources.

Due to the resource ranges available to various ISAPNP cards, the sequence of installation may affect resource allocation. If it is difficult to install two or more ISAPNP cards, try installing them in a different order and restarting the computer.

If you continue to experience difficulty installing an ISAPNP card, free up unused resources on your computer and retry installation. A recommended method is to disable unused Com1 or Com2 ports by standard means (system BIOS, motherboard jumpers, I/O card jumpers) and then reattempt to install the ISAPNP card on the newly available resources.

If a modem appears to be installed but is not accessible by an application (eg, HyperTerminal or Dial-Up Networking) try restarting the computer a second time to complete installation, then retry the communications application.

If an ISAPNP modem seems unreliable after installation (drops characters or is unstable during communications settings) be sure to check that 16550 UART support is available for the com port which supports the modem.

ISAPNP Modems with Jumpers
ISAPNP modems are available (eg, US Robotics and other manufacturers) that can contain both legacy (non-PnP) and full ISAPNP personalities. If modem card jumpers are installed, the modem behaves as a legacy card with specific IRQ and com port addresses and has no

apparent PnP function. If board jumpers are removed, full ISAPNP functionality is enabled. If you experience difficulty installing, try removing jumpers to enable full ISAPNP. Alternatively, try using jumpers if PnP installation proves difficult, since the modem control panel autodetection method will usually detect legacy configured cards.

Multiple Modem Installation
It is possible to mix installations of modem profiles. PCMCIA, external and ISAPNP modems can all be used on the same computer, assuming adequate resources are available.

PnP support for Serenum, Parallel port and PCMCIA
This is not supported by PNPISA.SYS.

Services for Macintosh (SFM)

▪ Macintosh Service functionality is included in File Manager and is not part of Windows NT Explorer. File Manager is installed in the **Start** menu in the Programs/Administrative Tools folder when SFM is installed.

▪ If you disable the bindings for the AppleTalk protocol on a network adapter, after restarting the computer and re-enabling the bindings, the AppleTalk protocol will not start even though it appears to be enabled.

To enable the AppleTalk protocol bindings, in the Network icon in Control Panel, in the **Services** tab select **Services for Macintosh** and click **Properties**. When the popup appears that states: "Setup could not get the zone list...", click **Yes**, and then click **OK**.

In the Devices icon in Control Panel, select **AppleTalk Protocol** and click **Start**.

Then, in the Services icon in Control Panel, select **File Server for Macintosh** and **Print Server for Macintosh** and click **Start**.

Network Adapter Drivers
Microsoft provides network adapter drivers from third-party vendors on the Windows NT Workstation and Windows NT Server version 4.0 compact discs. These drivers, which are located in the \DRVLIB directory, have all met specific standards for installation and operation.

Plug and Play ISA Network Adapters
A Plug and Play ISA network card will be automatically detected by the PnP ISA enabler if the card runs in PnP mode. An Install dialog box is displayed after the **New Hardware Found** dialog box. If you install the driver from the network category, another message box advises you to install the drivers using the **Network** icon in Control Panel. If the adapter has not been installed before, turn off the Plug and Play mode before installing the driver. If the adapter has already been installed, skip the installation.
For more information about the Plug and Play ISA enabler, see "Plug and Play ISA Device Installation and PNPISA.SYS" in the Readme.wri file.

Network Adapter Drivers Notes
▪ Most PCI, EISA, and MCA adapters in the \DRVLIB directory can be detected and successfully installed during Setup. Most ISA and PCMCIA adapters are not detected but can be installed manually during setup.

▪ Some adapters may quit functioning if you upgrade from an earlier version to the Windows NT version 4.0 final release. This can be caused by changes in the registry, such as adapter

driver name changes, service dependency changes, or an obsolete network adapter driver. Removing the old driver and installing it again from the menu will fix the startup problem for adapters listed on the Hardware Compatibility List (HCL). Xircom IIPS and Eicon ISDN are examples of adapters that will have to be reinstalled.

• Some adapters generate errors during Setup because the configuration settings cannot be verified. This can be caused by conflicting settings for interrupt and I/O addresses.   The error can also be displayed if Setup calls an executable helper which sets up the configuration. If the adapter driver starts and connects to the network, the error can be ignored. If not, the error is an indication of resource conflicts which will have to be fixed. The Intel E100B and IBM Streamer adapters are examples of drivers that use their own executable setup routines.

• The original Intel EtherExpress PRO/100 EISA and PCI adapters (E100A) are not supported in this release. These adapters have been replaced by the E100B PCI model which is not available for the EISA bus.

• During Setup, selecting any Eicon WAN or the USR WAN (non-ISDN) adapters will result in a dialog box that cannot be exited. This will cause the installation to fail because rebooting is necessary to recover. This tradeoff was made to save several megabytes of disk space on the target machine during Setup. For these adapters, complete the installation and add the adapter later.
Microsoft does not recommend the use of 8-bit network adapters with Windows NT Workstation or Windows NT Server. Support for these adapters is included in some cases due to customer requirements, but older hardware represented by this technology does not provide good performance or reliability.

• PnP mode is not supported for network adapters. Network adapters that support PnP mode must be reconfigured with a software setup utility provided by the manufacturer. This includes some system board mounted network adapters, 3Com 3C509B, SMC 8416, IBM Auto TR, Madge PnP, and Eicon DIVA PRO.

• Bus-Master adapters are not supported on Motorola Power PC computers. The adapters include the Proteon p1390, p1392, p1392plus, and IBM 4/16 Token Ring Adapter II. IBM Power PC systems do support these adapters.

• If your PCMCIA adapter does not start or operates incorrectly, try using a different interrupt for the network adapter. Interrupts 2, 5, and 10 are often reserved on portable computers. In these cases, Microsoft recommends changing the interrupt to 3, 11, or 15. If the settings are changed during installation, the adapter will not start until installation is completed and the system is rebooted. If you know the settings presented by Setup will cause a conflict, you can change them, but the adapter will not start until installation is completed and the computer is rebooted. Additionally, during Express mode installation, if a conflicting interrupt is the default, the network will not start and the value will need to be changed manually after Setup completes. Rebooting an additional time will be necessary to start the PCMCIA adapter driver.

• If you install Windows NT version 4.0 from a network drive and you have both an Intel EtherExpress PRO/10P PCI LAN Adapter driver and a PCI SCSI controller installed, Setup may indicate one or more files are corrupt when it verifies the copy from the temporary directory to the %systemroot%\system32\drivers directory. This problem occurs because the network adapter is not reset correctly when Setup warm boots the computer. You can turn the computer off and then back on and Setup will restart and not encounter the problem.

• Use of the Socket EA PCMCIA Ethernet adapter BNC port is not supported.

• Digiboard PCIMAC and PCIMAC/4 ISDN adapters may not work correctly in some machines with PCI bridges.

• The Cisco C320 Series EISA FDDI adapters are not supported in this release.

▪ Two or more 3Com Etherlink MC/32 (3C527) microchannel adapters cannot start in the same machine.
Windows NT version 4.0 does not support PCI sub-vendor IDs. Detection of OEM adapters can result in a selection that does not match your installed adapter. The selection has been tested and works with the detected adapter and the installed driver. However, you can manually select the adapter from the menu to install a driver that is written specifically for that adapter.

▪ Very early Madge Bus Master PCI adapters are not supported. However, both current production Madge PCI adapters are supported. If you have an early Madge PCI adapter (with Altera components) please contact Madge for adapter replacements.

▪ For ISA adapters that can be detected, two identical adapters cannot be detected during Setup. The one with the lowest I\O address will be detected, but the others will not. However, they can be manually added. For multiprocessor systems, two identical ISA adapters may not be supported due to hardware limitations of the adapter. The NE2000 is an example of this limitation.

▪ Digital Equipment Corporation adapters that use the DC21X4.SYS driver have the following limitation in this release: the AUI or BNC ports will only operate if the Auto port selection is selected. Selecting BNC or AUI will cause those ports to work intermittently.

▪ The AM1500T.SYS driver is available to support early AMD PCnet ISA adapters and system boards versions. However, these early implementations can drop network connections during heavy stress generated by operations such as large file copies. The ISA and system board adapters are not recommended for servers, but may be adequate to continue using on workstations.

▪ On some Intergraph TD-1 workstations, during installation of Windows NT version 4.0, AMD 2100/1500T cards are not detected.   To work around this problem, select AMD 2100/1500T from list rather than having Setup detect the adapter. The correct settings are IRQ=5; DMA=5; I0=360.