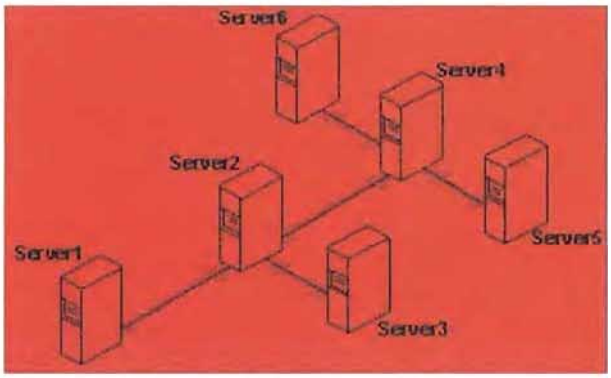
Configuring WINS Servers and Replication Partners

Configuring Replication Partners

WINS servers communicate among themselves to fully replicate their databases, ensuring that a name registered with one WINS server is eventually replicated to all other WINS servers within the internetwork. All mapping changes converge within the *replication period* for the entire WINS system, which is the maximum time for propagating changes to all WINS servers. All released names are propagated to all WINS servers after they become extinct, based on the interval specified in WINS Manager.

Replication is carried out among replication partners, rather than each server replicating to all other servers. In the following illustration, Server1 has only Server2 as a partner, but Server2 has three partners. So, for example, Server1 gets all replicated information from Server2, but Server2 gets information from Server1, Server3, and Server4.



Replication Configuration Example for WINS Servers

Ultimately, all replications are pulled from the other WINS servers on an internetwork, but triggers are sent by WINS servers to indicate when a replication should be pulled. To achieve replication, each WINS server is a push partner or pull partner with at least one other WINS server. A pull partner is a WINS server that pulls in database replicas from its push partner by requesting and then accepting replicas of new database entries in order to synchronize its own database. A push partner is a WINS server that sends notification of changes and then sends replicas to its pull partner upon receiving a request. When the server's pull partner replicates the information, it pulls replicas by asking for all records with a higher version number than the last record stored from the last replication for that server.

Choosing whether to configure another WINS server as a push partner or pull partner depends on several considerations, including the specific configuration of servers at your site, whether the partner is across a wide area network (WAN), and how important it is to propagate the changes.

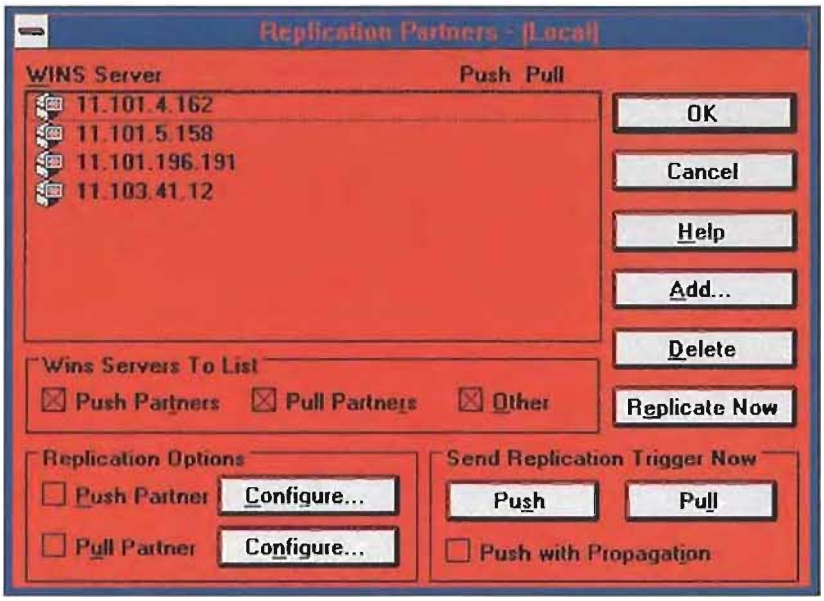
- If Server2, for example, needs to perform pull replications with ServerB, make sure it is a push partner of Server3.
- If Server2 needs to push replications to Server3, it should be a pull partner of WINS ServerB.

Replication is triggered when a WINS server polls another server to get a replica. This can begin at system startup and can also be at a specific time, and it can then repeat at the time interval specified for periodic replication. Replication is also triggered when a WINS server reaches a threshold set by the administrator, which is an *update count* for registrations and changes. In this case, the server notifies its pull partners that it has reached this threshold, and the other servers may then decide to pull replicas.

To add a replication partner for a WINS server

1. From the Server menu, choose the Replication Partners command.

   This command is available only if you are logged on as a member of the Administrators group for the local server.



2. In the Replication Partners dialog box, choose the Add button.

3. In the Add WINS Server dialog box, type the name or IP address of the WINS server that you want to add to the list, and then choose the OK button. If WINS Manager can find this server, it will add it to the WINS Server list in the Replication Partners dialog box.

4. From the WINS Server list in the Replication Partners dialog box, select the server you want to configure, and then complete the actions described in "Configuring Replication Partner Properties" later in this chapter.

5. If you want to limit which WINS servers are displayed in the Replication Partners dialog box, check or clear the options as follows:
   - Check Push Partners to display push partners for the current WINS server.
   - Check Pull Partners to display pull partners for the current WINS server.
   - Check Other to display the WINS servers that are neither push partners nor pull partners for the current WINS server.

6. To specify replication triggers for the partners you add, follow the procedures described in "Triggering Replication Between Partners" later in this chapter.

7. When you finish adding replication partners, choose the OK button.

To delete replication partners

1. From the Server menu, choose the Replication Partners command.

2. In the Replication Partners dialog box, select one or more servers in the WINS Server list, and then choose the Delete button, or press DEL.

   WINS Manager asks you to confirm the deletion if you checked the related confirmation option in the Preference dialog box, as described in "Setting Preferences for WINS Manager" later in this chapter.

Configuring Replication Partner Properties

When you designate replication partners, you need to specify parameters for when replication will begin.

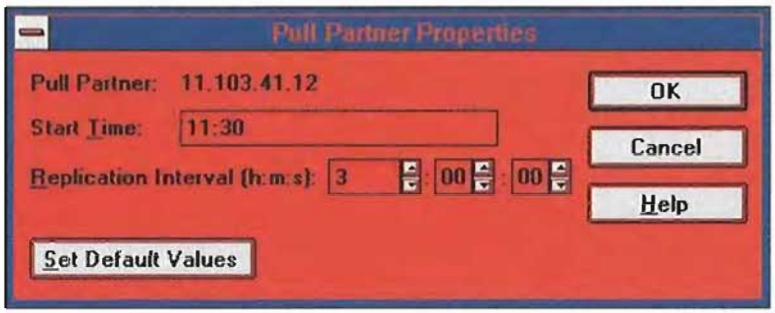
To configure replication partners for a WINS server

1. In the WINS Server list of the Replication Partners dialog box, select the server you want to configure.
2. Check either Push Partner or Pull Partner or both to indicate the replication partnership you want, and then choose the related Configure button.
3. Complete the entries in the appropriate Properties dialog box, as described in the following procedures.

To define pull partner properties

1. In the Start Time box of the Pull Partner Properties dialog box, type a time to indicate when replication should begin.

   You can use any separator for hours, minutes, and seconds. You can type AM or PM, for example, only if these designators are part of your time setting, as defined using the International option in Control Panel.



2. In the Replication Interval box, type a time in hours, minutes, and seconds to indicate how often replications will occur, or use the spin buttons to set the time you want.

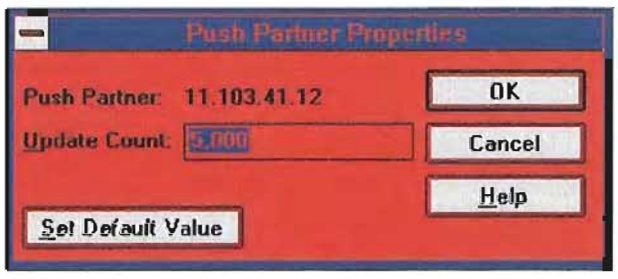
   If you want to return to the values specified in the Preferences dialog box, choose the Set Default Values button.

3. Choose the OK button to return to the Replication Partners dialog box.

To define push partner properties

1. In the Update Count box of the Push Partner Properties dialog box, type a number for how many additions and updates made to records in the database will result in changes that need replication. (Replications that have been pulled in from partners do not count as insertions or updates in this context.)

   The minimum value for Update Count is 5.



If you want to return to the value specified in the Preferences dialog box, choose the Set Default Values button.

2. Choose the OK button to return to the Replication Partners dialog box.

Triggering Replication Between Partners

You can also replicate the database between the partners immediately, rather than waiting for the start time or replication interval specified in the Preference dialog box, as described in "Setting Preferences for WINS Manager" later in this chapter.

You will probably want to begin replication immediately after you make a series of changes such as entering a range of static address mappings.

To send a replication trigger

- In the Replication Partners dialog box, select the WINS servers to which you want to send a replication trigger, and then choose the Push or Pull button, depending on whether you want to send the trigger to push partners or pull partners.

  Optionally, you can check the Push With Propagation box if you want the selected WINS server to propagate the trigger to all its pull partners.

  - If Push With Propagation is not checked, the selected WINS server will not propagate the trigger to its other partners.
  - If Push With Propagation is checked, the selected WINS server sends a propagate push trigger to its pull partners after it has pulled in the latest information from the source WINS server. If it does not need to pull in any replicas because it has the same or more up-to-date replicas than the source WINS server, it does not propagate the trigger to its pull partners.

To start replication immediately

- In the Replication Partners dialog box, choose the Replicate Now button.

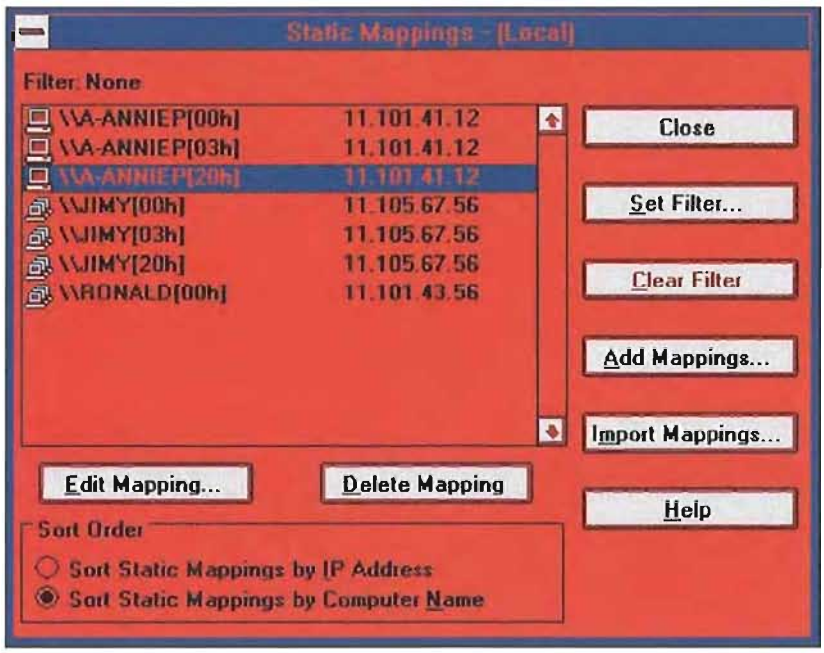
Managing Static Mappings

Static mappings are permanent lists of computer name-to-IP address mappings that cannot be challenged or removed, except when the administrator removes the specific mapping. You use the Static Mappings command in WINS Manager to add, edit, import, or delete static mappings for clients on the network that are not WINS enabled.

Important
If DHCP is also used on the network, a reserved (or static) IP address will override any WINS server settings. Static mappings should not be assigned to WINS-enabled computers.

To view static mappings

1. From the Mappings menu, choose the Static Mappings command.

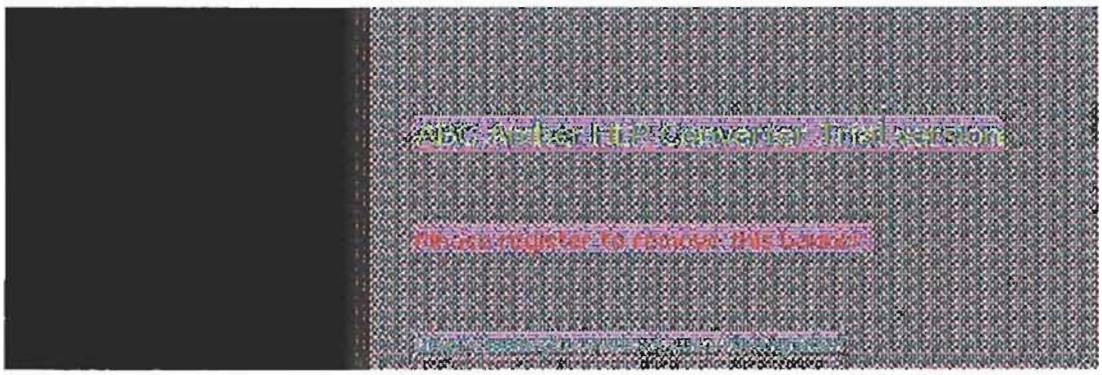


Caution
You cannot cancel changes made to the WINS database while working in the Static Mappings dialog box. You must manually delete any entries that are added in error or manually add back any entries that you mistakenly delete. This is because all changes to the WINS database made in this dialog box take effect immediately.

2. In the Static Mappings dialog box, select a Sort Order option, either by IP address or by computer name. This selection determines the order in which entries appear in the list of static mappings.
3. To edit or add a mapping, follow the procedures described in "Adding Static Mappings" and "Editing Static Mappings" later in this chapter.
4. To remove existing static mappings, select the mappings you want to delete from the list, and then choose the Delete Mapping button.

5. To limit the range of mappings displayed in the list of static mappings, choose the Set Filter button and follow the procedure in "Filtering the Range of Mappings" later in this chapter. To turn off filtering, choose the Clear Filter button.

6. When you finish viewing or changing the static mappings, choose the Close button.



Managing Static Mappings

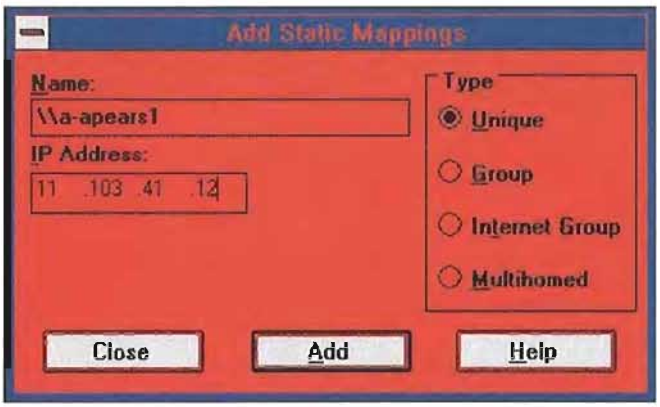
Adding Static Mappings

You can add static mappings to the WINS database for specific IP addresses using two methods:

- Type static mappings in a dialog box
- Import files that contain static mappings

To add static mappings to the WINS database by typing entries

1. In the Static Mappings dialog box, choose the Add Mappings button.



2. In the Name box of the Add Static Mappings dialog box, type the computer name of the system for which you are adding a static mapping. (If you want, you do not need to type two backslashes, because WINS Manager will add these for you.)

3. In the IP Address box, type the address for the computer.

   If Internet Group or Multihomed is selected as the Type option, the dialog box shows additional controls for adding multiple addresses. Use the down-arrow button to move the address you type into the list of addresses for the group. Use the up-arrow button to change the order of a selected address in the list.

4. Select a Type option to indicate whether this entry is a unique name or a kind of group with a special name, as described in the following list.

Type option	Meaning
Unique	Unique name in the database, with one address per name.
Group	Normal group, where addresses of individual members are not stored. The client broadcasts name packets to normal groups.
Internet group	Groups with NetBIOS names that have 0x1C as the 16th byte. An internet group stores up to 25 addresses for members. The maximum number of addresses is 25. For registrations after the 25th address, WINS overwrites a replica address or, if none is present, it overwrites the oldest registration.

Multihomed	Unique name that can have more than one address (multihomed computers). The maximum number of addresses is 25. For registrations after the 25th address, WINS overwrites a replica address or, if none is present, it overwrites the oldest registration.

Important
For internet group names defined in this dialog box (that is, added statically), make sure that the primary domain controller (PDC) for that domain is defined in the group if the PDC is running Windows NT Advanced Server version 3.1.

For more information, see "Managing Special Names" later in this chapter.

5. Choose the Add button.

   The mapping is immediately added to the database for that entry, and then the boxes are cleared so that you can add another entry.

6. Repeat this process for each static mapping you want to add to the database, and then choose the Close button.

Important
Because each static mapping is added to the database when you choose the Add button, you cannot cancel work in this dialog box. If you make a mistake in entering a name or address for a mapping, you must return to the Static Mappings dialog box and delete the mapping there.

You can also import entries for static mappings for unique and special group names from any file that has the same format as the LMHOSTS file (as described in Chapter 6, "Setting Up LMHOSTS"). Scope names and keywords other than #DOM are ignored. However, normal group and multihomed names can be added only by typing entries in the Add Static Mappings dialog box.

To import a file containing static mapping entries

1. In the Static Mappings dialog box, choose the Import Mappings button.

2. In the Select Static Mapping File dialog box, which is similar to the standard Windows NT Open dialog box, specify a filename for a static mappings file by typing its name in the box, or select one or more filenames in the list, and then choose the OK button to import the file.

The specified file is read, and a static mapping is created for each computer name and address. If the #DOM keyword is included for any record, an internet group is created (if it is not already present), and the address is added to that group.

Managing Static Mappings

Editing Static Mappings

You can change the IP addresses in static mappings owned by the WINS server you are currently administering.

To edit a static mapping entry

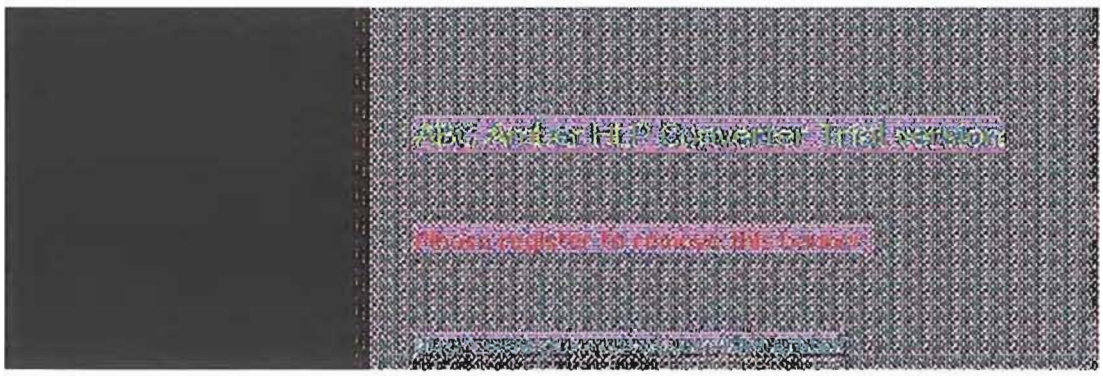
1. In the Static Mappings dialog box, select the mapping you want to change and choose the Edit Mapping button, or double-click the mapping entry in the list.

   You can view, but not edit, the Computer Name and Mapping Type option for the mapping in the Edit Static Mappings dialog box.

2. In the IP Address box, type a new address for the computer, and then choose the OK button.

   The change is made in the WINS database immediately.

Note
If you want to change the computer name or group type related to a specific IP address, you must delete the entry and redefine it in the Add Static Mappings dialog box.



Managing Static Mappings

Filtering the Range of Mappings

You may want to limit the range of IP addresses or computer names displayed in the Static Mappings or Show Database dialog boxes.

You can specify a portion of the computer name or IP address or both when filtering the list of mappings.

To filter mappings by address or name

1. In the dialog box for Static Mappings or Show Database, choose the Set Filter button.

2. In the Set Filter dialog box, type portions of the computer name, address, or both in the Computer Name or IP Address boxes.

   You can use the asterisk (*) wildcard for portions of the name or address or both. For example, you could type **\\acct*** to filter all computers with names that begin with **acct**. However, for the address, a wildcard can be used only for a complete octet. That is, you can type **11.101.*.***, but you cannot enter **11.1***.1.1 in these boxes.

3. Choose the OK button.

   The selected range is displayed in the Static Mappings or Show Database dialog box. The filtered range will remain until you clear the filter.

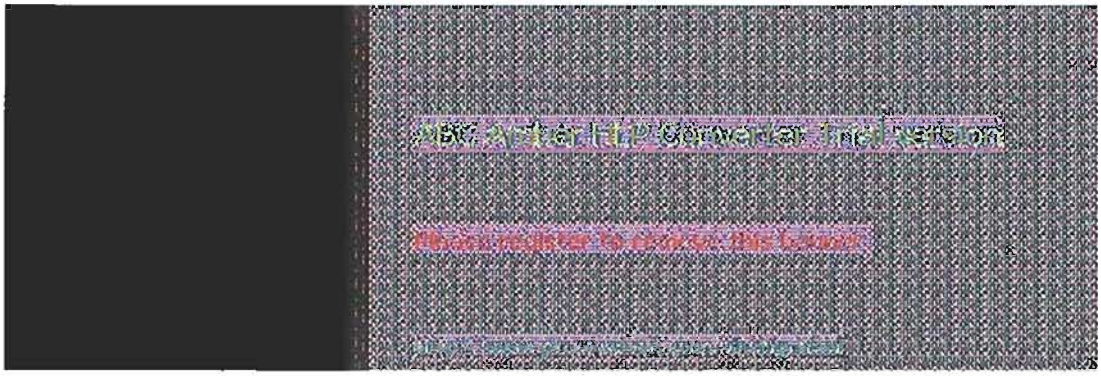
   A message will tell you if no mappings are found to match the range you specified, and the list of mappings will be empty.

If a filter is in effect for the range of mappings, the Clear Filter button is available for restoring the entire list.

To clear the filtered range of mappings

- In the Static Mappings or Show Database dialog box, choose the Clear Filter button.

  The list now shows all mappings found in the database.



Managing Static Mappings

Managing Special Names

WINS recognizes special names for several types of groups, including a normal group, multihomed, and internet group. This section describes these groups and presents some background details to help you understand how WINS manages these groups.

Normal Group Names

A group name does not have an address associated with it. It can be valid on any subnet and can be registered with more than one WINS server. A group's timestamp shows the last time for any change received for the group. If the WINS server receives a query for the group name, it returns FFFFFFFF (the limited broadcast address). The client then broadcasts on the subnet. The group name is renewed when any member of the group renews the group name.

Multihomed Names

A multihomed name is a single, unique name storing multiple addresses. A multihomed device is a computer with multiple network cards and/or multiple IP addresses bound to NetBIOS over TCP/IP. A multihomed device with multiple IP addresses can register one or more addresses by sending one address at a time in a special name registration packet. A multihomed name in a WINS database can have one or more addresses. The timestamp for the record reflects any changes made for any members of the name.

Each multihomed group name can contain a maximum of 25 IP addresses.

When you configure TCP/IP manually on a Windows NT computer, you use the Advanced Microsoft TCP/IP dialog box to specify the IP address and other information for each adapter on a multihomed computer.

Internet Group Names

The internet group name is read as configuration data. When dynamic name registrations for internet groups are received, the actual address (rather than the subnet broadcast address) is stored in the group with a timestamp and the owner ID, which indicates the WINS server registering that address.

The internet group name (which has a 16th byte ending in 0x1C reserved for domain names, as described in the following section) can contain a maximum of 25 IP addresses for primary and backup domain controllers in a domain. Dynamically registered names are added if the list is not static and has fewer than 25 members. If the list has 25 members, WINS removes a replica member (that is, a member registered by another WINS server) and adds the new member. If all members are owned by this WINS server, the oldest member is replaced by the new one.

WINS gives precedence over remote members to members in an internet group name that registered with it. This preference means that the group name always contains the geographically closest Windows NT Server computers. To establish the preference of members of internet groups registered with other WINS servers under the \Partners\Pull key in the Registry, a precedence is assigned for each WINS partner as a value of the **MemberPrec** Registry parameter. Preference should be given to WINS servers near the WINS server you are configuring. For more information about the value of this parameter, see its entry in "Advanced Configuration Parameters for WINS" later in this chapter.

The internet group name is handled specially by WINS, which returns the 24 closest Windows NT Server computers in the domain, plus the domain controller. The name ending in 1C is also used to discover a Windows NT Server computer in a domain when a computer running Windows NT Workstation or Windows NT Server needs a server for pass-through authentication.

If your network still has domain controllers running Windows NT Advanced Server version 3.1 to be included in the internet group name, you must add these to the group manually using WINS Manager. When you manually add such a computer to the internet group name, the list becomes static and no longer accepts dynamic updates from WINS-enabled computers.

For information about related issues in LMHOSTS for #DOM entries, see "Designating Domain Controllers Using #DOM" in Chapter 6, "Setting Up LMHOSTS."

How WINS Handles Special Names

Special names are indicated by a 16th byte appended to the computer name or domain name. The following table shows some special names that can be defined for static entries in the Add Static Mappings dialog box.

Special Names for Static Mappings

Name ending	Usage	How WINS handles queries
0x1E	A normal group. Browsers broadcast to this name and listen on it to elect a master browser. The broadcast is done on the local subnet and should not cross routers.	WINS always returns the limited broadcast address (FFFFFFFF).
0x1D	Clients resolve this name to access the master browser for server lists. There is one master browser on a subnet.	WINS always returns a negative response. If the node is h-node or m-node, the client broadcasts a name query to resolve the name. For registrations, WINS returns a positive response even though the names are not put into the database.
0x1C	The internet group name, which contains a list of the specific addresses of systems that have registered the name. The domain controller registers this name.	WINS treats this as an internet group, where each member of the group must renew its name individually or be released. The internet group is limited to 25 names. (Note, however, that there is no limit for #DOM entries in LMHOSTS.) WINS returns a positive response for a dynamic registration of a static 1C name, but the address is not added to the list. When a static 1C name is replicated that clashes with a dynamic 1C name on another WINS server, a union of the members is added, and the record is marked as static.

The following illustrates a sample NetBIOS name table for a Windows NT Server domain controller, such as the list that appears if you type **nbtstat -n** at the command prompt. This table shows the 16th byte for special names, plus the type (unique or group).

NetBIOS Local Name Table

Name		Type	Status
<0C29870B>		UNIQUE	Registered
ANNIEPS	<20>	UNIQUE	Registered
ANNIEPS	<00>	UNIQUE	Registered
ANNIEPDOM	<00>	GROUP	Registered
ANNIEPDOM	<1C>	GROUP	Registered

ANNIEPDOM	<1B>	UNIQUE	Registered
ANNIEPS	<03>	UNIQUE	Registered
ANNIEPS	<1E>	GROUP	Registered
ANNIEPS	<1D>	UNIQUE	Registered
.._MSBROWSE<01>		GROUP	Registered

Example NetBIOS Name Table for a Windows NT Domain Controller

As shown in this example, several special names are identified for both the computer and the domain. These special names include the following:

- 0x0 (shown as <00> in the example), the redirector name, which is used with **net view**.
- 0x3, the Messenger service name for sending messages.
- _MSBROWSE_, the name master browsers broadcast to on the local subnet to announce their domains to other master browsers. WINS handles this name by returning the broadcast address FFFFFFFF.
- 0x1B, the domain master browser name, which clients and browsers use to contact the domain master browser. A domain master browser gets the names of all domain master browsers. When WINS is queried for the domain master browser name, it handles the query like any other name query and returns its address.

  WINS assumes that the computer that registers a domain name with the 1B character is the domain controller. This name is registered by the browser running on the domain controller. This ensures that the domain controller is in the internet group name list that is returned when a 1C name is queried, for which WINS always returns the address of the 1B name along with the members of a 1C name.

Setting Preferences for WINS Manager

You can configure several options for administration of WINS servers. The commands for controlling preferences are on the Options menu.

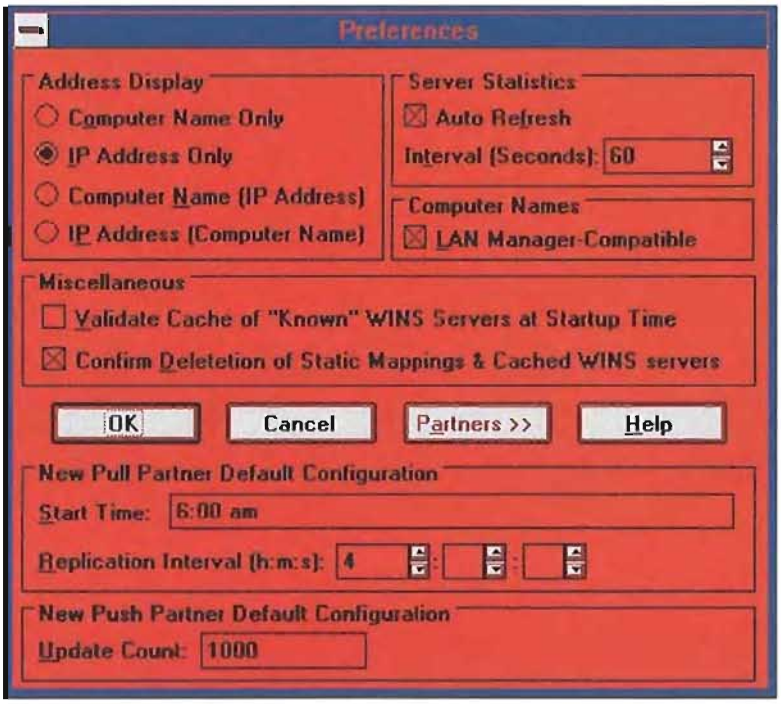
To display the status bar for help on commands

- From the Options menu, choose the Status Bar command.

  When this command is active, its name is checked on the menu, and the status bar at the bottom of the WINS Manager window displays descriptions of commands as they are highlighted in the menu bar.

To set preferences for WINS Manager

1. From the Options menu, choose the Preferences command.
2. To see all the available preferences, choose the Partners button in the Preferences dialog box.



3. Select an Address Display option to indicate how you want address information to be displayed throughout WINS Manager-as computer name, IP address, or an ordered combination of both.

   Note
   Remember that the kind of address display affects how a connection is made to the WINS server - for IP addresses, the connection is made via TCP/IP; for computer names, the connection is made via named pipes.

4. Check Auto Refresh if you want the statistics in the WINS Manager window to be refreshed automatically. Then enter a number in the Interval box to specify the number of seconds

between refresh actions.

WINS Manager also refreshes the statistical display automatically each time an action is initiated while you are working in WINS Manager.

5. Check the LAN Manager-Compatible check box if you want computer names to adhere to the LAN Manager naming convention.

   LAN Manager computer names are limited to 15 characters, as opposed to 16-character NetBIOS names used by some other sources, such as Lotus Notes®. In LAN Manager names, the 16th byte is used to indicate whether the device is a server, workstation, messenger, and so on. When this option is checked, WINS adds and imports static mappings with 0, 0x03, and 0x20 as the 16th byte.

   All Windows networking, including Windows NT, follows the LAN Manager convention. So this box should be checked unless your network accepts NetBIOS name from other sources.

6. Check Validate Cache Of Known WINS Servers At Startup Time if you want the system to query the list of servers each time the system starts to find out if each server is available.

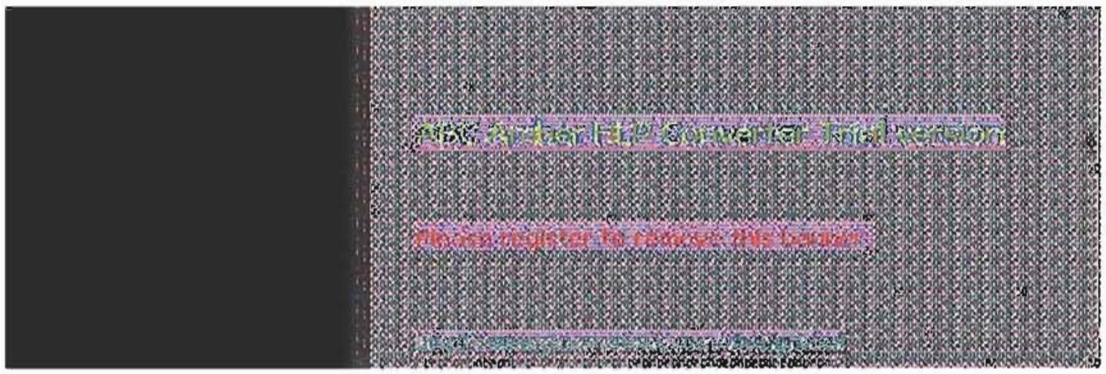
7. If you want a warning message to appear each time you delete a static mapping or the cached name of a WINS server, check the Confirm Deletion Of Static Mappings And Cached WINS Servers option.

8. In the Start Time box, type a time to specify the default for replication start time for new pull partners. Then specify values for the Replication Interval to indicate how often data replicas will be exchanged between the partners.

   The minimum value for the Replication Interval is 40 minutes.

9. In the Update Count box, type a number to specify a default for how many registrations and changes can occur locally before a replication trigger is sent by this server when it is a push partner. The minimum value is 5.

10. When all options are set for your preferences, choose the OK button.



Managing the WINS Database

The following files are stored in the *systemroot*\SYSTEM32\WINS directory that is created when you set up a WINS server:

- JET.LOG is a log of all transactions done with the database. This file is used by WINS to recover data if necessary.
- SYSTEM.MDB is used by WINS for holding information about the structure of its database.
- WINS.MDB is the WINS database file.
- WINSTMP.MDB is a temporary file that WINS creates. This file may remain in the \WINS directory after a crash.

You should back up these files when you back up other files on the WINS server.

Caution
The JET.LOG, SYSTEM.MDB, WINS.MDB, and WINSTMP.MDB files should not be removed or tampered with in any manner.

Like any database, the WINS database of address mappings needs to be cleaned and backed up periodically. WINS Manager provides the tools you need for maintaining the database. This section describes how to scavenge (clean), view, and back up the database. For information on restoring and moving the WINS database, see "Troubleshooting WINS" later in this chapter.

Managing the WINS Database

Scavenging the Database

The local WINS database should periodically be cleared of released entries and old entries that were registered at another WINS server but did not get removed from this WINS database for some reason. This process, called scavenging, is done automatically over intervals defined by the relationship between the Renewal and Extinct intervals defined in the Configuration dialog box. You can also clean the database manually.

For example, if you want to verify old replicas immediately instead of waiting the time interval specified for verification, you can manually scavenge the database.

To scavenge the WINS database

- From the Mappings menu, choose the Initiate Scavenging command.

The database is cleaned, with the results as shown in the following table.

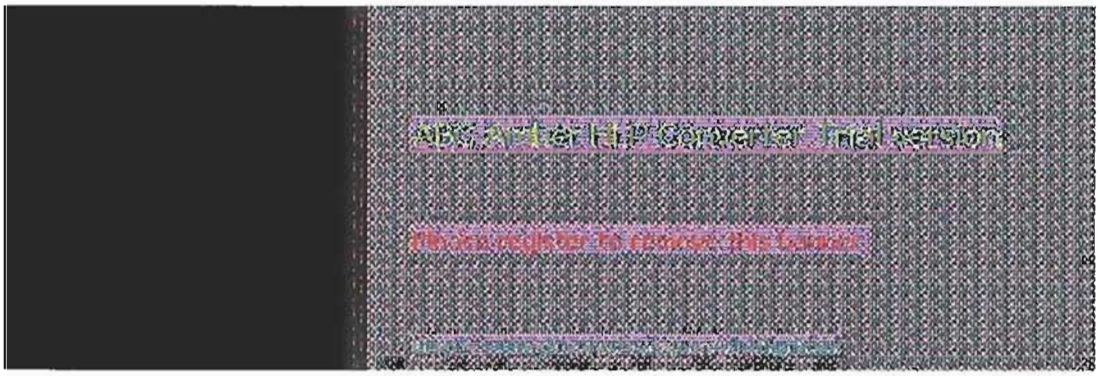
State before scavenging	State after scavenging
Owned active names for which the Renewal interval has expired	Marked *released*
Owned released name for which the Extinct interval has expired	Marked *extinct*
Owned extinct names for which the Extinct timeout has expired	Deleted
Replicas of extinct names for which the Extinct timeout has expired	Deleted
Replicas of active names for which the Verify interval has expired	Revalidated
Replicas of extinct or deleted names	Deleted

For information about the intervals and timeouts that govern database scavenging, see "Configuring WINS Servers" earlier in this chapter.

After WINS has been running for a while, the database may need to be compacted to improve WINS performance.

To compact the WINS database

1. At the WINS server, stop the Windows Internet Name Service using the Control Panel Services option or by typing **net stop wins** at the command prompt.
2. Run COMPACT.EXE (which is found in the *\systemroot*\SYSTEM32 directory).
3. Restart the Windows Internet Name Service on the WINS server.



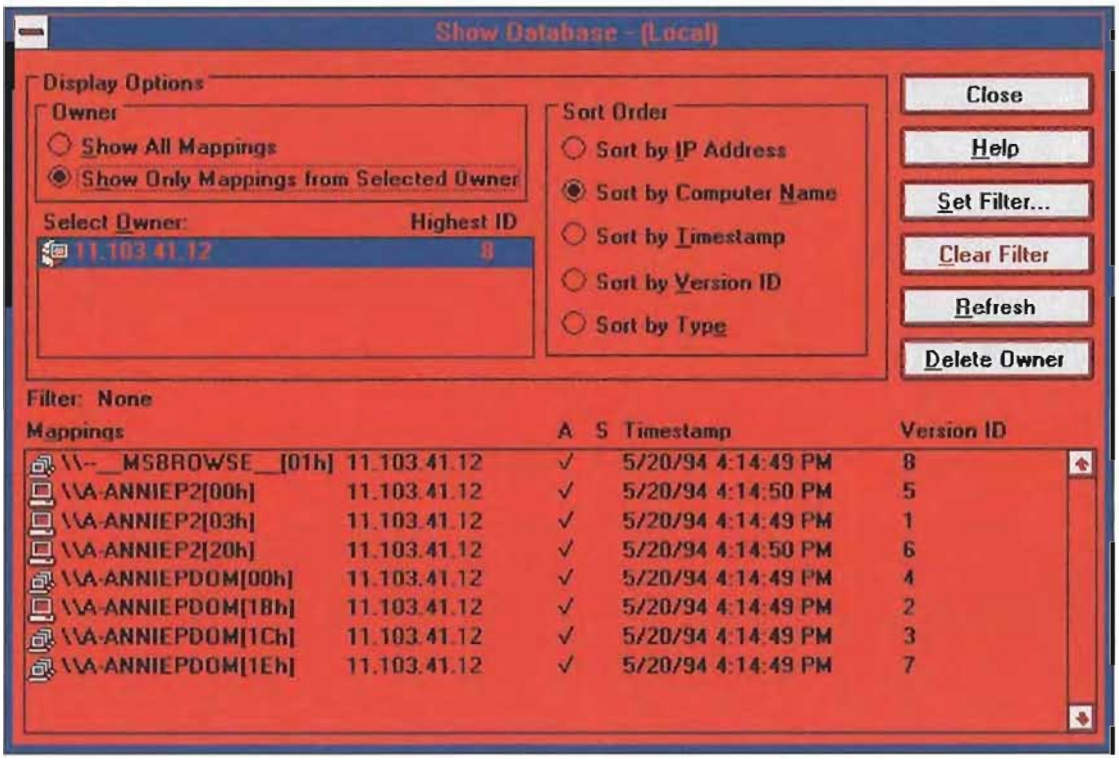
Managing the WINS Database

Viewing the WINS Database

You can view the actual active and static mappings stored in the WINS database, based on the WINS server that owns the entries.

To view the WINS database

1. From the Mappings menu, choose the Show Database command.



2. In the Show Database dialog box, to view the mappings in the database for a specific WINS server, select Show Only Mappings From Specific Owner, and then from the Select Owner list, select the WINS server whose database you want to view.

   By default, the Show Database dialog box shows all mappings for the WINS database on the currently selected WINS server.

3. Select a Sort Order option to sort by IP address, computer name, timestamp for the mapping, version ID, or type. (For information about types, see "Adding Static Mappings" earlier in this chapter.)

4. If you want to view only a range of mappings, choose the Set Filter button and follow the procedures described in "Filtering the Range of Mappings" earlier in this chapter. To turn off filtering, choose the Clear Filter button.

5. Use the scroll bars in the Mappings box to view entries in the database. Then choose the

Close button when you are finished viewing.

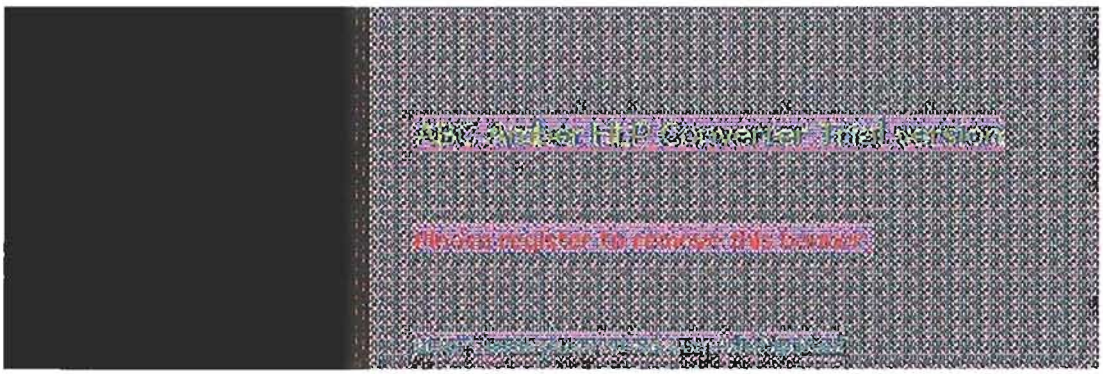
As shown in the Mappings list, each registration record in the WINS database includes these elements:

Item	Meaning
	Unique
	Group, internet group, or multihomed
Computer name	The NetBIOS computer name.
IP address	The assigned Internet Protocol address.
A or S	Whether the mapping is active (dynamic) or static.
Timestamp	Shows when the record was registered or updated. When a replica is stored in the database, its timestamp is set to the current time on the receiving WINS server.
Version ID	A unique hexadecimal number assigned by the WINS server during name registration, which is used by the server's pull partner during replication to find new records.

You can also use the Show Database dialog box to remove all references to a specific WINS server in the database, including all database entries owned by the WINS server.

To delete a specific WINS server's entries in the database

- In the Show Database dialog box, select a WINS server in the Select Owner list, and then choose the Delete Owner button.



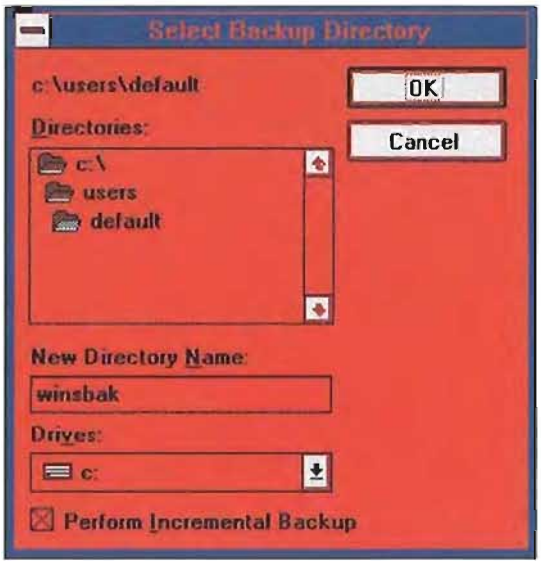
Managing the WINS Database

Backing Up the Database

WINS Manager provides backup tools so that you can back up the WINS database. After you specify a backup directory for the database, WINS performs complete database backups every 24 hours, using the specified directory.

To back up a WINS database

1. From the Mappings menu, choose the Backup Database command.



2. In the Select Backup Directory dialog box, specify the location for saving the backup files.

   Windows NT proposes a subdirectory of the \WINS directory. You can accept this proposed directory. The most secure location is to back up the database on another hard disk. Do not back up to a network drive, because WINS Manager cannot restore from a network source.

3. If you want to back up only the newest version numbers in the database (that is, changes that have occurred since the last backup), check Perform Incremental Backup.

   Note
   You must have performed a complete backup before this option can be used successfully.

4. Choose the OK button.

You should also periodically back up the Registry entries for the WINS server.

To back up the WINS Registry entries

1. Run REGEDT32.EXE.
2. In Registry Editor, select the HKEY_LOCAL_MACHINE window, and then select this key:
   ..SYSTEM\CurrentControlSet\Services\WINS

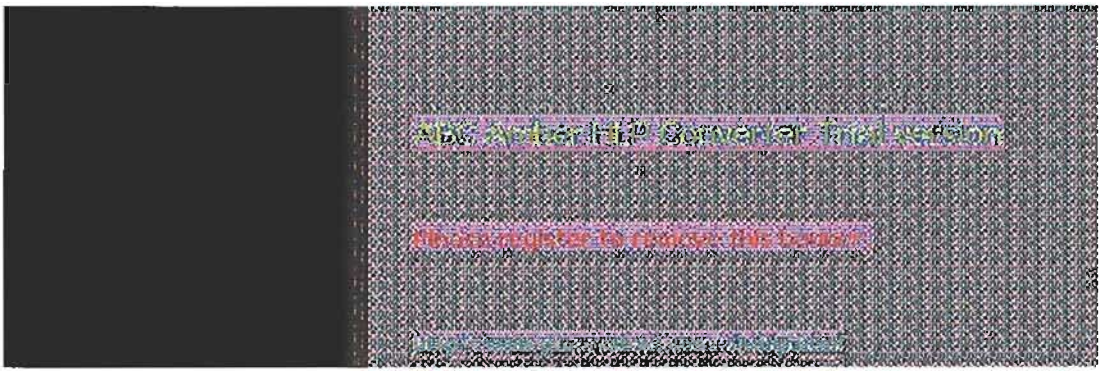
3. From the Registry menu, choose Save Key.

4. In the Save Key dialog box, specify the path where you store backup versions of the WINS database files.

For information about restoring the WINS database, see the following section, "Troubleshooting WINS."

Troubleshooting WINS

This section describes some basic troublesnooting steps for common problems and also describes how to restore or rebuild the WINS database.



Troubleshooting WINS

Basic WINS Troubleshooting

These error conditions can indicate potential problems with the WINS server:

- The administrator can't connect to a WINS server using WINS Manager. The message that appears might be, "The RPC server is unavailable."
- The WINS Client service or Windows Internet Name Service may be down and cannot be restarted.

The first troubleshooting task is to make sure the appropriate services are running.

To ensure the WINS services are running

1. Use the Services option in Control Panel to verify that the WINS services are running.

   In the Services dialog box for the client computer, Started should appear in the Status column for the WINS Client service. For the WINS server itself, Started should appear in the Status column for the Windows Internet Name Service.

2. If a necessary service is not started on either computer, start the service.

The following describes solutions to common WINS problems.

To locate the source of "duplicate name" error messages

- Check the WINS database for the name. If there is a static record, remove it from the database of the primary WINS server.

  Or

  Set the value of **MigrateOn** in the Registry to 1, so the static records in the database can be updated by dynamic registrations (after WINS successfully challenges the old address).

To locate the source of "network path not found" error messages on a WINS client

- Check the WINS database for the name. If the name is not present in the database, check whether the computer uses b-node name resolution. If so, add a static mapping for it in the WINS database.

  If the computer is configured as a p-node, m-node, or h-node and if its IP address is different from the one in the WINS database, then it may be that its address changed recently and the new address has not yet replicated to the local WINS server. To get the latest records, ask the WINS server that registered the address to perform a push replication with propagation to the local WINS server.

To discover why a WINS server cannot pull or push replications to another WINS server

1. Confirm that the router is working.

2. Ensure that each server is correctly configured as either a pull or push partner:

- If ServerA needs to perform pull replications with ServerB, make sure it is a push partner of ServerB.
- If ServerA needs to push replications to ServerB, it should be a pull partner of WINS ServerB.

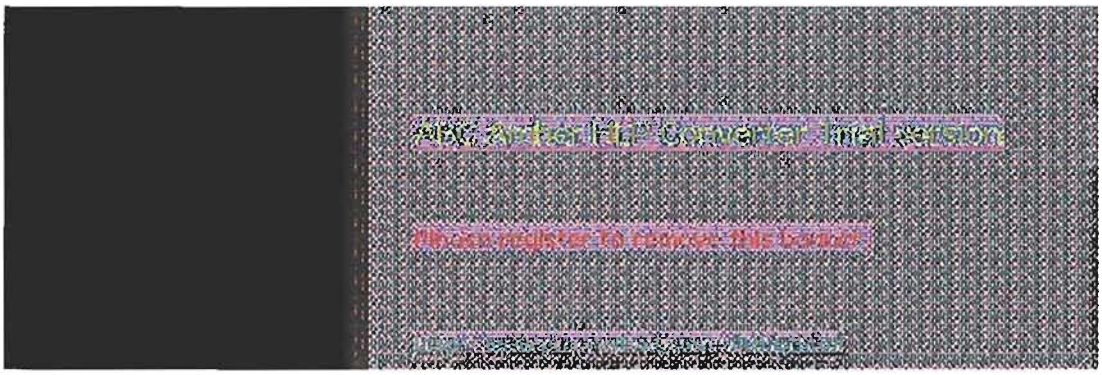
  To determine the configuration of a replication partner, check the values under the \Pull and \Push keys in the Registry, as described in "Advanced Configuration Parameters for WINS"

later in this chapter.

To determine why WINS backup is failing consistently

- Make sure the path for the WINS backup directory is on a local disk on the WINS server.

  WINS cannot back up its database files to a remote drive.



Troubleshooting WINS

Restoring or Moving the WINS Database

This section describes how to restore, rebuild, or move the WINS database.

Restoring a WINS Database

If you have determined that the Windows Internet Name Service is running on the WINS server, but you cannot connect to the server using WINS Manager, then the WINS database is not available or has becomes corrupted. If a WINS server fails for any reason, you can restore the database from a backup copy.

You can use the menu commands to restore the WINS database or restore it manually.

To restore a WINS database using menu commands

1. From the Mappings menu, choose the Restore Database command.
2. In the Select Directory To Restore From dialog box, select the location where the backup files are stored, and then choose the OK button.

To restore a WINS database manually

1. In the *\systemroot*\SYSTEM32\WINS directory, delete the JET.LOG, JET*.LOG, WINS.TMP, and SYSTEM.MDB files.
2. From the Windows NT Server installation source, copy SYSTEM.MDB on the WINS server. The installation source can be the Windows NT Server compact disc, the installation floppy disks, or a network directory that contains the master files for Windows NT Server.
3. Copy an uncorrupted backup version of WINS.MDB to the *\systemroot*\SYSTEM32\WINS directory.
4. Restart the Windows Internet Name Service on the WINS server.

Restarting and Rebuilding a Down WINS Server

In rare circumstances, the WINS server may not boot or a STOP error may occur. If the WINS server is down, follow these steps to restart

To restart a WINS server that is down

1. Turn off the power to the server and wait one minute.
2. Turn on the power, start Windows NT Server, and logon under an account with Administrator rights.
3. At the command prompt, type **net start wins** and press Enter.

If the hardware for the WINS server is malfunctioning or other problems prevent you from running Windows NT, you will have to rebuild the WINS database on another computer.

To rebuild a WINS server

1. If you can start the original WINS server using MS-DOS, use MS-DOS to make backup copies of the files in the *\systemroot*\SYSTEM32\WINS directory. If you cannot start the computer with MS-DOS, you will have to use the last backup version of the WINS database files.

2. Install Windows NT Server and Microsoft TCP/IP to create a new WINS server using the same hard drive location and *systemroot* directory. That is, if the original server stored the WINS files on C:\WINNT35\SYSTEM32\WINS, then the new WINS server should use this same path to the WINS files.

3. Make sure the WINS services on the new server are stopped, and then use Registry Editor to restore the WINS keys from backup files

4. Copy the WINS backup files to the *systemroot*\SYSTEM32\WINS directory.

5. Restart the new, rebuilt WINS server.

Moving the WINS Database

You may find a situation where you need to move a WINS database to another computer. To do this, follow these steps.

To move a WINS database

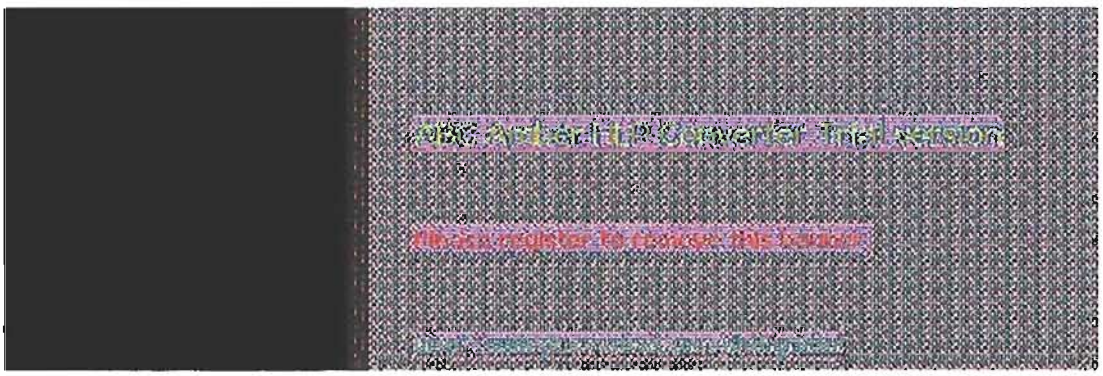
1. Stop the Windows Internet Name Service on the current computer.

2. Copy the \SYSTEM32\WINS directory to the new computer that has been configured as a WINS server.

   Make sure the new directory is under exactly the same drive letter and path as on the old computer.

   If you must copy the files to a different directory, copy WINS.MDB, but not SYSTEM.MDB. Use the version of SYSTEM.MDB created for that new computer.

3. Start the Windows Internet Name Service on the new computer. WINS will automatically use the .MDB and .LOG files copied from the old computer.



Advanced Configuration Parameters for WINS

This section presents configuration parameters that affect the behavior of WINS and that can be modified only through Registry Editor. For some parameters, WINS can detect Registry changes immediately. For other parameters, you must restart the Windows Internet Name Service for the changes to take effect.

Caution
You can impair or disable Windows NT if you make incorrect changes in the Registry while using Registry Editor. Whenever possible, use WINS Manager to make configuration changes, rather than using Registry Editor. If you make errors while changing values with Registry Editor, you will not be warned, because Registry Editor does not recognize semantic errors.

To make changes to WINS configuration using Registry Editor

1. Run REGEDT32.EXE from File Manager or Program Manager, or at a command prompt, type **start regedt32** and press ENTER.

   When the Registry Editor window appears, you can press F1 to get Help on how to make changes in Registry Editor.

2. In Registry Editor, click the window titled HKEY_LOCAL_MACHINE On Local Machine, and then click the icons for the SYSTEM subtree until you reach the appropriate subkey, as described later in this section.

The following describes the value entries for WINS parameters that can only be set by adding an entry or changing values in Registry Editor.

Advanced Configuration Parameters for WINS

Registry Parameters for WINS Servers

The Registry parameters for WINS servers are specified under the following key:

..\SYSTEM\CurrentControlSet\Services\Wins\Parameters

This subkey lists all the nonreplication-related parameters needed to configure a WINS server. It also contains a \Datafiles subkey, which lists all the files that should be read by WINS to initialize or reinitialize its local database.

DbFileNm

Data type = REG_EXPAND_SZ
Range = *path name*
Default = %SystemRoot%\system32\wins\wins.mdb

Specifies the full path name for the WINS database file.

DoStaticDataInit

Data type = REG_DWORD
Range = 0 or 1
Default = 0 (false-that is, the WINS server does not initialize its database)

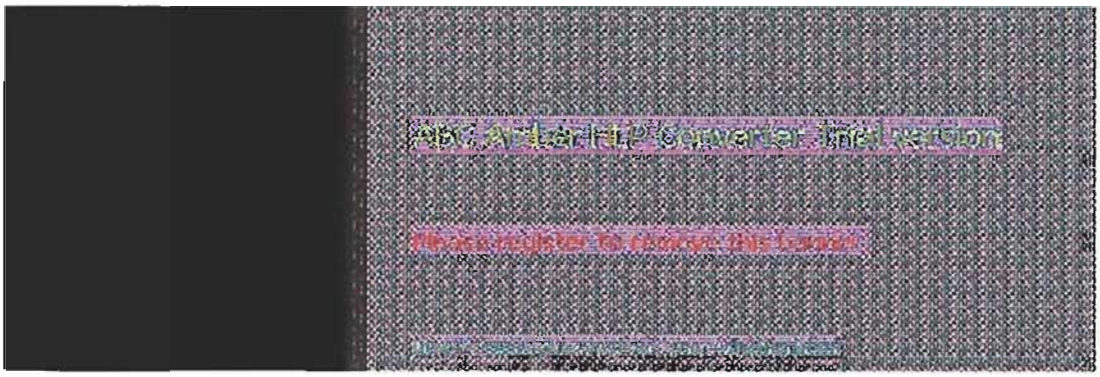
If this parameter is set to a non-zero value, the WINS server will initialize its database with records listed in one or more files listed under the \Datafiles subkey. The initialization is done at process invocation and whenever a change is made to one or more values of the \Parameters or \Datafiles keys (unless the change is to change the value of **DoStaticDataInit** to 0).

The following parameters in this subkey can be set using the options available in the WINS Server Configuration dialog box:

LogDetailedEvents
LogFilePath
LoggingOn
RefreshInterval
RplOnlyWCnfPnrs
TombstoneInterval (extinction interval)
TombstoneTimeout (extinction timeout)
VerifyInterval

Also, the \Wins\Parameters\Datafiles key lists one or more files that the WINS server should read to initialize or reinitialize its local database with static records. If the full path of the file is not listed, the directory of execution for the WINS server is assumed to contain the data file. The parameters can have any names (for example, DF1 or DF2). Their data types must be REG_SZ or REG_EXPAND_SZ.

Important
The \Wins\Performance key contains values used for WINS performance counters that can be viewed in Performance Monitor. These values should be maintained by the system, so do not change these values.


PDF Artist HTML Converter trial version

Advanced Configuration Parameters for WINS

Registry Parameters for Replication Partners

The \Wins\Partners key has two subkeys, \Pull and \Push, under which are subkeys for the IP addresses of all push and pull partners, respectively, of the WINS server.

Parameters for Push Partners

A push partner, listed under the \Partners\Pull key, is one from which a WINS server pulls replicas and from which it can expect update notification messages. The following parameter appears under the IP address for a specific push partner. This parameter can be set only by changing the value in Registry Editor:

MemberPrec

Data type = REG_DWORD
Range = 0 or 1
Default = None

Specifies the order of precedence for this WINS partner. 0 indicates low precedence, and 1 indicates high precedence. Notice that dynamically registered names are always high precedence. When a 1C name is pulled from this WINS partner, the addresses contained in it are given this precedence level. The value can be 0 (low) or 1 (high). Set this value to 1 if this WINS server is serving a geographic location that is nearby.

The following parameters appear under this subkey and can be set in the WINS Server Configuration dialog box:

..\SYSTEM\CurrentControlSet\Services\Wins\Partners\Pull

InitTimeReplication CommRetryCount

The following parameters appear under this subkey and can be set using the Preferences dialog box:

..\SYSTEM\CurrentControlSet\Services\Wins\Partners\Pull\<Ip Address>

SpTime (Start Time for pull partner default configuration)**TimeInterval** (Replication Interval)

For **SpTime**, WINS replicates at the set time if it is in the future for that day. After that, it replicates every number of seconds specified by **TimeInterval**. If **SpTime** is in the past for that day, WINS replicates every number of seconds specified by **TimeInterval**, starting from the current time (if **InitTimeReplication** is set to 1).

Parameters for Pull Partners

A pull partner of a WINS server, listed under the \Partners\Push key, is one from which it can expect pull requests to pull replicas and to which it sends update notification messages. The following parameters appear under this subkey and can be set using the options available in the WINS Server Configuration dialog box:

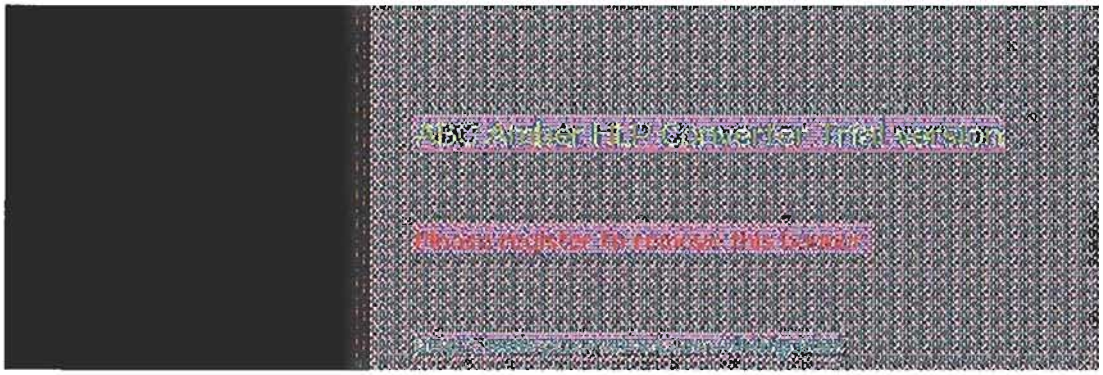
..\SYSTEM\CurrentControlSet\Services\Wins\Partners\Push

InitTimeReplicationRplOnAddressChg

The following parameter appears under this subkey and can be set using the options available in the Preferences dialog box:

..\SYSTEM\CurrentControlSet\Services\Wins\Partners\Push\<Ip Address>

UpdateCount



Planning a Strategy for WINS Servers

The planning issues for implementing WINS servers are similar to those for implementing DHCP servers, as described in Chapter 4, "Installing and Configuring DHCP Servers." Most network administrators will be installing both kinds of servers, so the planning and implementation tasks will be undertaken jointly for DHCP and WINS servers.

This section provides some additional planning issues for WINS servers.

Planning a Strategy for WINS Servers

Planning for Server Performance

A WINS server can typically service 1500 name registrations per minute and about 760 queries per minute. There is no built-in limit to the number of records that a WINS server can replicate or store.

Based on these numbers, and planning for large-scale power outage where many computers will come on line simultaneously, the conservative recommendation is that you plan to include one WINS server and a backup server for every 10,000 computers on the network.

Two factors can particularly enhance WINS server performance. WINS performance increases almost 25 percent on a computer with two processors. Also, using NTFS as the file system also improves performance.

After you establish WINS servers in the internetwork, you can adjust the Renewal interval. Setting this interval to reduce the numbers of registrations can help tune server response time. (The Renewal interval is specified in the WINS Server Configuration dialog box.)

Planning a Strategy for WINS Servers

Planning Replication Partners and Proxies

In one possible configuration, one WINS server can be designated as the central server, and all other WINS servers can be configured as both push partner and pull partner of this central server. Such a configuration ensures that the WINS database on each server contains addresses for every node on the WAN.

Another option is to set up a chain of WINS servers, where each server is both the push partner and pull partner with a nearby WINS server. In such a configuration, the two servers at the ends of the chain would also be push and pull partners with each other. Other replication partner configurations can be established for your site's needs.

Only a limited number of WINS proxies should be designated on each domain, so that a limited number of computers are using resources to respond to broadcast name requests.

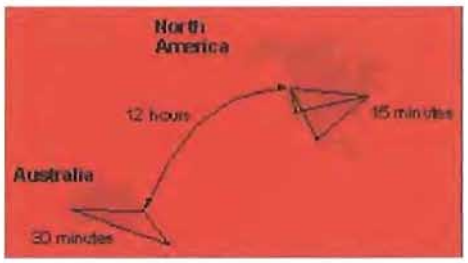
Planning a Strategy for WINS Servers

Planning Replication Frequency Between Hubs

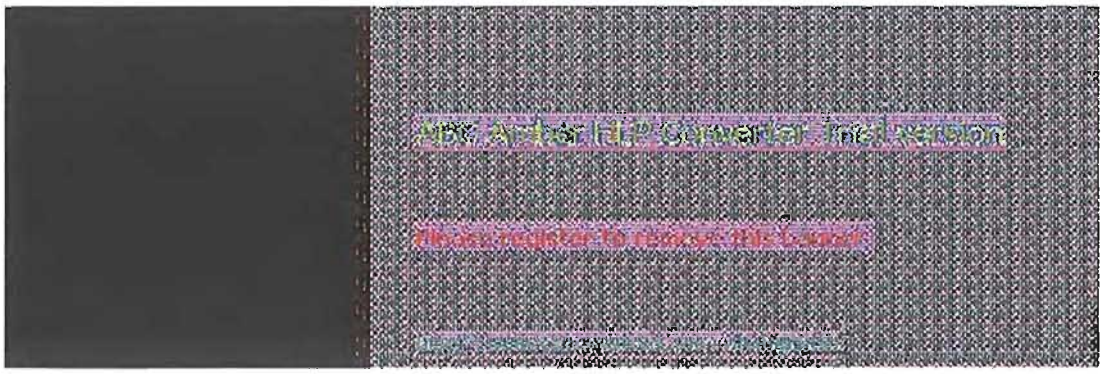
A major tuning issue for WINS servers is replication frequency. You want replication to occur frequently enough that any server being down will not interfere with the reliability of name query responses. However, for longer wide area network (WAN) lengths, you do not want replication to interfere with network throughput.

For multiple network hubs interconnected by WAN links, replication frequency can be configured to be low compared to the replication frequency of multiple WINS servers at a single hub. For long WAN links, infrequent replication ensures that the links are available to carry client traffic without WINS affecting throughput.

For example, the WAN servers at a central site might be configured to replicate every 15 minutes. Replication between WAN hubs of a greater distance might be scheduled for every 30 minutes. Replication between servers on different continents might replicate twice a day.



Example of an Enterprise-Wide Configuration for WINS Replication



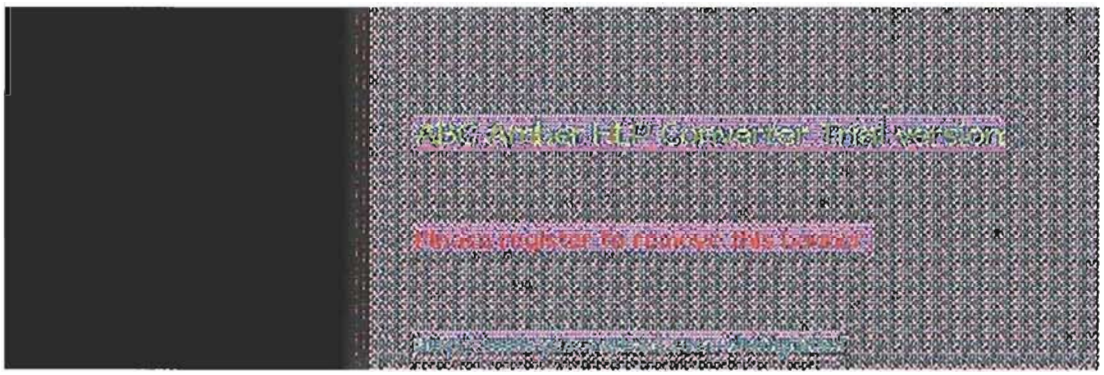
Setting Up LMHOSTS

The LMHOSTS file is commonly used on Microsoft networks to locate remote computers for network file, print, and remote procedure services and for domain services such as logons, browsing, replication, and so on.

You will want to use LMHOSTS for smaller networks or to find hosts on remote networks that are not part of the WINS database (since name query requests are not broadcast beyond the local subnet). If WINS servers are in place on an internetwork, users do not have to rely on broadcast queries for name resolution, since WINS is the preferred method for name resolution. With WINS servers in place, therefore, LMHOSTS may not be necessary.

This chapter presents the following topics:

- Editing the LMHOSTS file
- Using LMHOSTS with dynamic name resolution

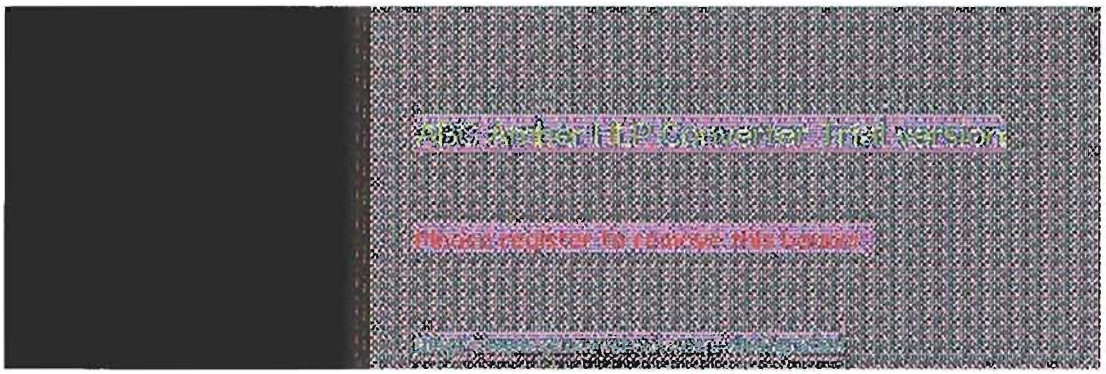


Editing the LMHOSTS File

The LMHOSTS file used by Windows NT contains mappings of IP addresses to Windows NT computer names (which are NetBIOS names). This file is compatible with Microsoft LAN Manager 2.x TCP/IP LMHOSTS files.

You can use Notepad or any other text editor to edit the sample LMHOSTS file that is automatically installed in the *\systemroot*\SYSTEM32\DRIVERS\ETC directory.

This section provides some basic rules and guidelines for LMHOSTS.



Editing the LMHOSTS File

Rules for LMHOSTS

The following rules apply for entries in LMHOSTS:

- Each entry should be placed on a separate line.
- The IP address should begin in the first column, followed by the corresponding computer name.
- The address and the computer name should be separated by at least one space or tab.
- NetBIOS names can contain uppercase and lowercase characters and special characters. If a name is placed between double quotation marks, it will be used exactly as entered. For example, "AccountingPDC" is a mixed-case name, and "HumanRscSr \0x03" generates a name with a special character.

> **Note**
> In Microsoft networks, a NetBIOS computer name in quotes that is less than 16 characters is padded with spaces. If you do not want this behavior, make sure the quoted string is 16 characters long.

- The # character is usually used to mark the start of a comment. However, it can also designate special keywords, as described in this section.

The keywords listed in the following table can be used in LMHOSTS under Windows NT. (LAN Manager 2.x, which also uses LMHOSTS for NetBIOS over TCP/IP name resolution, treats these keywords as comments.)

LMHOSTS Keywords

Keyword	Meaning
#PRE	Added after an entry to cause that entry to be preloaded into the name cache. By default, entries are not preloaded into the name cache but are parsed only after WINS and name query broadcasts fail to resolve a name. #PRE must be appended for entries that also appear in #INCLUDE statements; otherwise, the entry in #INCLUDE is ignored.
#DOM:<*domain*>	Added after an entry to associate that entry with the domain specified by <*domain*>. This keyword affects how the Browser and Logon services behave in routed TCP/IP environments. To preload a #DOM entry, you must also add the #PRE keyword to the line.
#INCLUDE <*filename*>	Forces the system to seek the specified <*filename*> and parse it as if it were local. Specifying a Uniform Naming Convention (UNC) <*filename*> allows you to use a centralized LMHOSTS file on a server. If the server is located outside of the local broadcast area, you must add a mapping for the server before its entry in the #INCLUDE section and also append #PRE to ensure that it preloaded.
#BEGIN_ALTERNATE	Used to group multiple #INCLUDE statements. Any single successful #INCLUDE causes the group to succeed.
#END_ALTERNATE	Used to mark the end of an #INCLUDE grouping.

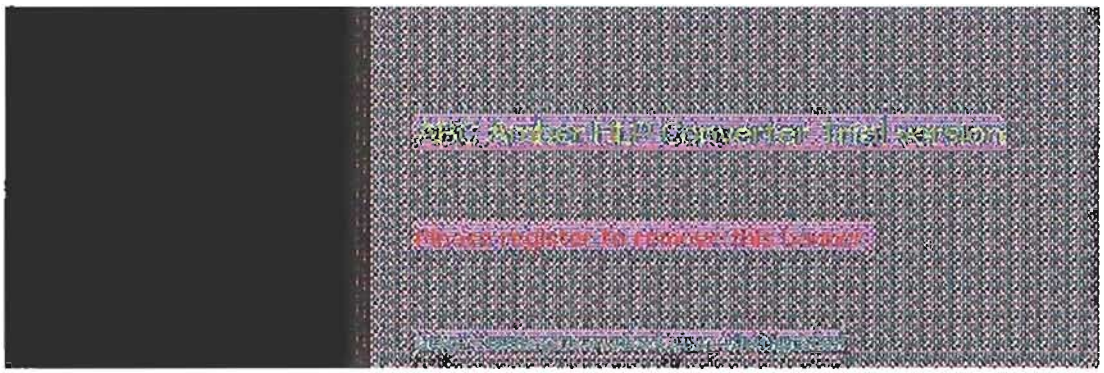
\0x*nn*	Support for nonprinting characters in NetBIOS names. Enclose the NetBIOS name in double quotation marks and use \0x*nn* notation to specify a hexadecimal value for the character. This allows custom applications that use special names to function properly in routed topologies. However, LAN Manager TCP/IP does not recognize the hexadecimal format, so you surrender backward compatibility if you use this feature. Note that the hexadecimal notation applies only to one character in the name. The name should be padded with blanks so the special character is last in the string (character 16).

The following example shows how all of these keywords are used:

```
102.54.94.98  localsrv  #PRE
102.54.94.97  trey       #PRE     #DOM:networking          #net group's PDC
102.54.94.102    "appname      \0x14"                                          #special app server
102.54.94.123    popular          #PRE                                              #source
server

#BEGIN_ALTERNATE
#INCLUDE \\localsrv\public\lmhosts                    #adds LMHOSTS from this server
#INCLUDE \\trey\public\lmhosts                        #adds LMHOSTS from this server
#END_ALTERNATE
```

In the above example:

- The servers named **localsrv** and **trey** are specified so they can be used later in an #INCLUDE statement in a centrally maintained LMHOSTS file.
- The server named **"appname \0x14"** contains a special character after the 15 characters in its name (including the blanks), so its name is enclosed in double quotation marks.
- The server named **popular** is preloaded, based on the #PRE keyword.

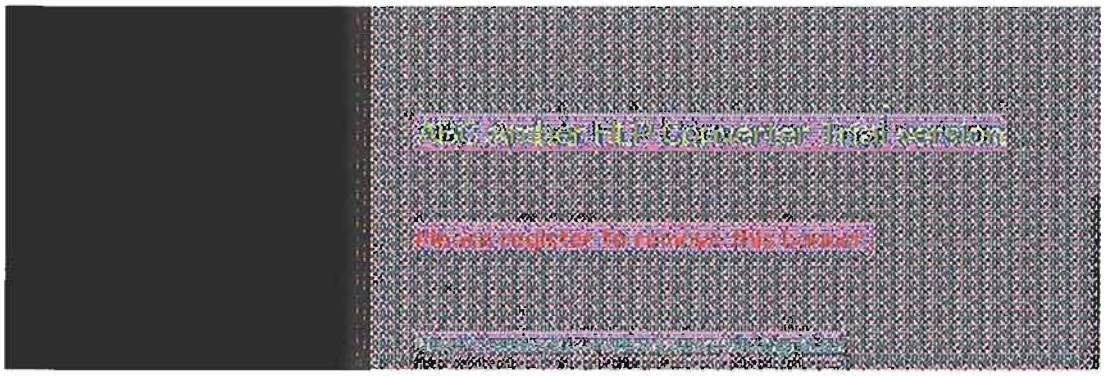


Editing the LMHOSTS File

Guidelines for LMHOSTS

When you use a host table file, be sure to keep it up to date and organized. Follow these guidelines:

- Update the LMHOSTS file whenever a computer is changed or removed from the network.
- Because LMHOSTS files are searched one line at a time from the beginning, list remote computers in priority order, with the ones used most often at the top of the file, followed by remote systems listed in #INCLUDE statements. Finally, the #PRE entries should be left for the end of the file, because these are preloaded into the cache at system startup time and are not accessed later. This increases the speed of searches for the entries used most often. Also, any comment lines add to the parsing time, because each line is processed individually.
- Use #PRE statements to preload popular entries and servers listed in #INCLUDE statements into the local computer's name cache.



Name Resolution

On networks that do not use WINS, the broadcast name resolution method used by Windows NT computers provides a simple, dynamic mechanism for locating resources by name on a TCP/IP network.

Because broadcast name resolution relies on IP-level broadcasts to locate resources, unwanted effects can occur in routed IP topologies. In particular, resources located on remote subnets do not receive name query requests, because routers do not pass IP-level broadcasts. For this reason, Windows NT allows you to manually provide computer name and IP address mappings for remote resources via LMHOSTS.

This section describes how the LMHOSTS file can be used to enhance Windows NT in routed environments. This section includes the following topics:

- Specifying remote servers in LMHOSTS
- Designating primary domain controllers using #DOM
- Using centralized LMHOSTS files

Using LMHOSTS with Dynamic Name Resolution

Specifying Remote Servers in LMHOSTS

Computer names can be resolved outside the local broadcast area if computer name and IP address mappings are specified in the LMHOSTS file. For example, suppose the computer named ClientA wants to connect to the computer named ServerB, which is outside of its IP broadcast area. Both Windows NT computers are configured with Microsoft TCP/IP.

Under a strict b-node broadcast protocol, as defined in RFCs 1001 and 1002, ClientA's name query request for ServerB would fail (by timing out), because ServerB is located on a remote subnet and does not respond to ClientA's broadcast requests. So an alternate method is provided for name resolution. Windows NT maintains a limited cache of computer name and IP address mappings, which is initialized at system startup. When a workstation needs to resolve a name, the cache is examined first and, if there is no match in the cache, Windows NT uses b-node broadcast name resolution. If this fails, the LMHOSTS file is used. If this last method fails, the name is unresolved, and an error message appears.

This strategy allows the LMHOSTS file to contain a large number of mappings without requiring a large chunk of static memory to maintain an infrequently used cache. At system startup, the name cache is preloaded only with entries from LMHOSTS tagged with the #PRE keyword. For example, the LMHOSTS file could contain the following:

```
102.54.94.91   accounting          #accounting server
102.54.94.94   payroll             #payroll server
102.54.94.97   stockquote          #PRE   #stock quote server
102.54.94.102  printqueue                  #print server in Bldg 10
```

In this example, the server named **stockquote** is preloaded into the name cache, because it is tagged with the #PRE keyword. Entries in the LMHOSTS file can represent Windows NT Workstation computers, Windows NT Server computers, LAN Manager servers, or Windows for Workgroups 3.11 computers running Microsoft TCP/IP. There is no need to distinguish between different platforms in LMHOSTS.

Note

The Windows NT tag #PRE allows backward compatibility with LAN Manager 2.x LMHOSTS files and offers added flexibility in Windows NT. Under LAN Manager, the # character identifies a comment, so all characters thereafter are ignored. But #PRE is a valid tag for Windows NT.

In the above example, the servers named **accounting**, **payroll**, and **printqueue** would be resolved only after the cache entries failed to match and after broadcast queries failed to locate them. After nonpreloaded entries are resolved, their mappings are cached for a period of time for reuse.

Windows NT limits the preload name cache to 100 entries by default. This limit only affects entries marked with #PRE. If you specify more than 100 entries, only the first 100 #PRE entries will be preloaded. Any additional #PRE entries will be ignored at startup but will be resolved when the system parses the LMHOSTS file after dynamic resolution fails.

Finally, you can reprime the name cache by using the **nbtstat -R** command to purge and reload the name cache, reread the LMHOSTS file, and insert entries tagged with the #PRE keyword. Use **nbtstat** to remove or correct preloaded entries that may have been mistyped or any names cached by successful broadcast resolution.


ABC Artech LLP Converter Trial Version

Using LMHOSTS with Dynamic Name Resolution

Designating Domain Controllers Using #DOM

The most common use of LMHOSTS is for locating remote servers for file and print services. But for Windows NT, LMHOSTS can also be used to find domain controllers running TCP/IP in routed environments. Windows NT primary domain controllers (PDCs) and backup domain controllers (BDCs) maintain the user account security database and manage other network-related services. Because large Windows NT domains can span multiple IP subnets, it is possible that routers could separate the domain controllers from one another or separate other computers in the domain from domain controllers.

The #DOM keyword can be used in LMHOSTS files to distinguish a Windows NT domain controller from a Windows NT Workstation computer, a LAN Manager server, or a Windows for Workgroups computer. To use the #DOM tag, follow the name and IP address mapping in LMHOSTS with the #DOM keyword, a colon, and the domain in which the domain controller participates. For example:

```
102.54.94.97  treydc     #DOM:treycorp     #The treycorp PDC
```

Using the #DOM keyword to designate domain controllers adds entries to a special *internet group name cache* that is used to limit internetwork distribution of requests intended for the local domain controller. When domain controller activity such as a logon request occurs, the request is sent on the special internet group name. In the local IP-broadcast area, the request is sent only once and picked up by any local domain controllers. However, if you use #DOM to specify domain controllers in the LMHOSTS file, Microsoft TCP/IP uses datagrams to also forward the request to domain controllers located on remote subnets.

Examples of such domain controller activities include domain controller pulses (used for account database synchronization), logon authentication, password changes, master browser list synchronization, and other domain management activities.

For domains that span subnets, LMHOSTS files can be used to map important members of the domain using #DOM. The following lists some guidelines for doing this.

- For each local LMHOSTS file on a Windows NT computer that is a member in a domain, there should be #DOM entries for all domain controllers in the domain that are located on remote subnets. This ensures that logon authentication, password changes, browsing, and so on all work properly for the local domain. These are the minimum entries necessary to allow a Windows NT system to participate in a Windows networking internetwork.
- For local LMHOSTS files on all servers that can be backup domain controllers, there should be mappings for the primary domain controller's name and IP address, plus mappings for all other backup domain controllers. This ensures that promoting a backup to primary domain controller status does not affect the ability to offer all services to members of the domain.
- If trust relationships exist between domains, all domain controllers for all trusted domains should also be listed in the local LMHOSTS file.
- For domains that you want to browse from your local domain, the local LMHOSTS files should contain at least the name and IP address mapping for the primary domain controller in the remote domain. Again, backup domain controllers should also be included so that promotion to primary domain controller does not impair the ability to browse remote domains.

For small to medium sized networks with fewer than 20 domains, a single common LMHOSTS file usually satisfies all workstations and servers on the internetwork. To achieve this, systems should use the Windows NT replicator service to maintain synchronized local copies of the global LMHOSTS or use centralized LMHOSTS files, as described in the following section.

Names that appear with #DOM in LMHOSTS are placed in a special domain name list in NetBIOS

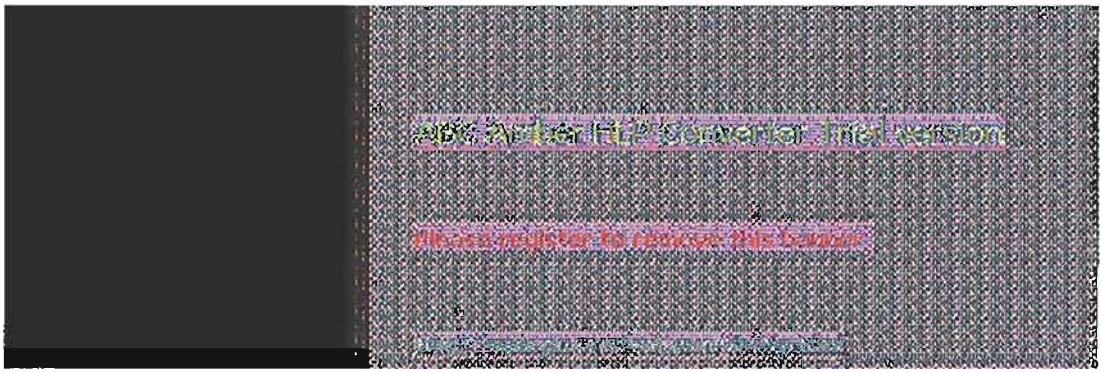
over TCP/IP. When a datagram is sent to this domain using the DOMAIN<1C> name, the name is resolved first via WINS or broadcast. The datagram is then sent to all the addresses on the list from LMHOSTS, and there is also a broadcast on the local subnet.

Important

To browse across domains, for Windows NT Advanced Server 3.1 and Windows NT 3.1, each computer must have an entry in its LMHOSTS file for the primary domain controller in each domain. This remains true for Windows NT version 3.5 clients, unless the Windows NT Server computer is also version 3.5 and, optionally, offers WINS name registration.

However, you cannot add an LMHOSTS entry for a Window NT Server that is a DHCP client, because the IP address changes dynamically. To avoid problems, any domain controllers whose names are entered in LMHOSTS files should have their IP addresses reserved as static addresses in the DHCP database rather than running as DHCP clients.

Also, all Windows NT Advanced Server 3.1 computers in a domain and its trusted domains should be upgraded to version 3.5, so that browsing across domains is possible without LMHOSTS.



Using LMHOSTS with Dynamic Name Resolution

Using Centralized LMHOSTS Files

With Microsoft TCP/IP, you can include other LMHOSTS files from local and remote computers. The primary LMHOSTS file is always located in the *\systemroot*\SYSTEM32\DRIVERS\ETC directory on the local computers. Most networks will also have an LMHOSTS file maintained by the network administrator, so administrators should maintain one or more global LMHOSTS files that users can rely on. This is done using #INCLUDE statements rather than copying the global file locally. Then use the replicator service to distribute multiple copies of the global file(s) to multiple servers for reliable access.

To provide a redundant list of servers maintaining copies of the same LMHOSTS file, use the #BEGIN_ALTERNATE and #END_ALTERNATE keywords. This is known as a *block inclusion*, which allows multiple servers to be searched for a valid copy of a specific file. The following example shows the use of the #INCLUDE and #_ALTERNATE keywords to include a local LMHOSTS file (in the C:\PRIVATE directory):

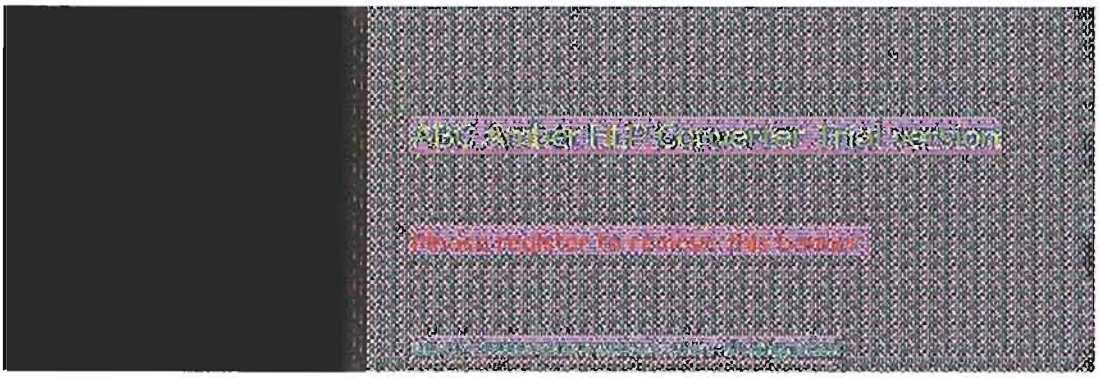
```
102.54.94.97  treydc        #PRE  #DOM:treycorp      #primary DC
102.54.94.99  treybdc       #PRE  #DOM:treycorp        #backup DC in domain
102.54.94.98     localsvr  #PRE  #DOM:treycorp

#INCLUDE      c:\private\lmhosts                        #include a local lmhosts

#BEGIN_ALTERNATE
#INCLUDE      \\treydc\public\lmhosts          #source for global file
#INCLUDE      \\treybdc\public\lmhosts         #backup source
#INCLUDE      \\localsvr\public\lmhosts        #backup source
#END_ALTERNATE
```

Important

This feature should never be used to include a remote file from a redirected drive, because the LMHOSTS file is shared between local users who have different profiles and different logon scripts, and even on single-user systems, redirected drive mappings can change between logon sessions.

In the above example, the servers **treydc** and **treybdc** are located on remote subnets from the computer that owns the file. The local user has decided to include a list of preferred servers in a local LMHOSTS file located in the C:\PRIVATE directory. During name resolution, the Windows NT system first includes this private file, then gets the global LMHOSTS file from one of three locations: **treydc**, **treybdc**, or **localsvr**. All names of servers in the #INCLUDE statements must have their addresses preloaded using the #PRE keyword; otherwise, the #INCLUDE statement will be ignored.

The block inclusion is satisfied if one of the three sources for the global LMHOSTS is available and none of the other servers are used. If no server is available, or for some reason the LMHOSTS file or path is incorrect, an event is added to the event log to indicate that the block inclusion failed.



Using the Microsoft FTP Server Service

The Microsoft FTP Server service allows other computers using the FTP utility to connect to this computer and transfer files. The FTP Server service supports all Windows NT ftp client commands. Non-Microsoft versions of FTP clients may contain commands that are not supported. The FTP Server service is implemented as a multithreaded Win32 service that complies with the requirements defined in Requests for Comments (RFCs) 959 and 1123.

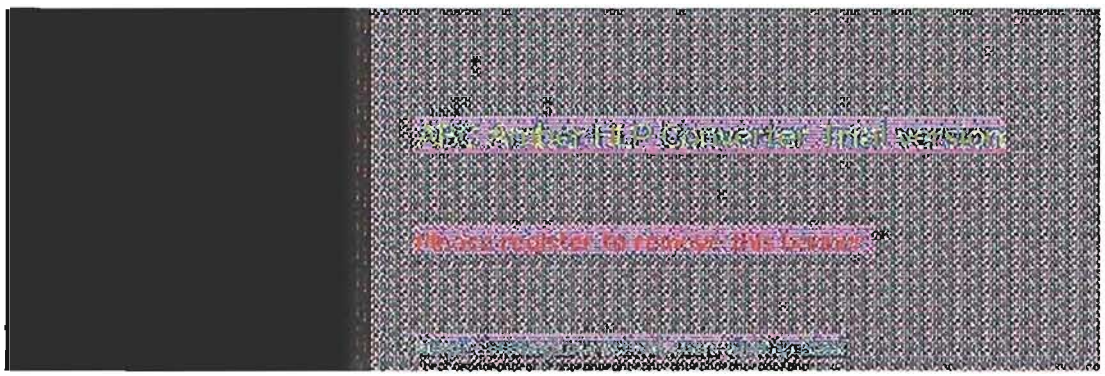
The FTP Server service is integrated with the Windows NT security model. Users connecting to the FTP Server service are authenticated based on their Windows NT user accounts and receive access based on their user profiles. For this reason, it is recommended that the FTP Server service be installed on an NTFS partition so that the files and directories made available via FTP can be secured.

Caution
The FTP Server protocol relies on the ability to pass user passwords over the network without data encryption. A user with physical access to the network could examine user passwords during the FTP validation process.

The following topics are included in this chapter:

- Installing the FTP Server service
- Configuring the FTP Server service
- Administering the FTP Server service
- Advanced configuration parameters for FTP Server service

For information about using performance counters to monitor FTP Server traffic, see Chapter 8, "Using Performance Monitor with TCP/IP Services."



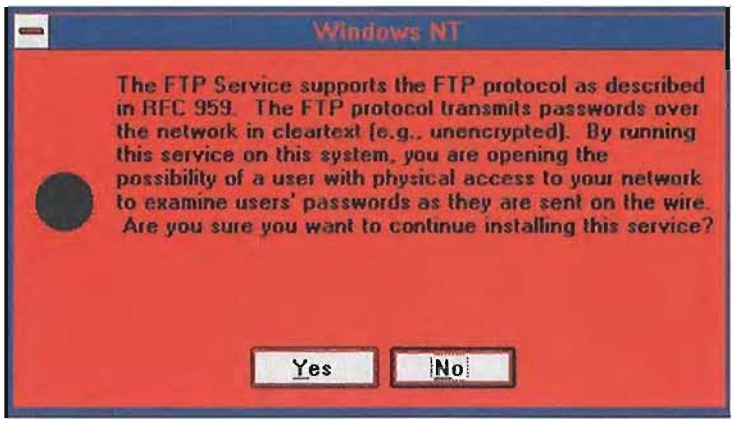
Installing the FTP Server Service

These procedures assume that you have installed any necessary devices and device drivers.

You must be logged on as a member of the Administrators group for the local computer to install and configure the FTP Server service.

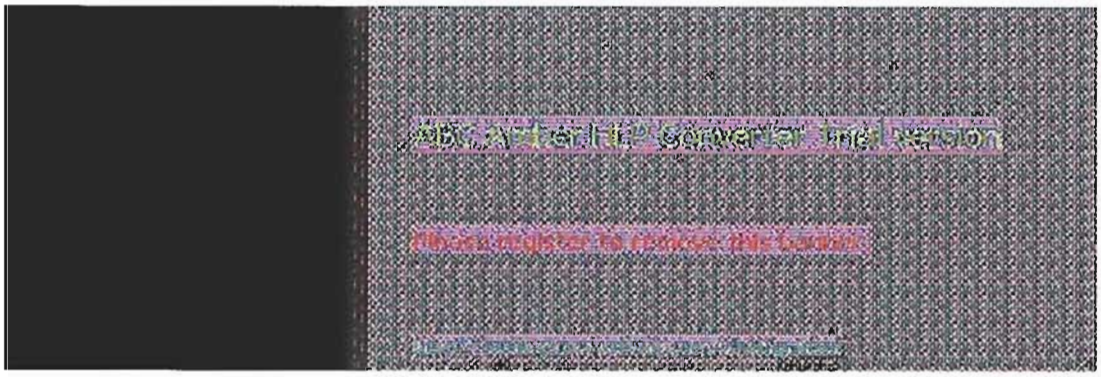
To install the FTP Server service

1. Choose the Network option in Control Panel.
2. In the Network Settings dialog box, choose the Add Software button to display the Add Network Software dialog box.
3. In the Network Software box, select TCP/IP Protocol And Related Components, and then choose the Continue button. When the Windows NT TCP/IP Installation Options dialog box appears, check the FTP Server Service option, and then choose the OK button.
4. When the message prompts you to confirm that you are familiar with FTP security, choose the Yes button to continue with FTP Server service installation.



5. When prompted for the full path to the Windows NT distribution files, provide the appropriate location, and then choose the Continue button.
6. After the necessary files are copied to your computer, the FTP Service dialog box appears so that you can continue with the configuration procedure as described in the next section. The FTP Server service must be configured in order to operate.

Note
For disk partitions that do not use the Windows NT file system (NTFS), you can apply simple read/write security by using the FTP Server tool in the Control Panel as described in the following section.



Configuring the FTP Server Service

After the FTP Server service software is installed on your computer, you must configure it to operate. When you configure the FTP Server service, your settings result in one of the following:

- No anonymous FTP connection allowed. In this case, each user must provide a valid Windows NT username and password. To configure the FTP Server service for this, make sure the Allow Anonymous Connection box is cleared in the FTP Service dialog box.
- Allow both anonymous and Windows NT users to connect. In this case, a user can choose to use either an anonymous connection or a Windows NT username and password. To configure the FTP Server service for this, make sure only the Allow Anonymous Connection box is checked in the FTP Service dialog box.
- Allow only anonymous FTP connections. In this case, a user cannot connect using a Windows NT username and password. To configure the FTP Server service for this, make sure both the Allow Anonymous Connections and the Allow Anonymous Connections Only boxes are checked in the FTP Service dialog box.

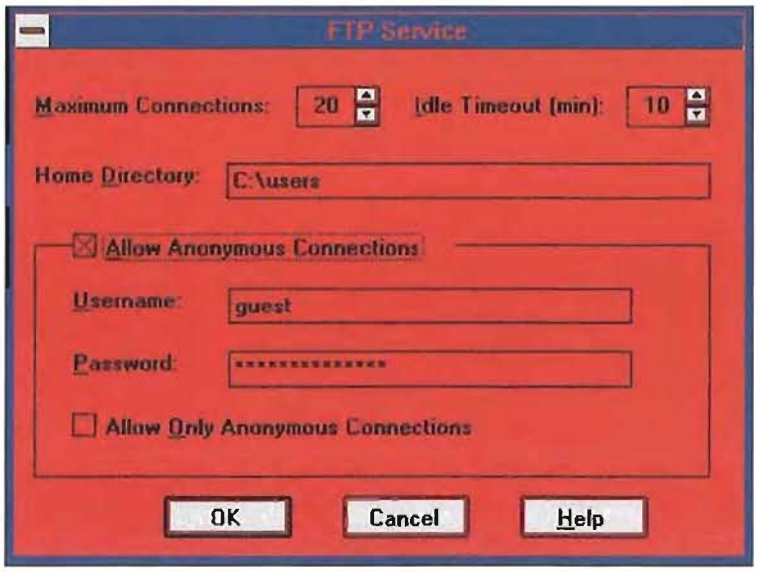
If anonymous connections are allowed, you must supply the Windows NT username and password to be used for anonymous FTP. When an anonymous FTP transfer takes place, Windows NT will check the username assigned in this dialog box to determine whether access is allowed to the files.

To configure or reconfigure the FTP Server service

1. The FTP Service dialog box appears automatically after the FTP Server service software is installed on your computer.

   Or

   If you are reconfiguring the FTP Server service, choose the Network option in Control Panel. In the Installed Network Software box, select FTP Server, and then choose the Configure button.



The FTP Service dialog box displays the following options:

Item	Description

Maximum Connections	Specifies the maximum number of FTP users who can connect to the system simultaneously. The default value is 20; the maximum is 50. A value of 0 means no maximum, that is, an unlimited number of simultaneous users. When the specified number of concurrent users are logged onto the FTP server, any subsequent attempts to connect will receive messages defined by the administrator. For information about defining custom messages, see "Advanced Configuration Parameters for FTP Server Service" later in this chapter.
Idle Timeout	Specifies how many minutes an inactive user can remain connected to the FTP Server service. The default value is 10 minutes; the maximum is 60 minutes. If the value is 0, users are never automatically disconnected.
Home Directory	Specifies the initial directory for users.
Allow Anonymous Connections	Enables users to connect to the FTP Server using the user name **anonymous** (or **ftp**, which is a synonym for **anonymous**). A password is not necessary, but the user will be prompted to supply a mail address as the password. By default, anonymous connections are not allowed. Notice that you cannot use a Windows NT user account with the name **anonymous** with the FTP Server. The **anonymous** user name is reserved in the FTP Server for the anonymous logon function. Users logging on with the username **anonymous** receive permissions based on the FTP Server configuration for anonymous logons.
Username	Specifies which local user account to use for FTP Server users who log on under **anonymous**. Access permissions for the anonymous FTP user will be the same as the specified local user account. The default is the standard Guest system account. If you change this, you must also change the password.
Password	Specifies the password for the user account specified in the Username box.
Allow Only Anonymous Connections	Allows only the user name **anonymous** to be accepted. This option is useful if you do not want users to log on using their own user names and passwords because FTP passwords are unencrypted. However, all users will have the same access privilege, defined by the anonymous account. By default, this option is not enabled.

2. Default values are provided for Maximum Connections, Idle Timeout, and Home Directory. Accept the default values, or change values for each field as necessary.

3. Choose the OK button to close the FTP Service dialog box and return to the Network Settings dialog box.

4. To complete initial FTP Server service installation and configuration, choose the OK button.

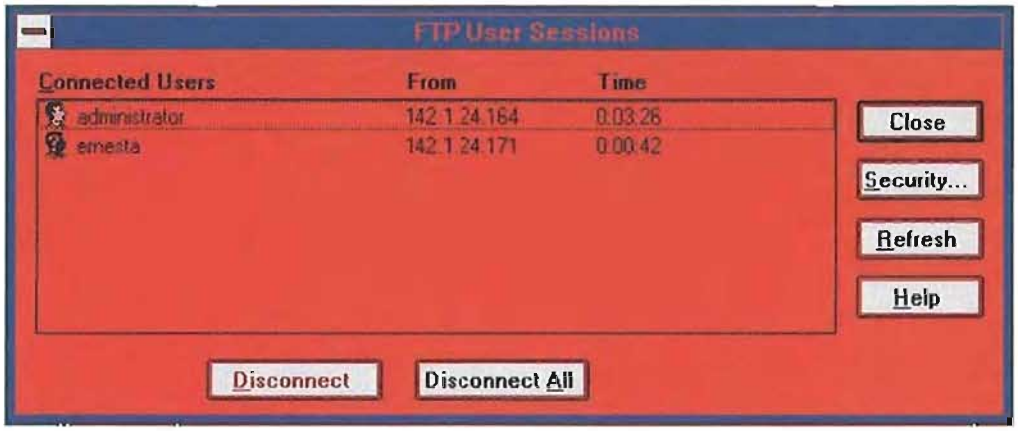
   A message reminds you that you must restart the computer so that the changes you made will take effect.

Note

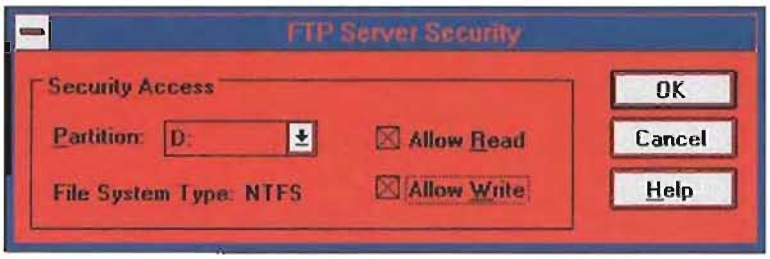
When you first install the FTP Server service, you must also complete the security configuration as described in the following procedure for users to access volumes on your computer.

To configure FTP Server security

1. After the FTP Server has been installed and you have restarted Control Panel, start the FTP Server option in Control Panel. Windows NT Server users can also use the FTP menu in Server Manager.



2. In the FTP User Sessions dialog box, choose the Security button.



3. In the Partition box of the FTP Server Security dialog box, select the drive letter you want to set security on, and then check the Allow Read or Allow Write check box, or both check boxes, depending on the security you want for the selected partition.

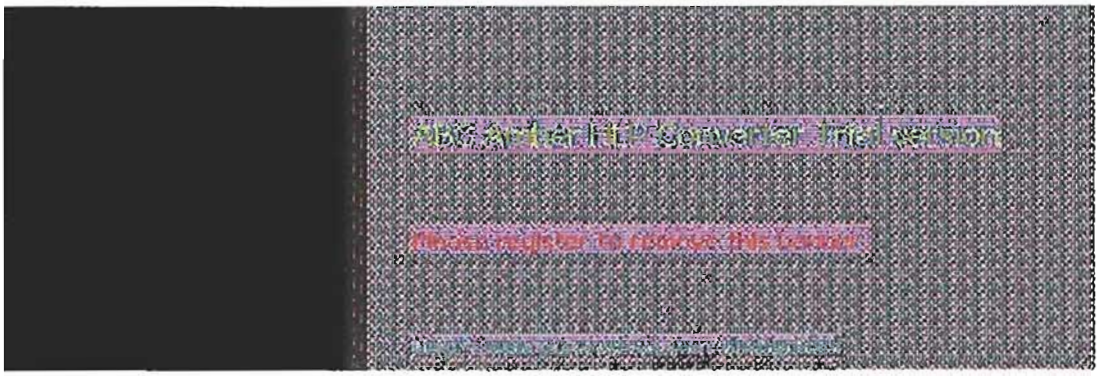
   Repeat this step for each partition.

   Setting these permissions will affect all files across the entire partition on file allocation table (FAT) and high-performance file system (HPFS) partitions. On NTFS partitions, this feature can be used to remove read or write access (or both) on the entire partition.

   Any restrictions set in this dialog box are enforced in addition to any security that might be part of the file system. That is, an administrator can use this dialog box to remove permissions on specific volumes but cannot use it to grant permissions beyond those maintained by the file system. For example, if a partition is marked as read-only, no one can write to the partition via FTP regardless of any permissions set in this dialog box.

4. Choose the OK button when you are finished setting security access on partitions.

   The changes take effect immediately. The FTP Server service is now ready to operate.



Administering the FTP Server Service

After initial installation is complete, the FTP Server service is automatically started in the background each time the computer is started. Remote computers can initiate an FTP session while the FTP Server service is running on your Windows NT computer. Both computers must be running the TCP/IP protocol.

You must be logged on as a member of the Administrators group to administer the FTP Server.

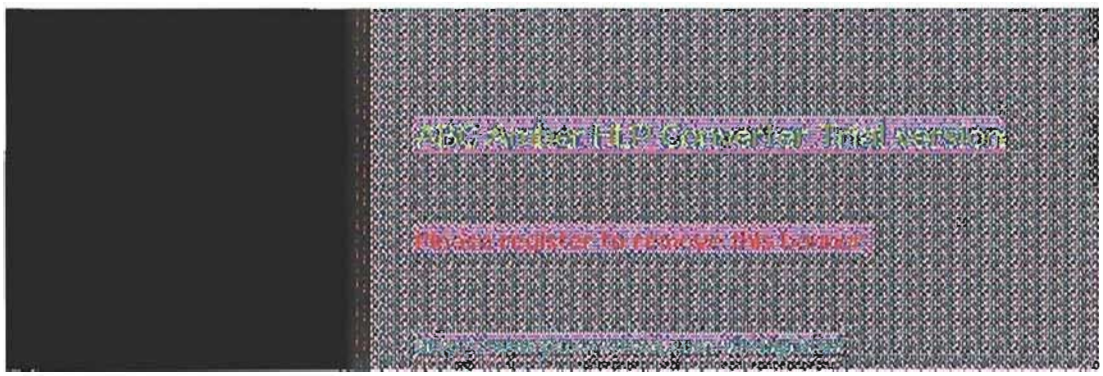
Remote users can connect to the FTP Server using their account on the FTP Server, an account on the FTP Server's domain or trusted domains (Windows NT Server only), or using the **anonymous** account if the FTP Server service is configured to allow anonymous logons.

When making any configuration changes to the FTP Server (with the exception of security configuration), you must restart the FTP Server by either restarting the computer or manually stopping and restarting the server, using the **net** command or Services icon in Control Panel.

To start or stop the FTP Server service

- Use the Services option in Control Panel, or at the command prompt use the commands **net stop ftpsvc** followed by **net start ftpsvc**.

Restarting the service in this way disconnects any users presently connected to the FTP Server without warning-so use the FTP Server option in Control Panel to determine if any users are connected. Pausing the FTP Server (by using the Services option in Control Panel or the **net pause** command) prevents any more users from connecting to the FTP Server but does not disconnect the currently logged on users. This feature is useful when the administrator wants to restart the server without disconnecting the current users. After the users disconnect on their own, the administrator can safely shut down the server without worrying that users will lose work. When attempting to connect to a Windows NT FTP Server that has been paused, clients receive the message "421 - Service not available, closing control connection."



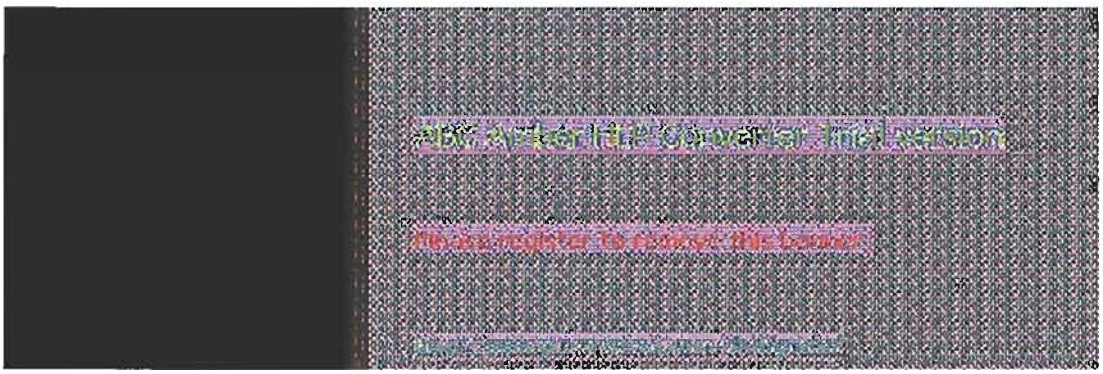
Administering the FTP Server Service

Using FTP Commands at the Command Prompt

When you install the FTP service, a set of **ftp** commands are automatically installed that you can use at the command prompt. For a summary list of these commands, see the **ftp** entry in Chapter 11, "Utilities Reference."

To get help on ftp commands

1. Double-click the Windows NT Help icon in the Program Manager group.
2. In the Windows NT help window, click the Command Reference Help button.
3. Click the **ftp commands** name in the Commands window.
4. Click an **ftp** command name in the Command Reference window to see a description of the command, plus its syntax and parameter definitions.



Administering the FTP Server Service

Managing Users

Use the FTP Server option in Control Panel to manage users connected to the FTP Server and to set security for each volume on the FTP Server. For convenience on Windows NT Server computers, the same dialog box can be reached from Server Manager by choosing the FTP menu command.

In the FTP User Sessions dialog box, the Connected Users box displays the names of connected users, their system's IP addresses, and how long they have been connected. For users who logged on using the **anonymous** user name, the display shows the passwords used when they logged on as their user names. If the user name contained a mail host name (for example, ernesta@trey-research.com) only the username (ernesta) appears. Anonymous users also have a question mark (?) over their user icons. Users who have been authenticated by Windows NT security have no question mark.

The FTP Server allows you to disconnect one or all users with the disconnect buttons. Users are not warned if you disconnect them.

The FTP Server displays users' names as they connect but does not update the display when users disconnect or when their connect time elapses. The Refresh button allows you to update the display to show only users who are currently connected.

Choosing the Security button displays the FTP Service Security dialog box, where you can set Read and Write permissions for each partition on the FTP Server, as described earlier in this chapter. You must set the permissions for each partition you want FTP users to have access to. If you do not set partition parameters, no users will be able to access files. If the partition uses a secure file system, such as NTFS, file system restrictions are also in effect.

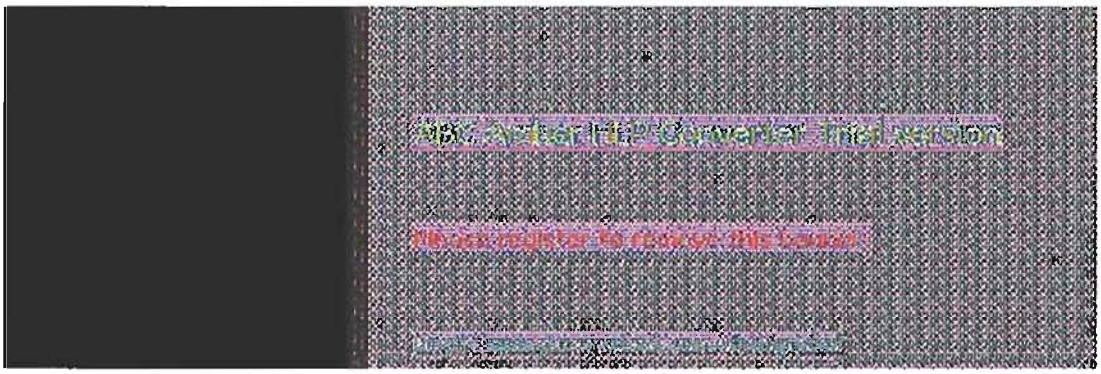
In addition to FTP Server partition security, if a user logs on using a Windows NT account, access permissions for that account are in effect.

Administering the FTP Server Service

Controlling the FTP Server and User Access

A network administrator can control several of the FTP Server configuration variables. One such variable, Maximum Connections, can be set by using the Network option in Control Panel to define a value between 0 and 50. Any value from 1 to 50 restricts concurrent FTP sessions to the value specified. A value of 0 allows unlimited connections to be established to the FTP Server until the system exhausts the available memory.

You can specify a custom message to be displayed when the maximum number of concurrent connections is reached. To do this, enter a new value for **MaxClientsMessage** in the Registry, as described in "Advanced Configuration Parameters for FTP Server Service" later in this chapter.



Administering the FTP Server Service

Annotating Directories

You can add directory descriptions to inform FTP users of the contents of a particular directory on the server by creating a file called ~FTPSVC~.CKM in the directory that you want to annotate. Usually you want to make this a hidden file so directory listings do not display this file. To do this, use File Manager or type the command **attrib +h ~ftpsvc~.ckm** at the command prompt.

Directory annotation can be toggled by FTP users on a user-by-user basis with a built-in, site-specific command called **ckm**. On most FTP client implementations (including the Windows NT FTP client), users type a command at the command prompt similar to **quote site ckm** to get this effect.

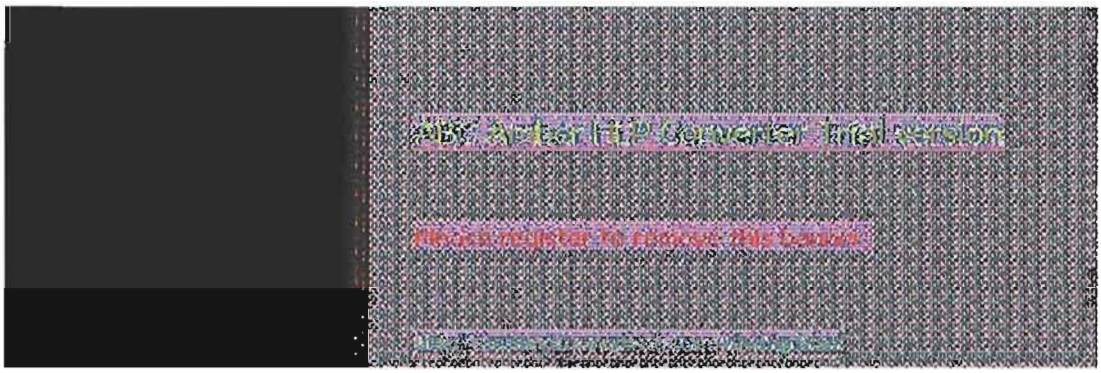
You can set the default behavior for directory annotation by setting a value for **AnnotateDirectories** in the Registry, as described in "Advanced Configuration Parameters for FTP Server Service" later in this chapter.

Administering the FTP Server Service

Changing Directory Listing Format

Some FTP client software makes assumptions based on the formatting of directory list information. The Windows NT FTP Server provides some flexibility for client software that requires directory listing similar to UNIX systems. Users can use the command **dirstyle** to toggle directory listing format between MS-DOSstyle (the default) and UNIX-style listings. On most FTP client implementations (including the Windows NT FTP client), users type a command at the command prompt similar to **quote site dirstyle** to get this effect.

You can set the default style for directory listing format by setting a value for **MsDosDirOutput** in the Registry, as described in "Advanced Configuration Parameters for FTP Server Service" later in this chapter.

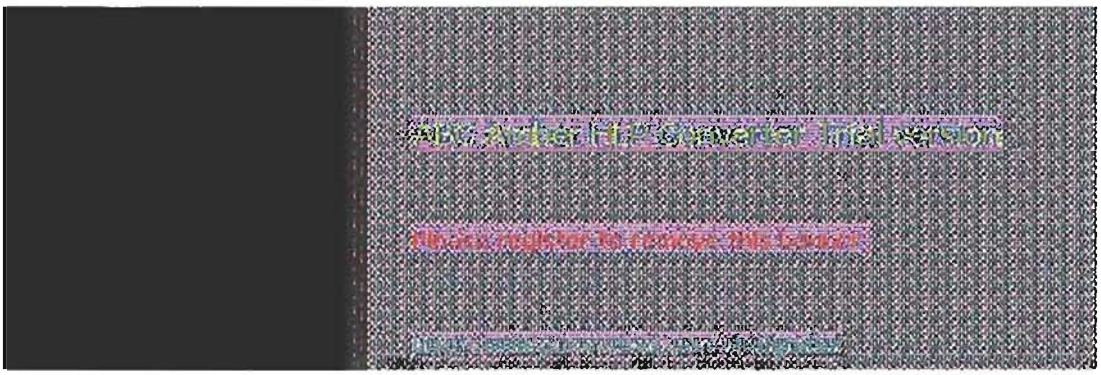


Administering the FTP Server Service

Customizing Greeting and Exit Messages

You can create customized greeting and exit messages by setting values for **GreetingMessage** and **ExitMessage** in the Registry, as described in "Advanced Configuration Parameters for FTP Server Service" later in this chapter. By default, these value entries are not in the Registry, so you must add them to customize the message text.

Greeting and exit messages are sent to users when they connect or disconnect from the FTP Server. When you create custom messages, you can add multiline messages of your choice.

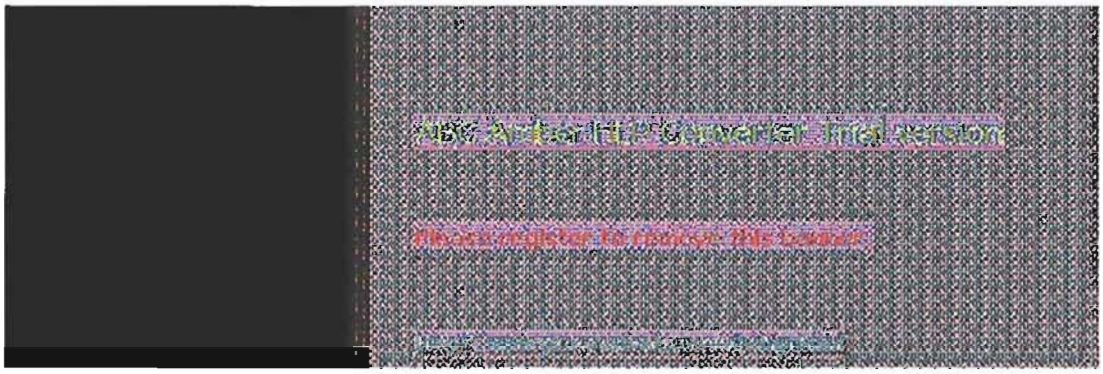


Administering the FTP Server Service

Logging FTP Connections

You can log incoming FTP connections in the System event log by setting values for **LogAnonymous** and **LogNonAnonymous** in the Registry, as described in "Advanced Configuration Parameters for FTP Server Service" later in this chapter. By default, these value entries are not in the Registry, so you must add them to log incoming connections.

You can specify whether event log entries are made for both anonymous and nonanonymous users connecting to the FTP Server. You can view such entries in the System event log by using Event Viewer.



Advanced Configuration Parameters for FTP Server Service

This section presents configuration parameters that affect the behavior of the FTP Server service and that can be modified only through Registry Editor. After you modify any of these value entries, you must restart the FTP Server service for the changes to take effect.

Caution

You can impair or disable Windows NT if you make incorrect changes in the Registry while using Registry Editor. Whenever possible, use administrative tools such as Control Panel to make configuration changes, rather than using Registry Editor. If you make errors while changing values with Registry Editor, you will not be warned, because Registry Editor does not recognize semantic errors.

To make changes to the FTP Server service configuration using Registry Editor

1. Run REGEDT32.EXE from File Manager or Program Manager, or at a command prompt, type **start regedt32** and press ENTER.

   When the Registry Editor window appears, you can press F1 to get Help on how to make changes in Registry Editor.

2. In Registry Editor, click the window titled HKEY_LOCAL_MACHINE On Local Machine, and then click the icons for the SYSTEM subtree until you reach this subkey:

   ..\SYSTEM\CurrentControlSet\Services\ftpsvc\Parameters

   All of the parameters described here are located under this Registry subkey.

The following describes the value entries for FTP Server service parameters that can only be set by adding an entry or changing their values in Registry Editor. These value entries do not appear by default in the Registry, so you must add an entry if you want to change its default value.

AnnotateDirectories

Data type = REG_DWORD
Range = 0 or 1
Default = 0 (false-that is, directory annotation is off)

This value entry defines the default behavior of directory annotation for newly connected users. Directory descriptions are used to inform FTP users of the contents of a directory on the server. The directory description is saved in a file named ~FTPSVC~.CKM, which is usually a hidden file. When this value is 1, directory annotation is on.

ExitMessage

Data type = REG_SZ
Range = String
Default = "Goodbye."

This value entry defines a signoff message that will be sent to FTP clients upon receipt of a **quit** command.

GreetingMessage

Data type = REG_MULTI_SZ
Range = String
Default = None (no special greeting message)

This value entry defines the message to be sent to new clients after their accounts have been

validated. In accordance with Internet behavior, if the client logs on as anonymous and specifies an identity that starts with a minus sign (), this greeting message is not sent.

LogAnonymous

Data type = REG_DWORD
Range = 0 or 1
Default = 0 (false-that is, do not log successful anonymous logons)

This value entry enables or disables logging of anonymous logons in the System event log.

LogNonAnonymous

Data type = REG_DWORD
Range = 0 or 1
Default = 0 (false-that is, do not log successful nonanonymous logons)

This value entry enables or disables logging of nonanonymous logons in the System event log.

LogFIleAccess

Data type = REG_DWORD
Range = 0 or 1
Default = 0 (do not log file accesses to FTPSVC.LOG)

If this value is non-zero, all file accesses are logged to the file FTPSVC.LOG in the service's current directory (typically *\systemroot*\SYSTEM32). For each file opened by the FTP Server, FTPSVC.LOG will contain a single line entry in the following format:

IPAddress username action path date_time

- *ip_address* is the client computer's IP address
- *username* is the user's name (or *password* for anonymous logons)
- *action* is either "opened," "created," or "appended"
- *path* is the fully qualified path of the file acted upon
- *date_time* is the date and time the action took place

Entries are also written to the log whenever the FTP Server starts or stops. For example:

********** FTP SERVER SERVICE STARTING Fri Apr 29 10:28:49 1994
11.101.199.173 daveo opened d:\tmp\ist.bat Fri Apr 29 10:29:42 1994
11.101.199.173 daveo created d:\tmp\new.txt Fri Apr 29 10:30:25 1994
11.101.199.173 daveo appended d:\tmp\new.txt Fri Apr 29 10:33:04 1994
********** FTP SERVER SERVICE STOPPING Fri Apr 29 10:33:08 1994

LowercaseFiles

Data type = REG_DWORD
Range = 0 or
1Default = 0 (do not map filenames to lowercase)

If this value is nonzero, all filenames returned by the lIst and nlst commands will be mapped to lowercase for noncase-preserving file systems. This mapping only occurs when a directory listing is requested on a noncase-preserving file system. If this value is 0, case in all filenames will be unaltered. Currently, FAT is the only noncase-preserving file system supported under Windows NT, so this flag has no effect when retrieving listings on HPFS or NTFS partitions.

MaxClientsMessage

Data type = REG_SZ
Range = String
Default = "Maximum clients reached, service unavailable."

This value entry specifies the message to be sent to an FTP client if the maximum number of clients has been reached or exceeded. This message indicates that the server is refusing additional clients because it is currently servicing the maximum number of connections (as specified in the FTP Service dialog box or the **MaxConnections** value in the Registry).

MsdosDirOutput

Data type = REG_DWORD
Range = 0 or 1
Default = 1 (true-that is, directory listings will look like MS-DOS)

This value entry specifies the default behavior for whether the output of the **list** command will look like the output of the MS-DOS **dir** command or the output of the UNIX ls command. This value also controls the direction of slashes in paths sent by the **pwd** command.

When this value is 1, directory listings will look like MS-DOS listings, and the path will contain backward slashes (\). If this value is 0, listings will look like UNIX listings, and the path will contain forward slashes (/).

The following Registry parameters can be set using the options available when configuring the FTP Server service in the Network Settings dialog box:

AllowAnonymous

AnonymousOnly

AnonymousUsername

ConnectionTimeout

HomeDirectory

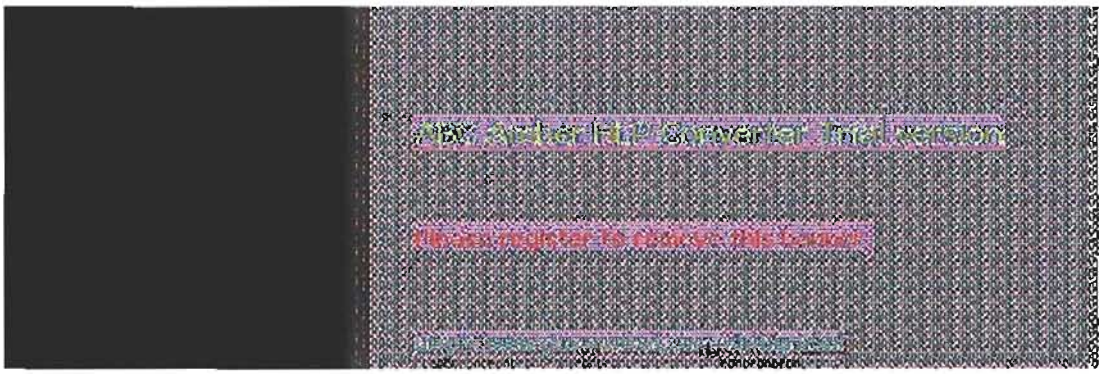
MaxConnections

The following Registry parameters can be set using the options available when you select the FTP Server icon in Control Panel and then choose the Security button:

ReadAccessMask

WriteAccessMask

The ranges of values that can be entered for these parameters in Registry Editor are the same as those described in the related dialog boxes earlier in this chapter. You should use only the FTP Server service dialog boxes to set these values.



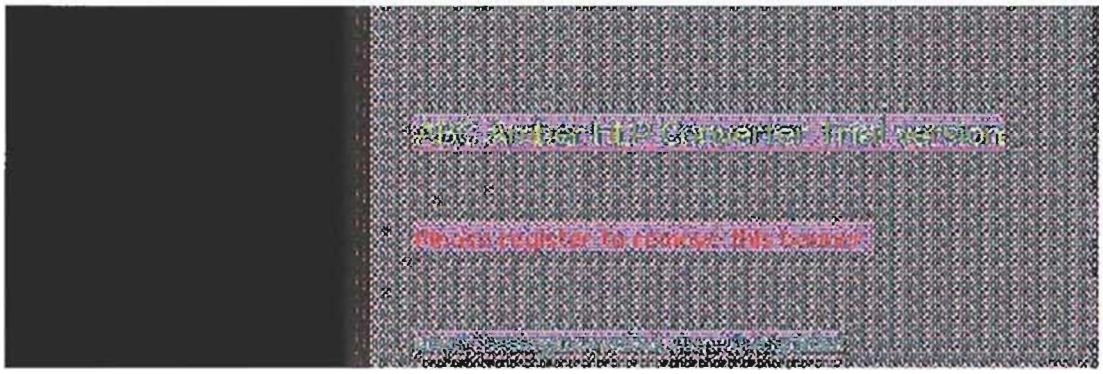
Using Performance Monitor with TCP/IP Services

This chapter describes the performance counters that can be charted in Performance Monitor so you can track performance of the IP protocols, FTP Server service traffic, and WINS servers.

The performance counters are described in the following topics in this chapter:

- Using Performance Monitor with TCP/IP
- Monitoring TCP/IP performance
- Monitoring FTP Server service traffic
- Monitoring WINS server performance

Important
To use the TCP/IP performance counters in Performance Monitor, you must install the SNMP service, as described in Chapter 2, "Installing and Configuring Microsoft TCP/IP and SNMP."

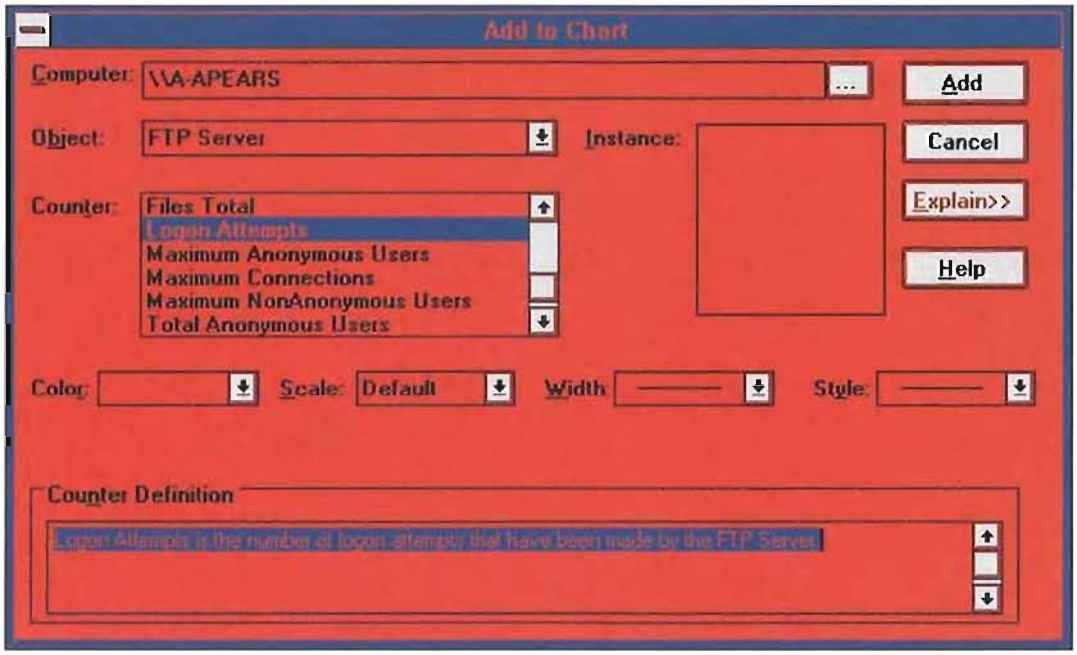


Using Performance Monitor with TCP/IP

After elements of Microsoft TCP/IP are installed, you can use Performance Monitor to track performance.

To use Performance Monitor with TCP/IP

1. In the Administrative Tools group in Program Manager, double-click Performance Monitor.
2. From the Edit menu, choose Add To Chart.



3. In the Computer list in the Add To Chart dialog box, select the computer you want to monitor.
4. In the Object list, select the TCP/IP-related process you want to monitor: FTP Server, ICMP, IP, Network Interface, TCP, UDP, or WINS Server.
5. In the Counter list, select the counters you want to monitor for each process, and then choose the Add button.

   For information about each counter, choose the Explain button, or see the definition tables later in this chapter.
6. When you have selected all the counters you want for a particular chart, choose the Done button.

For more information about using Performance Monitor, see Chapter 19, "Performance Monitor," in the *Windows NT Server System Guide*.

Monitoring TCP/IP Performance

Each of the different elements that make up the TCP/IP protocol suite can be monitored separately in Performance Monitor if SNMP services are installed on the computer.

To view counters specific to TCP/IP processes

- In the Add To Chart dialog box in Performance Monitor, select ICMP, IP, Network Interface, TCP, or UDP in the Object list.

The counters for each of these object types are described in the following sections.

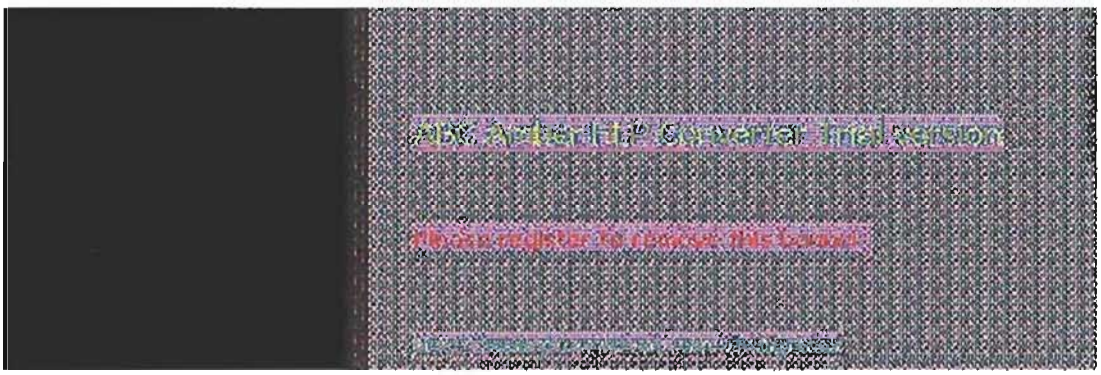
Monitoring TCP/IP Performance

ICMP Performance Counters

The ICMP Object Type includes those counters that describe the rates that Internet Control Message Protocol (ICMP) messages are received and sent by a certain entity using the ICMP protocol. It also describes various error counts for the ICMP protocol.

ICMP performance counter	Meaning
Messages Outbound Errors	The number of ICMP messages that this entity did not send because of problems discovered within ICMP, such as lack of buffers. This value should not include errors discovered outside the ICMP layer, such as the inability of IP to route the resultant datagram. In some implementations, there may be no types of error that contribute to this counter's value.
Messages Received Errors	The number of ICMP messages that the entity received, but determined as having errors (bad ICMP checksums, bad length, and so on).
Messages Received/Second	The rate at which ICMP messages are received by the entity. The rate includes those messages received in error.
Messages Sent/Second	The rate at which ICMP messages are attempted to be sent by the entity. The rate includes those messages sent in error.
Messages/Second	The total rate at which ICMP messages are received and sent by the entity. The rate includes those messages received or sent in error.
Received Address Mask	The number of ICMP Address Mask Request messages received.
Received Address Mask Reply	The number of ICMP Address Mask Reply messages received.
Received Destination Unreachable	The number of ICMP Destination Unreachable messages received.
Received Echo Reply/Second	The rate of ICMP Echo Reply messages received.
Received Echo/Second	The rate of ICMP Echo messages received.
Received Parameter Problem	The number of ICMP Parameter Problem messages received.
Received Redirect/Second	The rate of ICMP Redirect messages received.
Received Source Quench	The number of ICMP Source Quench messages received.
Received Time Exceeded	The number of ICMP Time Exceeded messages received.
Received Timestamp Reply/Second	The rate of ICMP Timestamp Reply messages received.
Received Timestamp/Second	The rate of ICMP Timestamp (request) messages received.

Sent Address Mask	The number of ICMP Address Mask Request messages sent.
Sent Address Mask Reply	The number of ICMP Address Mask Reply messages sent.
Sent Destination Unreachable	The number of ICMP Destination Unreachable messages sent.
Sent Echo Reply/Second	The rate of ICMP Echo Reply messages sent.
Sent Echo/Second	The rate of ICMP Echo messages sent.
Sent Parameter Problem	The number of ICMP Parameter Problem messages sent.
Sent Redirect/Second	The rate of ICMP Redirect messages sent.
Sent Source Quench	The number of ICMP Source Quench messages sent
Sent Time Exceeded	The number of ICMP Time Exceeded messages sent.
Sent Timestamp Reply/Second	The rate of ICMP Timestamp Reply messages sent.
Sent Timestamp/Second	The rate of ICMP Timestamp (request) messages sent



Monitoring TCP/IP Performance

IP Performance Counters

The IP Object Type includes those counters that describe the rates that Internet Protocol (IP) datagrams are received and sent by a certain computer using the IP protocol. It also describes various error counts for the IP protocol.

IP performance counter	Meaning
Datagrams Forwarded/Second	The rate of input datagrams for which this entity was not their final IP destination that resulted in an attempt to find a route to forward them to that final destination. In entities that do not act as IP Gateways, this rate will include only those packets that were Source-Routed via this entity, when the Source-Route option processing was successful.
Datagrams Outbound Discarded	The number of output IP datagrams for which no problems were encountered to prevent their transmission to their destination, but which were discarded (for example, for lack of buffer space.) This counter would include datagrams counted in Datagrams Forwarded if any such packets met this (discretionary) discard criterion.
Datagrams Outbound No Route	The number of IP datagrams discarded because no route could be found to transmit them to their destination. This counter includes any packets counted in Datagrams Forwarded that meet this "no route" criterion.
Datagrams Received Address Errors	The number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity. This count includes invalid addresses (for example, 0.0.0.0) and addresses of unsupported Classes (for example, Class E). For entities that are not IP gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
Datagrams Received Delivered/Second	The rate at which input datagrams are successfully delivered to IP user protocols (including ICMP).
Datagrams Received Discarded	The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (for example, for lack of buffer space). This counter does not include any datagrams discarded while awaiting reassembly.
Datagrams Received Header Errors	The number of input datagrams discarded because of errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, and so on.
Datagrams Received Unknown Protocol	The number of locally addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.

Datagrams Received/Second	The rate at which IP datagrams are received from the interfaces, including those in error.
Datagrams Sent/Second	The rate at which IP datagrams are supplied to IP for transmission by local IP user protocols (including ICMP). This counter does not include any datagrams counted in Datagrams Forwarded.
Datagrams/Second	The rate at which IP datagrams are received from or sent to the interfaces, including those in error. Any forwarded datagrams are not included in this rate.
Fragment Re-assembly Failures	The number of failures detected by the IP reassembly algorithm (for whatever reason: timed out, errors, and so on). This is not necessarily a count of discarded IP fragments, because some algorithms (notably RFC 815) can lose track of the number of fragments by combining them as they are received.
Fragmentation Failures	The number of IP datagrams that have been discarded because they needed to be fragmented at this entity but could not be, for example, because their "Don't Fragment" flag was set.
Fragmented Datagrams/Second	The rate at which datagrams are successfully fragmented at this entity.
Fragments Created/Second	The rate at which IP datagram fragments have been generated as a result of fragmentation at this entity.
Fragments Re-assembled/Second	The rate at which IP fragments are successfully reassembled.
Fragments Received/Second	The rate at which IP fragments that need to be reassembled at this entity are received.

Monitoring TCP/IP Performance

Network Interface Performance Counters for TCP/IP

The Network Interface Object Type includes those counters that describe the rates at which bytes and packets are received and sent over a network TCP/IP connection. It also describes various error counts for the same connection.

Network Interface counter	Meaning
Bytes Received/Second	The rate at which bytes are received on the interface, including framing characters.
Bytes Sent/Second	The rate at which bytes are sent on the interface, including framing characters.
Bytes Total/Second	The rate at which bytes are sent and received on the interface, including framing characters.
Current Bandwidth	An estimate of the interface's current bandwidth in bits per second (bps). For interfaces that do not vary in bandwidth or for those where no accurate estimation can be made, this value is the nominal bandwidth.
Output Queue Length	The length of the output packet queue (in packets.) If this is longer than 2, delays are being experienced and the bottleneck should be found and eliminated if possible. Since the requests are queued by NDIS in this implementation, this will always be 0
Packets Outbound Discarded	The number of outbound packets that were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
Packets Outbound Errors	The number of outbound packets that could not be transmitted because of errors.
Packets Received Discarded	The number of inbound packets that were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space
Packets Received Errors	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Packets Received Non-Unicast/Second	The rate at which non-unicast (that is, subnet broadcast or subnet multicast) packets are delivered to a higher-layer protocol.
Packets Received Unicast/Second	The rate at which (subnet) unicast packets are delivered to a higher-layer protocol.
Packets Received Unknown	The number of packets received via the interface that were discarded because of an unknown or unsupported protocol.
Packets Received/Second	The rate at which packets are received on the network interface.

Packets Sent Non-Unicast/Second	The rate at which packets are requested to be transmitted to non-unicast (that is, subnet broadcast or subnet multicast) addresses by higher-level protocols. The rate includes the packets that were discarded or not sent.
Packets Sent Unicast/Second	The rate at which packets are requested to be transmitted to subnet-unicast addresses by higher-level protocols. The rate includes the packets that were discarded or not sent.
Packets Sent/Second	The rate at which packets are sent on the network interface.
Packets/Second	The rate at which packets are sent and received on the network interface.

Monitoring TCP/IP Performance

TCP Performance Counters

The TCP Object Type includes those counters that describe the rates that Transmission Control Protocol (TCP) segments are received and sent by a certain entity using the TCP protocol. In addition, it describes the number of TCP connections that are in each of the possible TCP connection states.

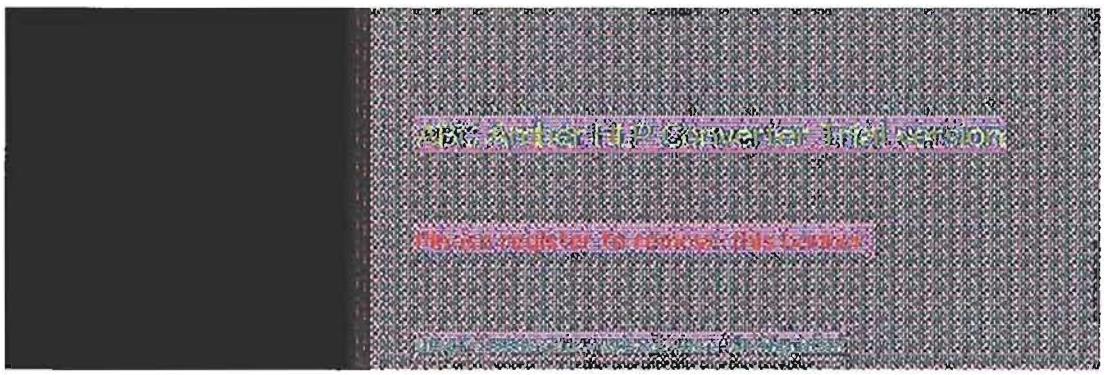
TCP performance counter	Meaning
Connection Failures	The number of times TCP connections have made a direct transition to the CLOSED state from the SYN-SENT state or the SYN-RCVD state, plus the number of times TCP connections have made a direct transition to the LISTEN state from the SYN-RCVD state.
Connections Active	The number of times TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state.
Connections Established	The number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT.
Connections Passive	The number of times TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state.
Connections Reset	The number of times TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state.
Segments Received/Second	The rate at which segments are received, including those received in error. This count includes segments received on currently established connections.
Segments Retransmitted/Second	The rate at which segments are retransmitted, that is, segments transmitted containing one or more previously transmitted bytes.
Segments Sent/Second	The rate at which segments are sent, including those on current connections, but excluding those containing only retransmitted bytes.
Segments/Second	The rate at which TCP segments are sent or received using the TCP protocol.

Monitoring TCP/IP Performance

UDP Performance Counters

The UDP Object Type includes those counters that describe the rates that User Datagram Protocol (UDP) datagrams are received and sent by a certain entity using the UDP protocol. It also describes various error counts for the UDP protocol.

UDP performance counter	Meaning
Datagrams No Port/Second	The rate of received UDP datagrams for which there was no application at the destination port.
Datagrams Received Errors	The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.
Datagrams Received/Second	The rate at which UDP datagrams are delivered to UDP users.
Datagrams Sent/Second	The rate at which UDP datagrams are sent from the entity.
Datagrams/Second	The rate at which UDP datagrams are sent or received by the entity.



Monitoring FTP Server Traffic

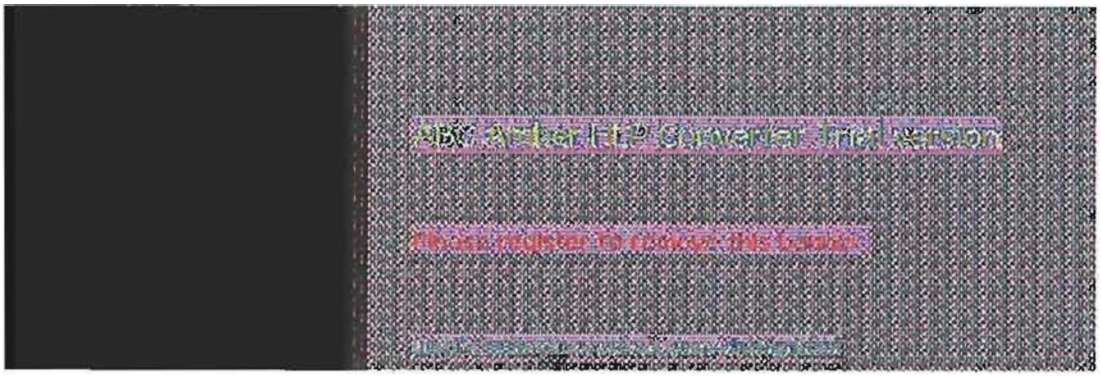
When you install the FTP Server services, the necessary software is also installed so that you can monitor and graph various FTP Server statistics using Performance Monitor. Using Performance Monitor to view activity on remote Windows NT systems makes FTP Server administration more convenient when you are administering multiple Windows NT FTP Servers.

To view counters specific to the FTP Server service

- In the Performance Monitor window, select FTP Server in the Object list.

The FTP Server performance counters are cleared each time you start and stop the FTP Server service.

FTP performance counter	Meaning
Bytes Received/Second	The rate at which data bytes are received by the FTP Server.
Bytes Sent/Second	The rate at which data bytes are sent by the FTP Server.
Bytes Total/Second	The sum of Bytes Sent/Second and Bytes Received/Second. This is the total rate of bytes transferred by the FTP Server.
Connection Attempts	The number of connection attempts that have been made to the FTP Server.
Current Anonymous Users	The number of anonymous users currently connected to the FTP Server.
Current Connections	The current number of connections to the FTP Server.
Current NonAnonymous Users	The number of nonanonymous users currently connected to the FTP Server.
Files Received	The total number of files received by the FTP Server.
Files Sent	The total number of files sent by the FTP Server.
Files Total	The sum of Files Sent and Files Received. This is the total number of files transferred by the FTP Server.
Logon Attempts	The number of logon attempts that have been made to the FTP Server.
Maximum Anonymous Users	The maximum number of anonymous users simultaneously connected to the FTP Server.
Maximum Connections	The maximum number of simultaneous connections to the FTP Server.
Maximum NonAnonymous Users	The maximum number of nonanonymous users simultaneously connected to the FTP Server.
Total Anonymous Users	The total number of anonymous users that have ever connected to the FTP Server.
Total NonAnonymous Users	The total number of nonanonymous users that have ever connected to the FTP Server.


ABC Amber IEC® Converter Trial Version
Click register to remove this banner

Monitoring WINS Server Performance

When you install a WINS server and SNMP services, counters are automatically installed so that you can use Performance Monitor to view WINS Server service performance.

To view counters specific to the WINS Server service

WINS performance counter	Meaning
Failed Queries/Second	The total number of failed queries per second.
Failed Releases/Second	The total number of failed releases per second.
Group Conflicts/Second	The rate at which group registrations received by the WINS server resulted in conflicts with records in the database.
Group Registrations/Second	The rate at which group registrations are received by the WINS server.
Group Renewals/Second	The rate at which group renewals are received by the WINS server.
Queries/Second	The total number of queries per second, which is the rate at which queries are received by the WINS server.
Releases/Second	The total number of releases per second, which is the rate at which releases are received by the WINS server.
Successful Queries/Second	The total number of successful queries per second.
Successful Releases/Second	The total number of successful releases per second.
Total Number of Conflicts/Second	The sum of the Unique and Group conflicts per second, which is the total rate at which conflicts were seen by the WINS server.
Total Number of Registrations/Second	The sum of the Unique and Group registrations per second. This is the total rate at which registrations are received by the WINS server.
Total Number of Renewals/Second	The sum of the Unique and Group registrations per second, which is the total rate at which renewals are received by the WINS server.
Unique Conflicts/Second	The rate at which unique registrations and renewals received by the WINS server resulted in conflicts with records in the database.
Unique Registrations/Second	The rate at which unique registrations are received by the WINS server.
Unique Renewals/Second	The rate at which unique renewals are received by the WINS server.

Internetwork Printing with TCP/IP

Users on any Microsoft networking computer can print to direct-connect TCP/IP printers or to printers that are physically attached to UNIX computers if at least one Windows NT computer has Microsoft TCP/IP printing installed.

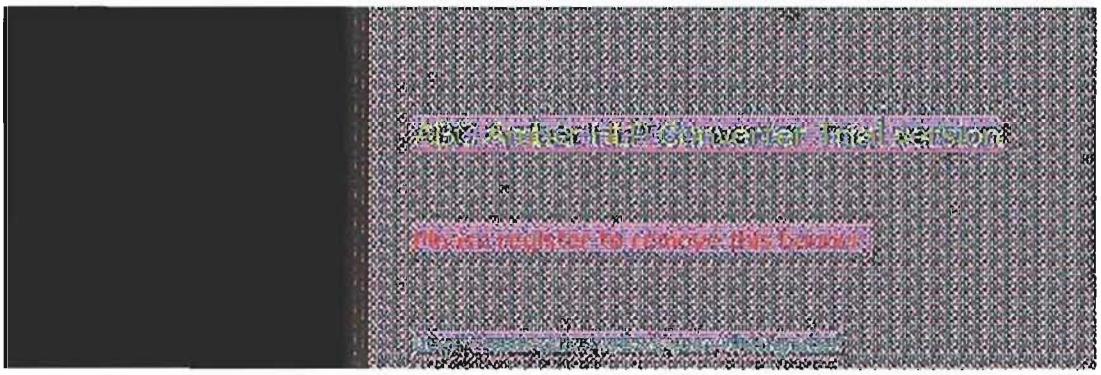
Microsoft TCP/IP printing conforms with Request for Comment (RFC) 1179.

This chapter describes how to create a TCP/IP printer when TCP/IP is installed on a Windows NT computer and how to print to a Windows NT print server from a UNIX computer.

The topics in this chapter include:

- Overview of TCP/IP printing
- Setting up Windows NT for TCP/IP printing
- Creating a printer for TCP/IP printing
- Printing to Windows NT from UNIX clients

For complete information about working with printers, see Chapter 6, "Print Manager," in the *Windows NT System Guide*.



Overview of TCP/IP Printing

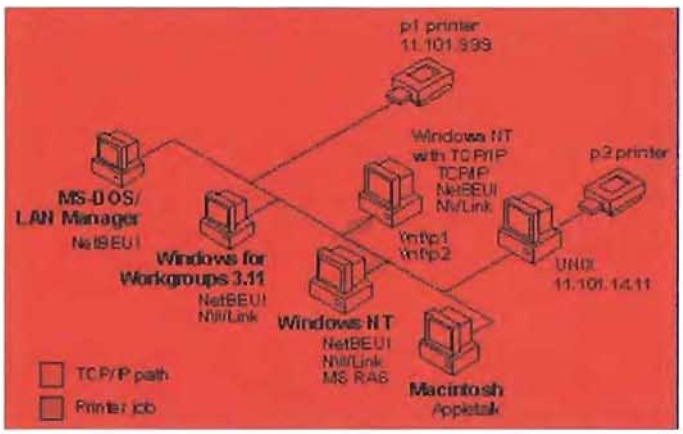
In a Windows NT internetwork with multiple kinds of computers and operating systems, users can take advantage of Microsoft TCP/IP to easily print to computers that are connected through a UNIX computer or that are connected directly to the network (via a built-in network adapter card or through a serial/parallel ethernet print server).

Such an internetwork might include computers running Windows NT Workstation and Windows NT Server, plus computers with only Microsoft Windows for Workgroups 3.11 or MS-DOS with LAN Manager networking software.

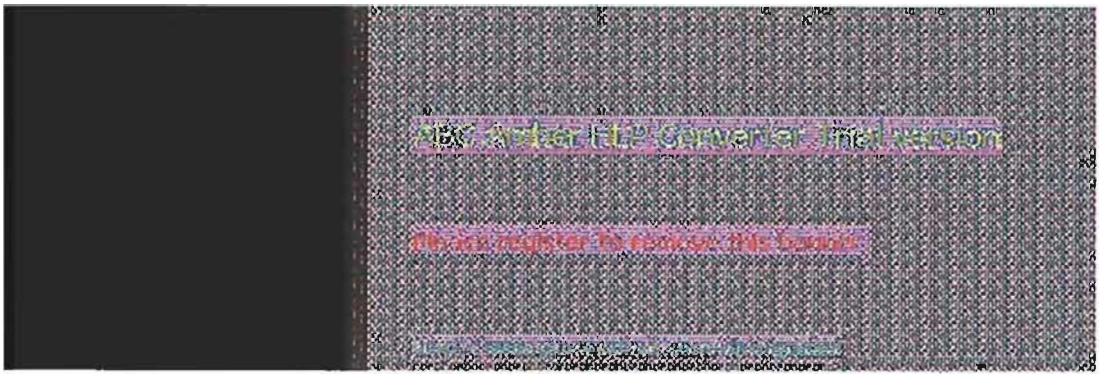
To take advantage of the printing capabilities of Microsoft TCP/IP, only the single Windows NT computer that defines a TCP/IP printer needs to have TCP/IP installed. The other client computers do not need to have TCP/IP installed. All other computers can print to the TCP/IP printers over any protocol they share with the Windows NT TCP/IP print server. That is, the computer acting as the Windows NT TCP/IP print server must be configured with all protocols used by any clients that will be printing to the TCP/IP printer.

Any Windows NT computer with TCP/IP printing installed can print directly to these kinds of printers and can function as a gateway for other network users.

In the following sample configuration of a Microsoft network, all computers can connect to printers named **\\nt\p1** and **\\nt\p2** on the network. The Windows NT computer with Microsoft TCP/IP installed created these TCP/IP printers, which consist of a direct-connect printer and a printer connected to a UNIX computer. The Windows NT computer with TCP/IP is named **nt** in this example, and the printers are named **p1** and **p2**, respectively.



Printing to TCP/IP or UNIX Printers Using Microsoft TCP/IP


ABC Amber FLP Converter Trial version

Setting Up Windows NT for TCP/IP Printing

Any Windows NT computer can be used to create a TCP/IP printer if Microsoft TCP/IP is installed with TCP/IP printing support.

To configure a Windows NT computer for TCP/IP printing

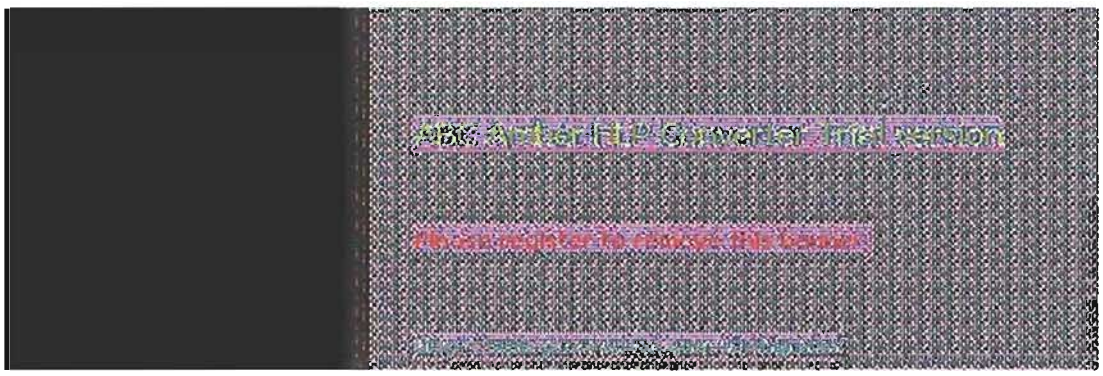
1. Start the Network option in Control Panel. When the Network Settings dialog box appears, choose the Add Software button to display the Add Network Software dialog box.
2. Select TCP/IP Protocol And Related Components in the Network Software list box, and then choose the Continue button.
3. In the Windows NT TCP/IP Installation Options dialog box, check the TCP/IP Network Printing Support option.

   If Microsoft TCP/IP is not already installed on this computer, check the other options you want, as described in Chapter 2, "Installing and Configuring Microsoft TCP/IP and SNMP."
4. Choose the OK button. Windows NT Setup displays a message asking for the full path to the Windows NT distribution files. Provide the appropriate location, and choose the Continue button.

   All necessary files are copied to your hard disk.
5. If the Enable Automatic DHCP Configuration option is not checked in the Windows NT TCP/IP Installation Options dialog box, you must complete all the required procedures for manually configuring TCP/IP as described in "Configuring TCP/IP" in Chapter 2.

   When the Network Settings dialog box reappears after you finish configuring TCP/IP, choose the Close button, and then restart your computer for the changes to take effect.

You can now create a TCP/IP printer on this Windows NT computer.



Creating a Printer for TCP/IP Printing

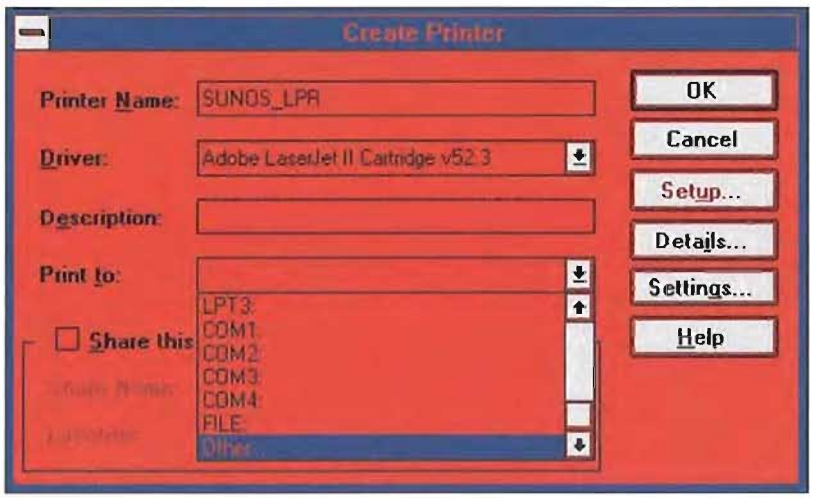
You can use Print Manager to create a TCP/IP printer in the same way that you create any printer to be used on a Windows NT network. You need the following information to create a TCP/IP printer:

- The IP identifier of the host where the printer is connected. This can be the DNS name or the IP address. A direct-connect printer has its own IP identifier. For a printer connected to a UNIX computer, this is the computer's IP identifier.
- The printer name as it is identified on the host. This is the name defined on the UNIX computer or the name defined by the manufacturer for the direct-connect printer.

The computer where you create the TCP/IP printer must have TCP/IP installed and configured with the TCP/IP Network Printing Support option, as described in Chapter 2.

To create a TCP/IP printer

1. From the Printer menu in Print Manager, choose Create Printer.



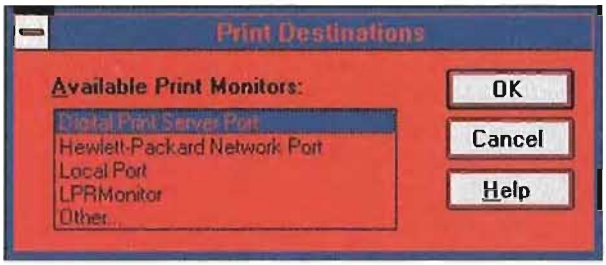
2. In the Printer Name box of the Create Printer dialog box, type a name of up to 32 characters. This name appears in the title bar of the printer window, and Windows NT users see this name when connecting to this printer if it is shared.

   This name can be the same as the printer name as it is identified on the printer's UNIX host, but it does not have to be.

   For a direct-connect printer, see the hardware documentation to find the name by which the network printer identifies the print queue.

3. In the Driver list, select the appropriate driver and, optionally, type text to inform network users about the printer in the Description box.

4. In the Print To box, select Other to display the Print Destinations dialog box.



5. In the Available Print Destinations list, select LPR Print Monitor, and then choose OK.

6. In the Name Or Address Of Host Providing LPD box of the Add LPR Compatible Printer dialog box, type the DNS name or IP address of the host for the printer you are adding.

   This can be the DNS name or IP address of the direct-connect TCP/IP printer or of the UNIX computer to which the printer is connected. The DNS name can be the name specified for the host in the HOSTS file.

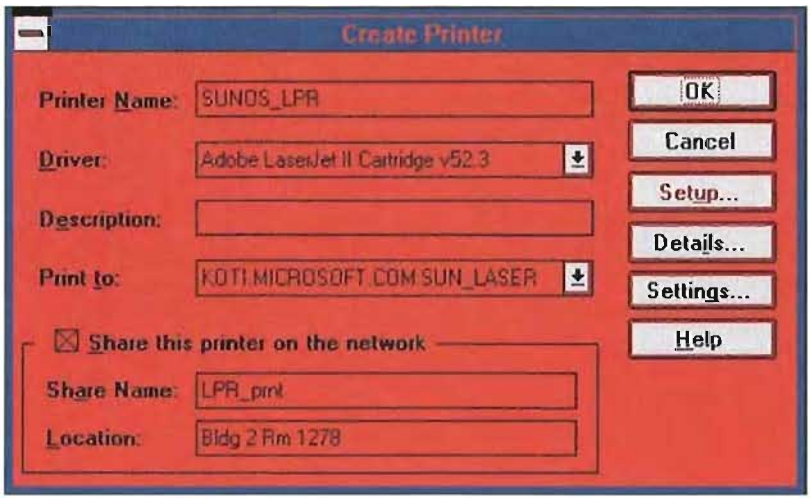
   LPR stands for Line Printing utility, and LPD stands for Line Printing Daemon, which is how these elements are known on UNIX.

7. In the Name Of Printer On That Machine box, type the name of the printer as it is identified by the host, which is either the direct-connect printer itself or the UNIX computer.

   For example, you might have a UNIX computer running the print server component (**lpd**) with which the TCP/IP printer you are creating will interact. If **lpd** recognizes a printer attached to the UNIX computer by the name Crisp, the name you should type in this box is **Crisp**.

   For a direct-connect printer, this is whatever name was used to create the printer while running **lpd**.

8. When the Create Printer dialog box reappears, check the Share This Printer On The Network option if this definition is being created on a Windows NT computer that will serve as a print server for other users to access this printer.

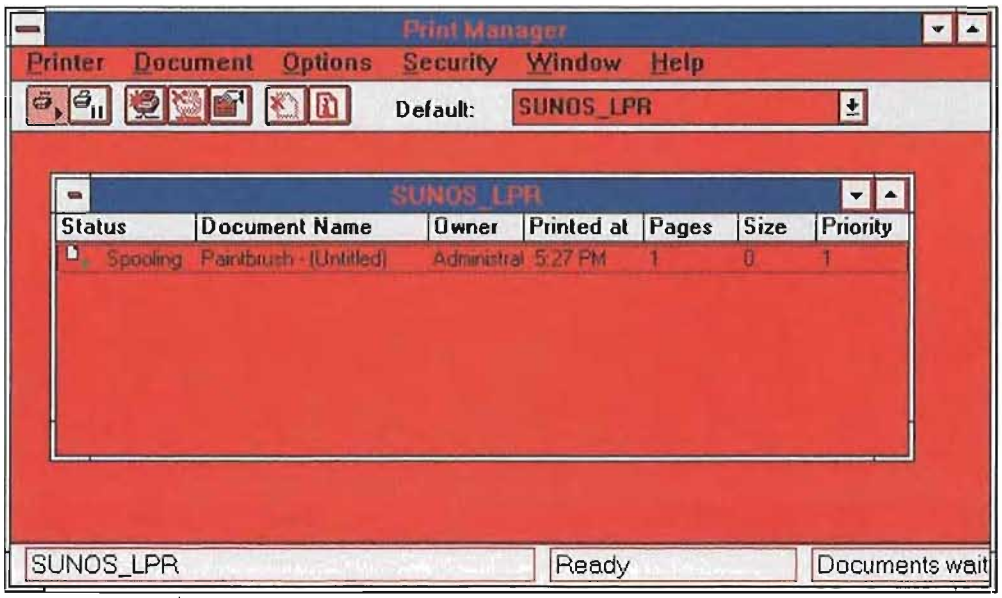


9. By default, in the Share Name box, Printer Manager creates a shared resource name that is compatible with MS-DOSbased computers. You can edit this name, which users will see when browsing to find this printer on the network.

10. Optionally, in the Location box, you can type information about where this printer is located. Users can see this location information when they connect to the printer.

11. Complete any other configuration information in the Create Printer dialog box, as described in Chapter 6 of the *Windows NT System Guide*, and then choose the OK button.

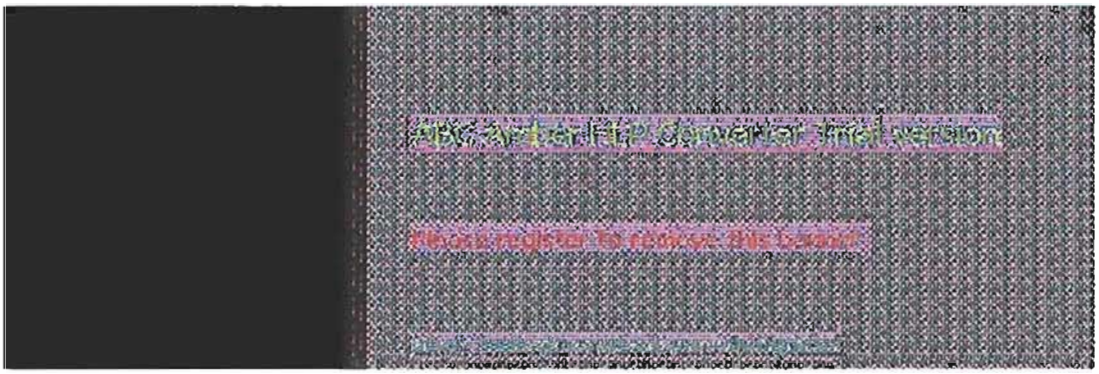
In Print Manager, the printer name you specified in the Create Printer dialog box appears in the title bar of the printer's window. For client computers configured with Microsoft Network Client version 2.0 for MS-DOS, users will see only the shared name, not the printer name. Users who connect to this TCP/IP printer can select it and print to it from applications like any other printer. Users and administrators can use Print Manager to secure and audit the use of the printer and change its properties.



Tip

You can use the **lpr** connectivity utility at the command prompt to print a file to a host running an LPD server. You can also use the **lpq** diagnostic utility to obtain the status of a print queue on a

host running the LPD server. For information, see the entries for **lpr** and **lpq** in Chapter 11, "Utilities Reference."



Printing to Windows NT from UNIX Clients

The Lpdsvc service is the server side of TCP/IP printing for UNIX clients. If any UNIX clients on the network want to print to a printer connected to a Windows NT computer, this service needs to be running on the Windows NT computer so it can accept requests from the UNIX clients. The Lpdsvc service supports any print format, including plain-text. It does not perform any additional processing.

To start or stop the Lpdsvc service

- At the command prompt, type **net start lpdsvc** or **net stop lpdsvc** and press Enter.

  Or

  In Control Panel, choose the Services option. Then select Lpdsvc in the Service list and choose the Start button.

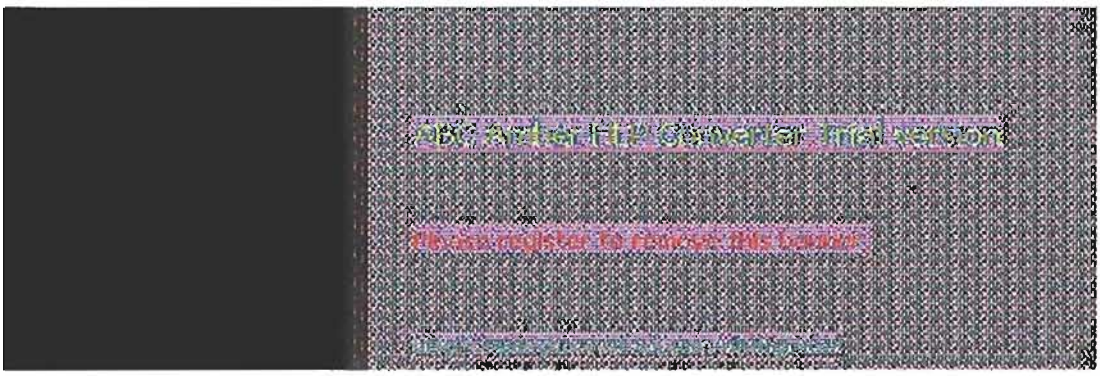
On the UNIX computer, you can use the Windows NT printer by typing a command such as the following:

lpr -S *NTHost* -P *LpdPrinter myfile.txt*

Where:

- *NTHost* is the Windows NT Server running the Lpdsvc service. This Windows NT computer should be listed in the HOSTS file on the UNIX computer or on the DNS server.
- *LpdPrinter* is the name of the printer created on *NTHost*.
- *myfile.txt* is the file to be printed.

The Lpdsvc service is independent of the Lprmon service. The Lprmon service runs automatically to allow a Windows NT computer (and all clients who can access this computer) to print to a printer connected to a UNIX system, as described in the previous section.



Troubleshooting TCP/IP

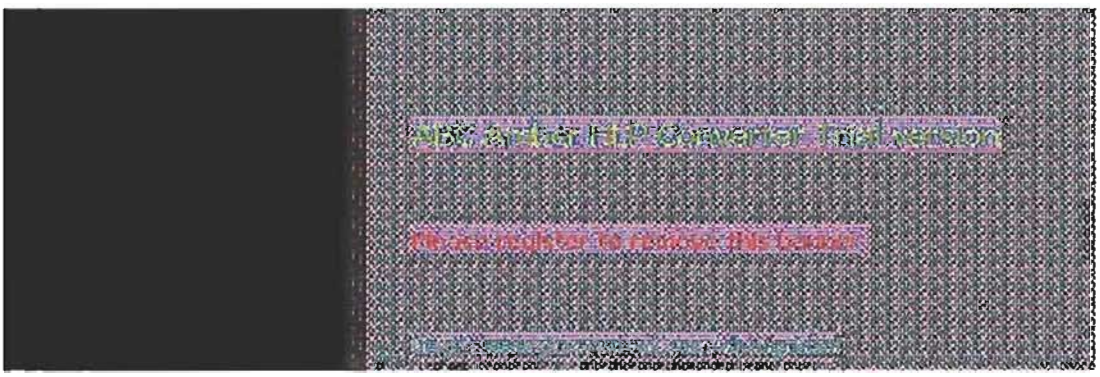
The following diagnostic utilities included with Microsoft TCP/IP can be used to find solutions to TCP/IP networking problems.

Utility	Usage
arp	View the ARP (address resolution protocol) table on the local computer to detect invalid entries.
hostname	Print the name of the current host.
ipconfig	Display current TCP/IP network configuration values, and update or release TCP/IP network configuration values.
nbtstat	Check the state of current NetBIOS over TCP/IP connections, update the LMHOSTS cache, and determine the registered name and scope ID.
netstat	Display protocol statistics and the state of current TCP/IP connections.
ping	Verify whether TCP/IP is configured correctly and that a remote TCP/IP system is available.
tracert	Check the route to a remote system.

For complete details about the utilities included with Windows NT, see Chapter 11, "Utilities Reference." See also the online Command Reference.

These other Windows NT tools can be used for TCP/IP troubleshooting:

- Microsoft SNMP service, to supply statistical information to SNMP management systems, as described in Chapter 2, "Installing Microsoft TCP/IP and SNMP."
- Event Viewer, to track errors and events, as described in the Event Viewer chapter in the *System Guide*.
- Performance Monitor, to analyze TCP/IP, FTP, and WINS server performance, as described in Chapter 8, "Using Performance Monitor with TCP/IP Services." (Microsoft SNMP must be installed if you want to monitor TCP/IP.)
- Registry Editor, to browse and edit Registry parameters, as described in README.WRI in your *systemroot* directory.



Troubleshooting IP Configuration

If you have trouble installing Microsoft TCP/IP on your computer, follow the suggestions in the error messages. You can also use the **ping** utility to isolate network hardware problems and incompatible configurations, allowing you to verify a physical connection to a remote computer.

Use the **ping** utility to test both the host name and the IP address of the host. For the syntax and description of the **ping** command, see Chapter 11, "Utilities Reference."

To test TCP/IP using the ping utility

1. If the computer was configured using DHCP, use **ipconfig** to learn the IP address.
2. Use **ping** to check the loopback address by typing **ping 127.0.0.1** and pressing ENTER at the command prompt. The computer should respond immediately.

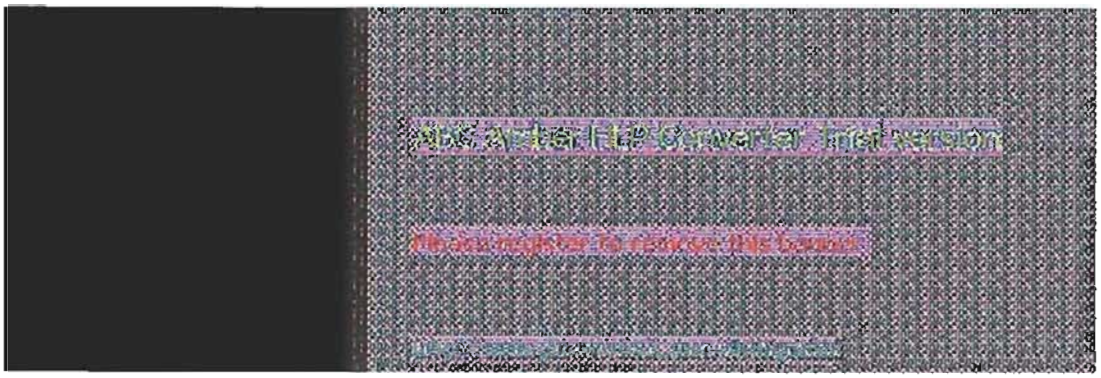
   If **ping** is not found or the command fails, check the event log with Event Viewer and look for problems reported by Setup or the TCP/IP service.
3. To determine whether you configured IP properly, use **ping** with the IP address of your computer, your default gateway, and a remote host.

If you cannot use **ping** successfully at any point, check the following:

- The computer was restarted after TCP/IP was installed and configured
- The local computer's IP address is valid and appears correctly in the TCP/IP Configuration dialog box
- The IP address of the default gateway and remote host are correct
- IP routing is enabled and the link between routers is operational

If you can use **ping** to connect to other Windows NT computers on a different subnet but cannot connect through File Manager or with **net use** *\\server\share*, check the following:

- The computer is WINS-enabled (if the network includes WINS servers).
- The WINS server addresses are correct, and the WINS servers are functioning.
- The correct computer name was used.
- The target host uses NetBIOS. If not, you must use FTP or Telnet to make a connection; in this case, the target host must be configured with the FTP server daemon or Telnet server daemon, and you must have correct permissions on the target host.
- The scope ID on the target host is the same as the local computer.
- A router exists between your system and the target system.
- LMHOSTS contains correct entries, so that the computer name can be resolved. For more information, see "Troubleshooting Name Resolution Problems" later in this chapter.
- The computer is not configured to use WINS.



Troubleshooting IP Configuration

Troubleshooting Name Resolution Problems

If the IP address responds but the host name does not when you use **ping**, you have a name resolution problem. In this case, use the following lists of common problems in name resolution to find solutions.

Name Resolution Problems in HOSTS

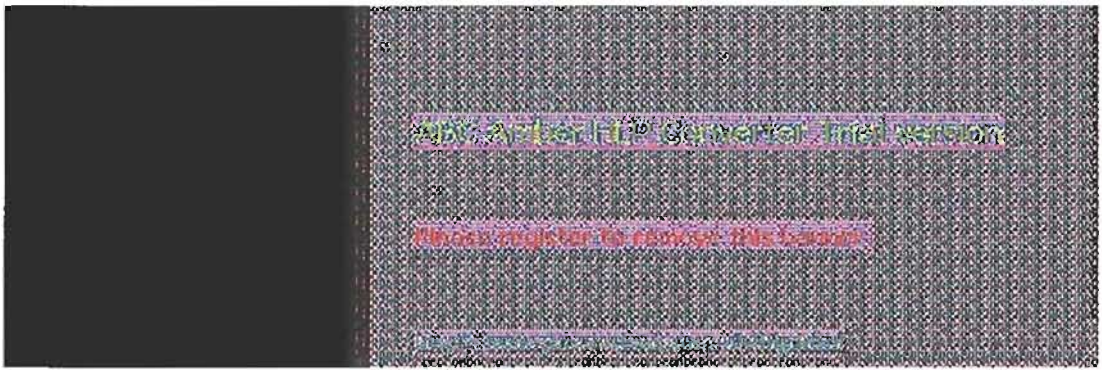
These problems can occur because of errors related to the HOSTS file:

- The HOSTS file or DNS do not contain the particular host name.
- The host name in the HOSTS file or in the command is misspelled or uses different capitalization. (Host names are case-sensitive.)
- An invalid IP address is entered for the host name in the HOSTS file.
- The HOSTS file contains multiple entries for the same host on separate lines.
- A mapping for a computer name-to-IP address was mistakenly added to the HOSTS file (rather than LMHOSTS).

Name Resolution Problems in LMHOSTS

These problems can occur because of errors related to the LMHOSTS file:

- The LMHOSTS file does not contain an entry for the remote server.
- The computer name in LMHOSTS is misspelled. (Notice that LMHOSTS names are converted to uppercase.)
- The IP address for a computer name in LMHOSTS is not valid.



Troubleshooting IP Configuration

Troubleshooting Other Connection Problems

In addition to **ping**, the other diagnostic utilities such as **netstat** and **nbtstat** can be used to find and resolve connection problems. Although this is not a complete list, these examples show how you might use these utilities to track down problems on the network.

To determine the cause of Error 53 when connecting to a server

1. If the computer is on the local subnet, confirm that the name is spelled correctly and that the target computer is running TCP/IP as well. If the computer is not on the local subnet, be sure that its name and IP address mapping are available in the LMHOSTS file or the WINS database.

   Error 53 is returned if name resolution fails for a particular computer name.

2. If all TCP/IP elements appear to be installed properly, use **ping** with the remote computer to be sure that its TCP/IP software is working.

To determine the cause of long connect times after adding to LMHOSTS

- Because this behavior can occur with a large LMHOSTS file with an entry at the end of the file, mark the entry in LMHOSTS as a preloaded entry by following the mapping with the #PRE tag. Then use the **nbtstat -R** command to update the local name cache immediately.

  Or

  Place the mapping higher in the LMHOSTS file.

  As discussed in Chapter 6, the LMHOSTS file is parsed sequentially to locate entries without the #PRE keyword. Therefore, you should place frequently used entries near the top of the file and place the #PRE entries near the bottom.

To determine the cause of connection problems when specifying a server name

- Use the **nbtstat -n** command to determine what name the server registered on the network.

  The output of this command lists several names that the computer has registered. A name resembling the computer's computer name should be present. If not, try one of the other unique names displayed by **nbtstat**.

  The **nbtstat** utility can also be used to display the cached entries for remote computers from either #PRE entries in LMHOSTS or recently resolved names. If the name the remote computers are using for the server is the same, and the other computers are on a remote subnet, be sure that they have the computer's mapping in their LMHOSTS files.

To determine why only IP addresses work for connections to foreign systems but not host names

1. Make sure that the appropriate HOSTS file and DNS setup have been configured for the computer by checking the host name resolution configuration using the Network icon in Control Panel and then choosing the DNS button in the TCP/IP Configuration dialog box.

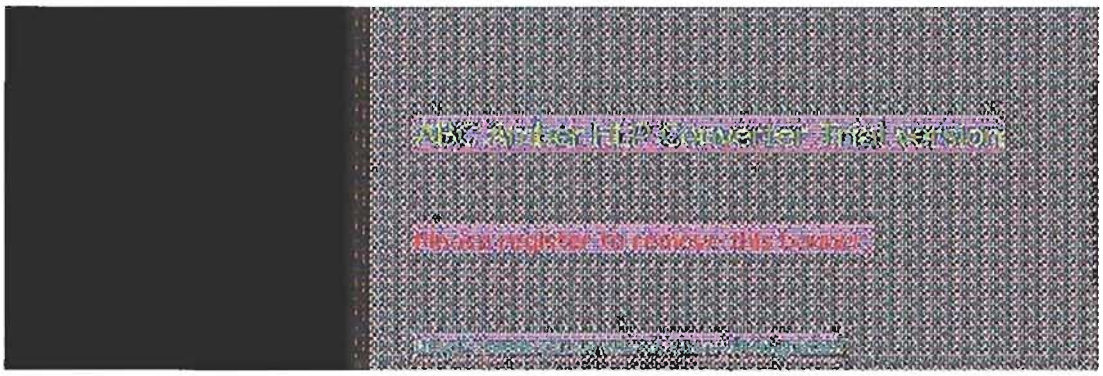
2. If you are using a HOSTS file, make sure that the name of the remote computer is spelled the same and capitalized the same in the file and by the application using it.

3. If you are using DNS, be sure that the IP addresses of the DNS servers are correct and in the

proper order. Use **ping** with the remote computer by typing both the host name and IP address to determine whether the host name is being resolved properly.

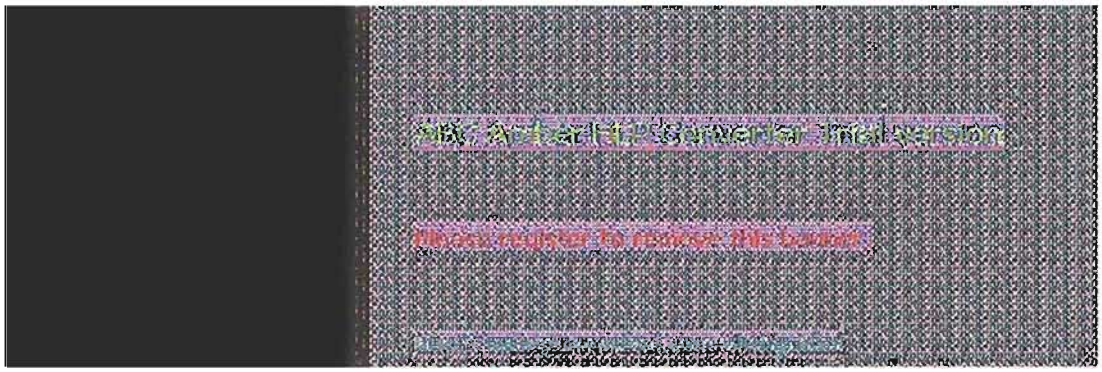
- **To determine why a TCP/IP connection to a remote computer is not working properly**
  - Use the **netstat -a** command to show the status of all activity on TCP and UDP ports on the local computer.

    The state of a good TCP connection is usually established with 0 bytes in the send and receive queues. If data is blocked in either queue or if the state is irregular, there is probably a problem with the connection. If not, you are probably experiencing network or application delay.



Troubleshooting Other Problems

This section presents some possible TCP/IP symptoms with recommendations for using the diagnostic utilities to determine the source of the problems.

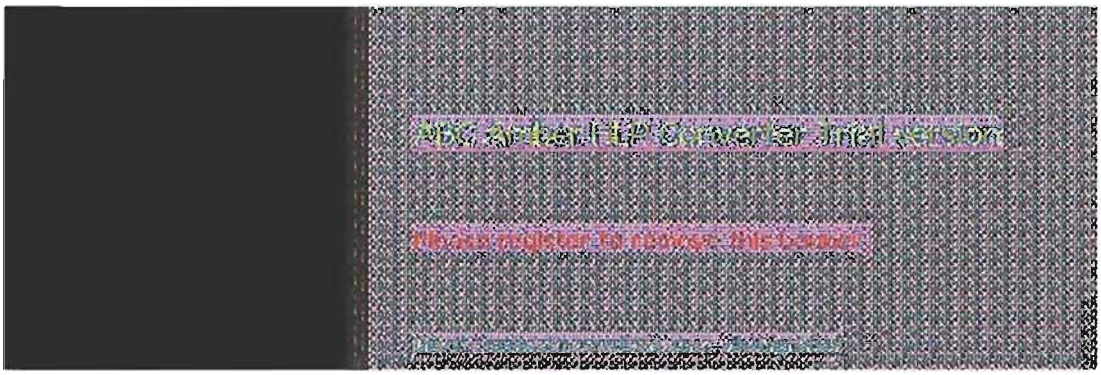


Troubleshooting Other Problems

Troubleshooting the FTP Server Service

- **To determine whether the FTP Server service is installed correctly**
  - Use **ftp** on the local computer by typing the IP loopback address from the command line; for example, type **ftp 127.0.0.1** and press ENTER.

    The interaction with the server locally is identical to the interaction expected for other Windows NT (and most UNIX) clients. You can also use this utility to determine whether the directories, permissions, and so on are configured properly for the FTP Server service.



Troubleshooting Other Problems

Troubleshooting Telnet

To determine why the banner displayed with Telnet identifies a different computer, even when specifying the correct IP address

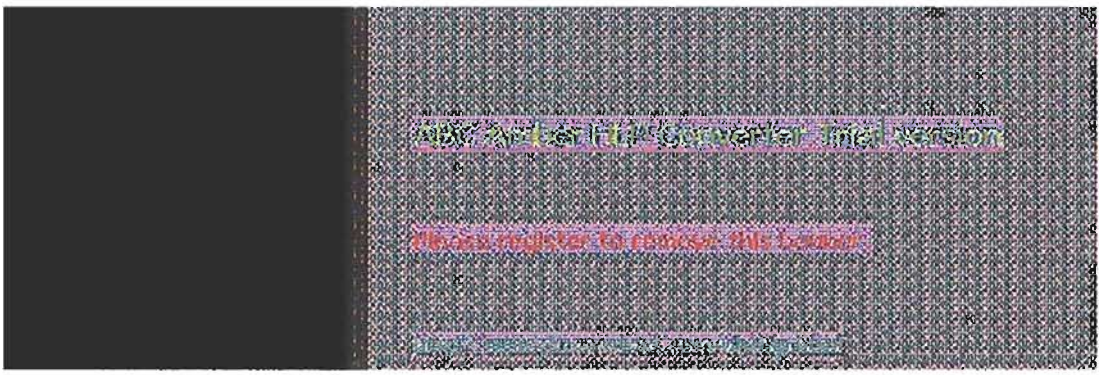
1. Make sure the DNS name and hosts table are up to date.

2. Make sure that two computers on the same network are not mistakenly configured with the same IP address.

   The ethernet and IP address mapping is done by the ARP (address resolution protocol) module, which believes the first response it receives. Therefore, the impostor computer's reply sometimes comes back before the intended computer's reply.

   These problems are difficult to isolate and track down. Use the **arp -g** command to display the mappings in the ARP cache. If you know the ethernet address for the intended remote computer, you can easily determine whether the two match. If not, use **arp -d** to delete the entry, then use **ping** with the same address (forcing an ARP), and check the ethernet address in the cache again by using **arp -g**.

   Chances are that if both computers are on the same network, you will eventually get a different response. If not, you may have to filter the traffic from the impostor host to determine the owner or location of the system.



Troubleshooting Other Problems

Troubleshooting Gateways

- **To determine the cause of the message, "Your default gateway does not belong to one of the configured interfaces..." during Setup**
  - Find out whether the default gateway is located on the same logical network as the computer's network adapter by comparing the network ID portion of the default gateway's IP address with the network ID(s) of any of the computer's network adapters.

    For example, a computer with a single network adapter configured with an IP address of 102.54.0.1 and a subnet mask of 255.255.0.0 would require that the default gateway be of the form 102.54.*a.b* because the network ID portion of the IP interface is 102.54.

Troubleshooting TCP/IP Database Files

The following UNIX-style database files are stored in the *\systemroot*\SYSTEM32\DRIVERS\ETC when you install Microsoft TCP/IP:

Filename	Use
HOSTS	Provides hostname-to-IP address resolution for Windows Sockets applications
LMHOSTS	Provides NetBIOS name-to-IP address resolution for Windows networking
NETWORKS	Provides network name-to-network ID resolution for TCP/IP management
PROTOCOLS	Provides protocol name-to-protocol ID resolution for Windows Sockets applications
SERVICES	Provides service name-to-port ID resolution for Windows Sockets applications

To troubleshoot any of these files on a local computer:

- Make sure the format of entries in each file matches the format defined in the sample file originally installed with Microsoft TCP/IP.
- Check for spelling or capitalization errors.
- Check for invalid IP addresses and identifiers.

Utilities Reference

This chapter is a reference for using Microsoft TCP/IP utilities, which provide diagnostic and connectivity utilities for network and connectivity administration. These client utilities are provided for file transfer, terminal emulation, and network diagnostics. Besides the connectivity support built into Windows NT, some third-party vendors are developing advanced connectivity utilities such as X Window servers, Network File System (NFS) implementations, and so on.

Diagnostic commands help you detect TCP/IP networking problems. *Connectivity commands* allow users to interact with and use resources on non-Microsoft hosts such as UNIX workstations. The following commands are included:

- Diagnostic commands: **arp**, **hostname**, **ipconfig**, **lpq**, **nbtstat**, **netstat**, **ping**, **route**, and **tracert**
- Connectivity commands: **finger**, **ftp**, **lpr**, **rcp**, **rexec**, **rsh**, **telnet**, and **tftp**

Important

The **ftp**, **ftpsvc**, **rexec**, and **telnet** utilities all rely on password authentication by the remote computer. Passwords are not encrypted before being sent over the network. This allows another user equipped with a network analyzer on the same network to steal a user's remote account password. For this reason, it is strongly recommended that users of these utilities choose different passwords for their Windows NT workgroup, workstation, or domain from the passwords used on systems they are connecting to that are not Microsoft systems. All passwords used by Windows networking services are encrypted.

To get help on TCP/IP utilities

- At the command prompt, type the command name with -?. For example, type **nbtstat** -? to get help on this command.

  Or

1. In the Program Manager Main group, double-click the Windows NT Help icon.
2. In the Windows NT Help window, click the Command Reference Help button.
3. In the Commands window, click a command name.

   Or

   Choose the Search button in the Command Reference window, and then type a command name in the box or select a command name from the list.

Note

Switches used in the syntax for TCP/IP commands are case-sensitive. For example, for **nbtstat**, the switch **-R** has a different effect from the **-r** switch.

arp

This diagnostic command displays and modifies the IP-to-Ethernet or Token Ring physical address translation tables used by the Address Resolution Protocol (ARP).

Syntax

arp -a [inet_addr] [-N [if_addr]]**arp** -**d** inet_addr [if_addr]**arp** -**s** inet_addr ether_addr [if_addr]

Parameters

-a

Displays current ARP entries by querying TCP/IP. If *inet_addr* is specified, only the IP and physical addresses for the specified computer are displayed

-d

Deletes the entry specified by *inet_addr*.

-s

Adds an entry in the ARP cache to associate the IP address *inet_addr* with the physical address *ether_addr*. The physical address is given as 6 hexadecimal bytes separated by hyphens. The IP address is specified using dotted decimal notation. The entry is permanent, that is, it will not be automatically removed from the cache after the timeout expires.

-N [*if_addr*]

Displays the ARP entries for the network interface specified by *if_addr*.

ether_addr

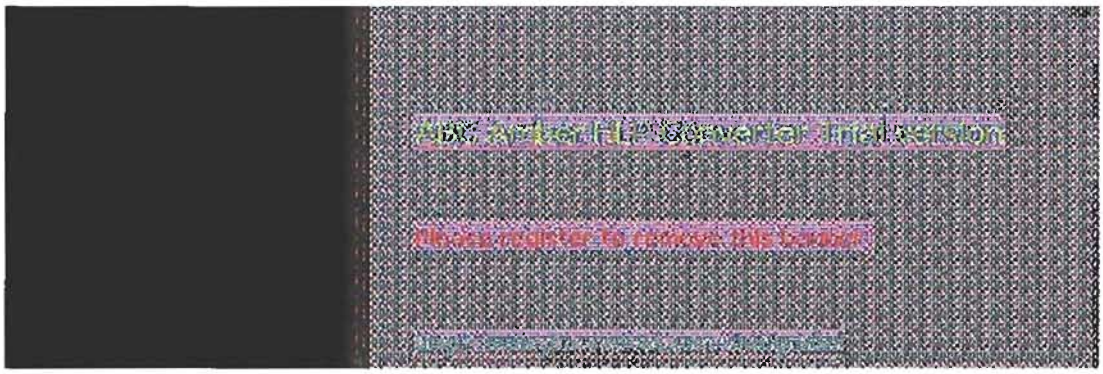
Specifies a physical address.

if_addr

Specifies, if present, the IP address of the interface whose address translation table should be modified. If not present, the first applicable interface will be used.

inet_addr

Specifies an IP address in dotted decimal notation.



finger

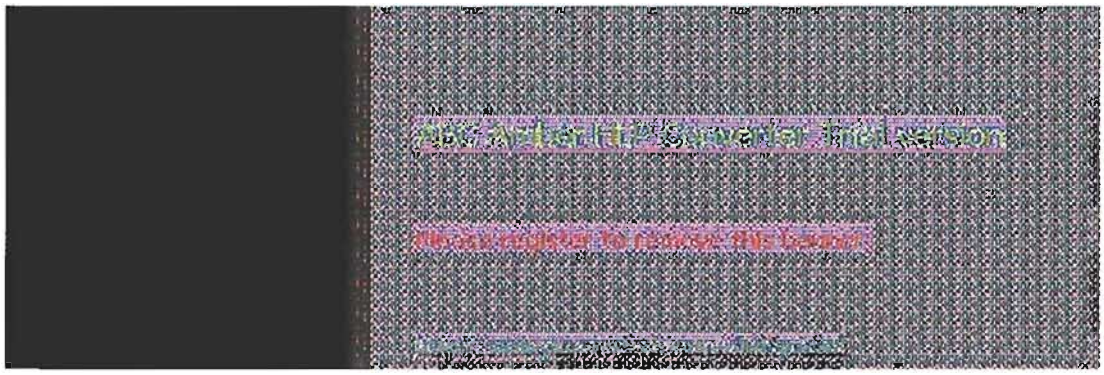
This connectivity command displays information about a user on a specified system running the Finger service. Output varies based on the remote system.

Syntax
finger [-l] [*user*]@*host* [...]

Parameters
-l
Displays information in long list format; not supported on all remote systems.

user
Specifies the user you want information about. Omit the *user* parameter to display information about all users on the specified host.

@*host*
Specifies the host name or the IP address of the remote system whose users you want information about.



ftp

This connectivity command transfers files to and from a computer running an FTP service. **Ftp** can be used interactively or by processing ASCII text files.

Syntax

ftp [-v] [-n] [-i] [-d] [-g] [*host*] [-s: *filename*]

Parameters

-v
Suppresses display of remote server responses.

-n
Suppresses autologon upon initial connection.

-i
Turns off interactive prompting during multiple file transfers.

-d
Enables debugging, displaying all **ftp** commands passed between the client and server.

-g
Disables filename globbing, which permits the use of wildcard characters in local file and path names. (See the **glob** command in the online Command Reference.)

host
Specifies the host name or IP address of the remote host to connect to.

-s: *filename*
Specifies a text file containing **ftp** commands; the commands will automatically run after **ftp** starts. Use this switch instead of redirection (>).

The following table shows the **ftp** commands available when the FTP service is installed on a Windows NT computer. For details about syntax for individual **ftp** commands, choose the **ftp commands** topic in the Commands list in Command Reference.

FTP Commands in Windows NT

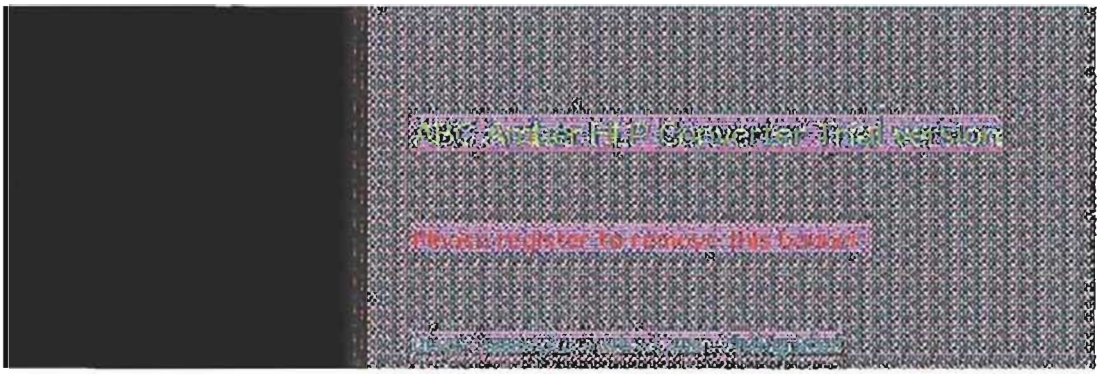
Command	Purpose
!	Runs the specified command on the local computer.
?	Displays descriptions for **ftp** commands. ? is identical to **help**.
append	Appends a local file to a file on the remote computer using the current file type setting.
ascii	Sets the file transfer type to ASCII, which is the default.
bell	Toggles a bell to ring after each file transfer command is completed. By default, the bell is off.
binary	Sets the file transfer type to binary.
bye	Ends the FTP session with the remote computer and exits **ftp**.
cd	Changes the working directory on the remote computer.
close	Ends the FTP session with the remote server and returns to the command interpreter.
debug	Toggles debugging. When debugging is on, each command sent to the remote computer is printed, preceded by the string --->. By default, debugging is off.
delete	Deletes files on remote computers.
dir	Displays a list of a remote directory's files and subdirectories.
disconnect	Disconnects from the remote computer, retaining the **ftp** prompt.

get	Copies a remote file to the local computer using the current file transfer type.
glob	Toggles filename globbing. Globbing permits use of wildcard characters in local file or path names. By default, globbing is on.
hash	Toggles hash-sign (#) printing for each data block transferred. The size of a data block is 2048 bytes. By default, hash-sign printing is off.
help	Displays descriptions for **ftp** commands.
lcd	Changes the working directory on the local computer. By default, the current directory on the local computer is used.
literal	Sends arguments, verbatim, to the remote FTP server. A single FTP reply code is expected in return.
ls	Displays an abbreviated list of a remote directory's files and subdirectories.
mdelete	Deletes files on remote computers.
mdir	Displays a list of a remote directory's files and subdirectories. **Mdir** allows you to specify multiple files.
mget	Copies remote files to the local computer using the current file transfer type.
mkdir	Creates a remote directory.
mls	Displays an abbreviated list of a remote directory's files and subdirectories.
mput	Copies local files to the remote computer using the current file transfer type.
open	Connects to the specified FTP server.
prompt	Toggles prompting. **Ftp** prompts during multiple file transfers to allow you to selectively retrieve or store files; **mget** and **mput** transfer all files if prompting is turned off. By default, prompting is on.
put	Copies a local file to the remote computer using the current file transfer type.
pwd	Displays the current directory on the remote computer.
quit	Ends the FTP session with the remote computer and exits **ftp**.
quote	Sends arguments, verbatim, to the remote FTP server. A single FTP reply code is expected in return. **Quote** is identical to **literal**.
recv	Copies a remote file to the local computer using the current file transfer type. **Recv** is identical to **get**.
remotehelp	Displays help for remote commands.
rename	Renames remote files.
rmdir	Deletes a remote directory.
send	Copies a local file to the remote computer using the current file transfer type. **Send** is identical to **put**.
status	Displays the current status of FTP connections and toggles.
trace	Toggles packet tracing; **trace** displays the route of each packet when running an **ftp** command.
type	Sets or displays the file transfer type.
user	Specifies a user to the remote computer.
verbose	Toggles verbose mode. If on, all **ftp** responses are displayed; when a file transfer completes, statistics regarding the efficiency of the transfer are also displayed. By default, verbose is on.

hostname

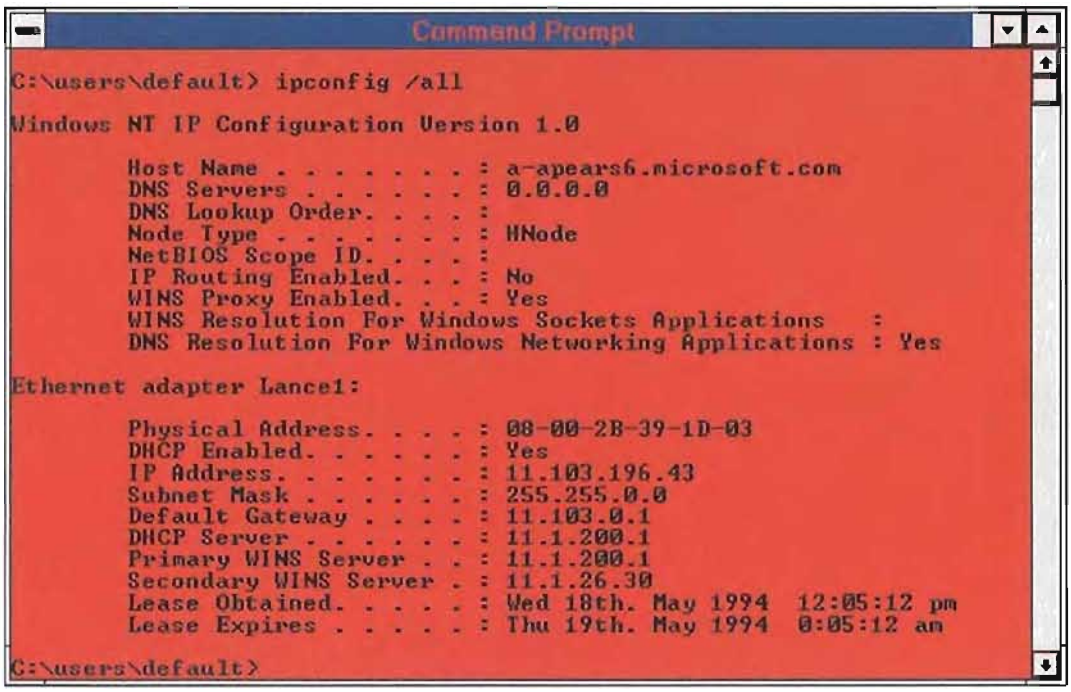
This diagnostic command prints the name of the current host.

Syntax
hostname



ipconfig

This diagnostic command displays all current TCP/IP network configuration values. This command is of particular use on systems running DHCP, allowing users to determine which TCP/IP configuration values have been configured by DHCP. With no parameters, **ipconfig** displays all of the current TCP/IP configuration values, including IP address, subnet mask, and WINS and DNS configuration.



Syntax

ipconfig [/all | /renew [*adapter*] | /release [*adapter*]]

Parameters

all

Produces a full display. Without this switch, **ipconfig** displays only the IP address, subnet mask, and default gateway values for each network card.

renew [*adapter*]

Renews DHCP configuration parameters. This option is available only on systems running the DHCP Client service. To specify an adapter name, type the adapter name that appears when you use **ipconfig** without parameters. For example, in the illustration above, the adapter name is Lance1.

release [*adapter*]

Releases the current DHCP configuration. This option disables TCP/IP on the local system and is available only on DHCP clients. To specify an adapter name, type the adapter name that appears when you use **ipconfig** without parameters.

lpq

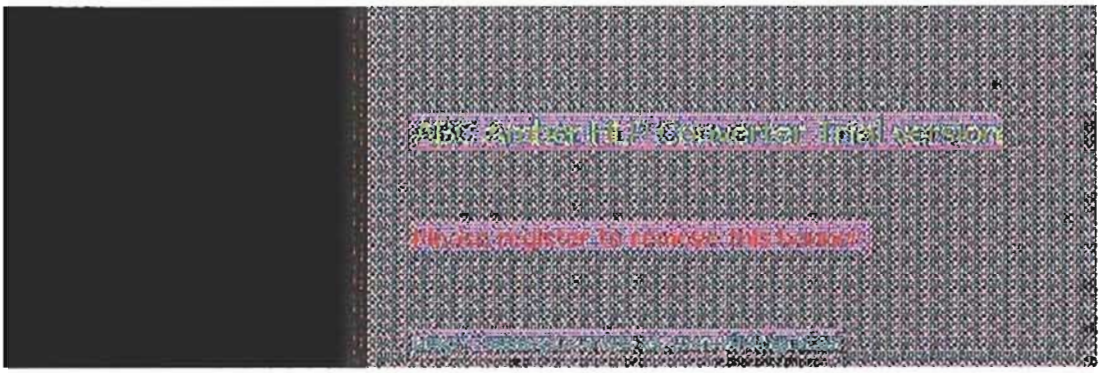
This diagnostic utility is used to obtain status of a print queue on a host running the LPD server.

Syntax
lpq -S *Server* **-P** *Printer* **[-l]**

Parameters
-S *Server*
Specifies the name of the host that has the printer attached to it.

-P *Printer*
Specifies the name of the printer for the desired queue.

-l
Specifies that a detailed status should be given.



lpr

This connectivity utility is used to print a file to a host running an LPD server.

Syntax
lpr -**S***Server* -**P***Printer* [-**C***Class*] [-**J***Jobname*] *filename*

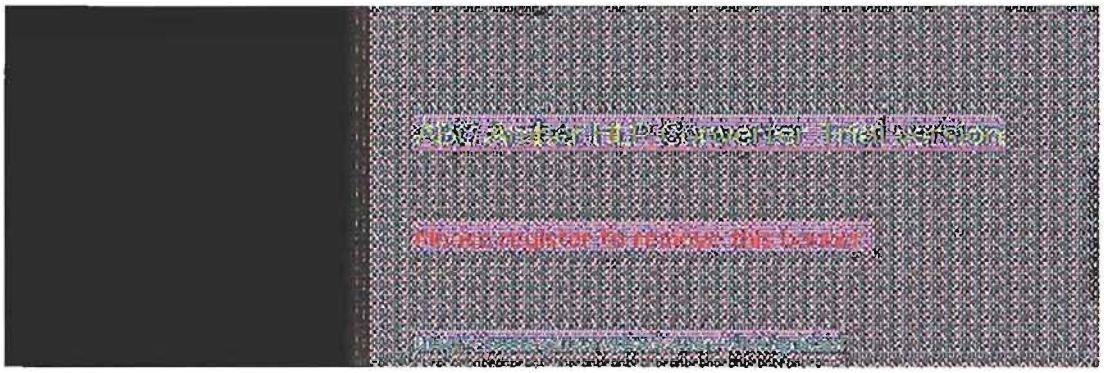
Parameters
-**S***Server*
Specifies the name of the host that has the printer attached to it.

-**P***Printer*
Specifies the name of the printer for the desired queue.

-**C***Class*
Specifies the content of the banner page for the class.

-**J***Jobname*
Specifies the name of this job.

filename
The name of the file to be printed.



nbtstat

This diagnostic command displays protocol statistics and current TCP/IP connections using NetBIOS over TCP/IP.

Syntax
nbtstat [-c] [-n] [-R] [-r] [-S] [-s] [*interval*]

Parameters

-c
Lists the contents of the NetBIOS name cache, giving the IP address of each name.

-n
Lists local NetBIOS names.

-R
Reloads the LMHOSTS file after purging all names from the NetBIOS name cache.

-r
Lists name resolution statistics for Windows networking. On a Windows NT computer configured to use WINS, this option returns the number of names resolved and registered via broadcast or via WINS.

-S
Displays both workstation and server sessions, listing the remote hosts by IP address only.

-s
Displays both workstation and server sessions. It attempts to convert the remote host IP address to a name using the HOSTS file.

interval
Redisplays selected statistics, pausing *interval* seconds between each display. Press Ctrl+C to stop redisplaying statistics. If this parameter is omitted, **nbtstat** prints the current configuration information once.

Notes
The column headings generated by the **nbtstat** utility have the following meanings.

In
Number of bytes received.

Out
Number of bytes sent.

In/Out
Whether the connection is from the computer (outbound) or from another system to the local computer (inbound).

Life
The remaining time that a name table cache entry will live before it is purged.

Local Name
The local NetBIOS name associated with the connection.

Remote Host
The name or IP address associated with the remote host.

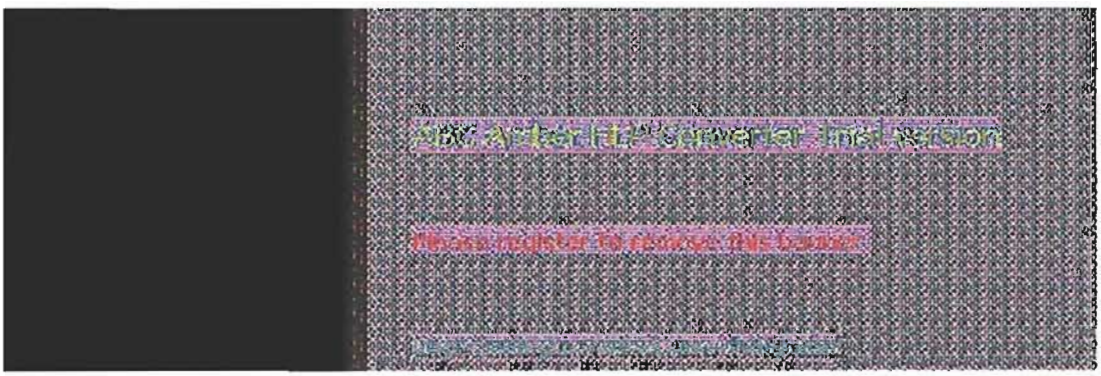
Type
This refers to the type of name. A name can either be a unique name or a group name.

<03>
Each NetBIOS name is 16 characters long. The last byte often has special significance, because the same name can be present several times on a computer. This notation is simply the last byte converted to hexadecimal. For example, <20> is a space in ASCII.

State

The state of NetBIOS connections. The possible states are shown in the following list:

State	Meaning
Connected	The session has been established
Associated	A connection endpoint has been created and associated with an IP address
Listening	This endpoint is available for an inbound connection
Idle	This endpoint has been opened but cannot receive connections
Connecting	The session is in the connecting phase where the name-to-IP address mapping of the destination is being resolved
Accepting	An inbound session is currently being accepted and will be connected shortly
Reconnecting	A session is trying to reconnect if it failed to connect on the first attempt
Outbound	A session is in the connecting phase where the TCP connection is currently being created
Inbound	An inbound session is in the connecting phase
Disconnecting	A session is in the process of disconnecting
Disconnected	The local computer has issued a disconnect, and it is waiting for confirmation from the remote system



netstat

This diagnostic command displays protocol statistics and current TCP/IP network connections.

Syntax
netstat [-a] [-e][n][s] [-p *protocol*] [-r] [*interval*]

Parameters

-a
Displays all connections and listening ports; server connections are usually not shown.

-e
Displays Ethernet statistics. This may be combined with the **-s** option.

-n
Displays addresses and port numbers in numerical form (rather than attempting name lookups).

-p *protocol*
Shows connections for the protocol specified by *protocol*; *protocol* can be **tcp** or **udp**. If used with the **-s** option to display per-protocol statistics, *protocol* can be **tcp**, **udp**, or **ip**.

-r
Displays the contents of the routing table.

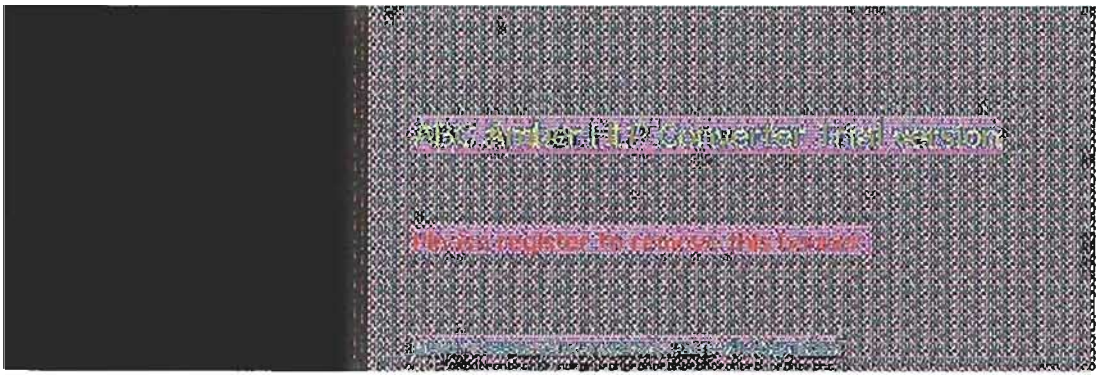
-s
Displays per-protocol statistics. By default, statistics are shown for TCP, UDP and IP; the **-p** option may be used to specify a subset of the default.

interval
Redisplays selected statistics, pausing *interval* seconds between each display. Press Ctrl+C to stop redisplaying statistics. If this parameter is omitted, **netstat** prints the current configuration information once.

Notes
The **netstat** utility provides statistics on the following network components.

Statistic	Purpose
Foreign Address	The IP address and port number of the remote computer to which the socket is connected. The name corresponding to the IP address is shown instead of the number if the HOSTS file contains an entry for the IP address. In cases where the port is not yet established, the port number is shown as an asterisk (*).
Local Address	The IP address of the local computer, as well as the port number the connection is using. The name corresponding to the IP address is shown instead of the number if the HOSTS file contains an entry for the IP address. In cases where the port is not yet established, the port number is shown as an asterisk (*).
Proto	The name of the protocol used by the connection.
(state)	Indicates the state of TCP connections only. The possible states are:

CLOSED	FIN_WAIT_1	SYN_RECEIVED
CLOSE_WAIT	FIN_WAIT_2	SYN_SEND
ESTABLISHED	LISTEN	TIMED_WAIT
LAST_ACK		



ping

This diagnostic command verifies connections to one or more remote hosts

Syntax

ping [-t] [-a] [-n *count*] [-l *length*] [-f] [-i *ttl*] [-v *tos*] [-r *count*] [-s *count*] [[-j *host-list*] | [-k *host-list*]] [-w *timeout*] *destination-list*

Parameters

-t
Pings the specified host until interrupted.

-a
Resolve addresses to hostnames.

-n *count*
Sends the number of ECHO packets specified by *count*. The default is 4.

-l *length*
Sends ECHO packets containing the amount of data specified by *length*. The default is 64 bytes; the maximum is 8192.

-f
Sends a Do Not Fragment flag in the packet. The packet will not be fragmented by gateways on the route.

-i *ttl*
Sets the Time To Live field to the value specified by *ttl*.

-v *tos*
Sets the Type Of Service field to the value specified by *tos*.

-r *count*
Records the route of the outgoing packet and the returning packet in the Record Route field. A minimum of 1 to a maximum of 18 hosts must be specified by *count*.

-s *count*
Specifies the timestamp for the number of hops specified by *count*.

-j *host-list*
Routes packets via the list of hosts specified by *host-list*. Consecutive hosts may be separated by intermediate gateways (loose source routed). The maximum number allowed by IP is 9.

-k *host-list*
Routes packets via the list of hosts specified by *host-list*. Consecutive hosts may not be separated by intermediate gateways (strict source routed). The maximum number allowed by IP is 9.

-w *timeout*
Specifies a timeout interval in milliseconds.

destination-list
Specifies the remote hosts to ping.

Note

The **ping** command verifies connections to remote host or hosts by sending ICMP echo packets to the host and listening for echo reply packets. **Ping** waits for up to 1 second for each packet sent and prints the number of packets transmitted and received. Each received packet is validated against the transmitted message. By default, four echo packets containing 64 bytes of data (a periodic uppercase sequence of alphabetic characters) are transmitted.

You can use the **ping** utility to test both the host name and the IP address of the host. If the IP address is verified but the host name is not, you may have a name resolution problem. In this case, be sure that the host name you are querying is in either the local HOSTS file or in the DNS

database.

The following shows sample output for **ping**:

C:\>ping ds.internic.net

Pinging ds.internic.net [192.20.239.132] with 32 bytes of data:

Reply from 192.20.239.132: bytes=32 time=101ms TTL=243
Reply from 192.20.239.132: bytes=32 time=100ms TTL=243
Reply from 192.20.239.132: bytes=32 time=120ms TTL=243
Reply from 192.20.239.132: bytes=32 time=120ms TTL=243

rcp

This connectivity command copies files between a Window NT computer and a system running **rshd**, the remote shell server. The **rcp** command can also be used for third-party transfer to copy files between two computers running **rshd** when the command is issued from a Windows NT computer. The **rshd** server is available on UNIX computers, but not on Windows NT, so the Windows NT computer can only participate as the system from which the commands are issued.

Syntax

rcp [-a | -b] [-h] [-r] *source1 source2 ... sourceN destination*

Parameters

-a

Specifies ASCII transfer mode. This mode converts the carriage return/linefeed characters to carriage returns on outgoing files, and linefeed characters to carriage return/linefeeds for incoming files. This is the default transfer mode.

-b

Specifies binary image transfer mode. No carriage return/linefeed conversion is performed.

-h

Transfers source files marked with the hidden attribute on the Windows NT computer. Without this option, specifying a hidden file on the **rcp** command line has the same effect as if the file did not exist.

-r

Recursively copies the contents of all subdirectories of the source to the destination. Both the *source* and *destination* must be directories.

source and *destination*

Must be of the form [*host*[.*user*]:]*filename*. If the [*host*[.*user*]:] portion is omitted, the host is assumed to be the local computer. If the *user* portion is omitted, the currently logged on Windows NT username is used. If a fully qualified host name is used, which contains the period (.) separators, then the [.*user*] must be included. Otherwise, the last part of the hostname will be interpreted as the username. If multiple source files are specified, the *destination* must be a directory.

If the filename does not begin with a forward slash (/) for UNIX or a backward slash (\) for Windows NT systems, it is assumed to be relative to the current working directory. On Windows NT, this is the directory from which the command is issued. On the remote system, it is the logon directory for the remote user. A period (.) means the current directory. Use the escape characters (\ , ", or ') in remote paths to use wildcard characters on the remote host.

Notes

Remote Privileges

The **rcp** command does not prompt for passwords; the current or specified user name must exist on the remote host and allow remote command execution via **rcp**.

The .rhosts file specifies which remote system or users can assess a local account using **rsh** or **rcp**. This file (or a HOSTS equivalent) is required on the remote system for access to a remote system using these commands. **Rsh** and **rcp** both transmit the local username to the remote system. The remote system uses this name plus the IP address (usually resolved to a host name) or the requesting system to determine whether access is granted. There is no provision for specifying a password to access an account using these commands.

If the user is logged on to a Windows NT Server domain, the domain controller must be available to resolve the currently logged on name, because the logged on name is not cached on the local computer. Because the username is required as part of the **rsh** protocol, the command will fail if the username cannot be obtained.

The .rhosts File

The .rhosts file is a text file where each line is an entry. An entry consists of the local host name, the local user name, and any comments about the entry. Each entry is separated by a tab or space, and comments begin with a hash mark (#), for example:

```
computer5    marie      #This computer is in room 31A
```

The .rhosts file must be in the user's home directory on the remote computer. For more information about a remote computer's specific implementation of the .rhosts file, see the remote system's documentation.

Additionally, have your host name added to the remote system's /ETC/HOSTS file. This will allow the remote system to authenticate remote requests for your computer using the Microsoft TCP/IP utilities.

Specifying Hosts

Use the *host.user* variables to use a user name other than the current user name. If *host.user* is specified with *source*, the .rhosts file on the remote host must contain an entry for *user*. For example,

```
rcp rhino.johnb:file1  buffalo.admin:file2
```

The .rhosts file on BUFFALO should have an entry for Johnb on RHINO.

If a host name is supplied as a full domain name containing dots, a user name must be appended to the host name, as previously described. This prevents the last element of the domain name from being interpreted as a user name. For example,

```
rcp domain-name1.user:johnm  domain-name2.user:billr
```

Remote Processing

Remote processing is performed by a command run from the user's logon shell on most UNIX systems. The user's .profile or .cshrc is executed before parsing filenames, and exported shell variables may be used (using the escape character or quotation marks) in remote filenames.

Copying Files

If you attempt to copy a number of files to a file rather than a directory, only the last file is copied. Also, the **rcp** command cannot copy a file onto itself.

Examples

These examples show syntax for some common uses of **rcp**.

To copy a local file to the logon directory of a remote computer:

```
rcp filename remotecomputer:
```

To copy a local file to an existing directory and a new filename on a remote computer:

```
rcp filename remotecomputer:/directory/newfilename
```

To copy multiple local files to a subdirectory of a remote logon directory:

```
rcp file1 file2 file3 remotecomputer::subdirectory/filesdirectory
```

To copy from a remote source to the current directory of the local computer:

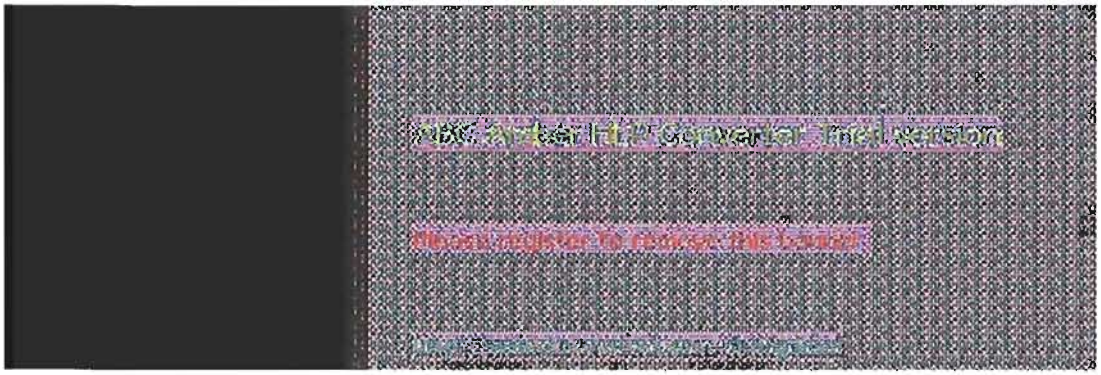
```
rcp remotecomputer:filename .
```

To copy from multiple files from multiple remote sources to a remote destination with different usernames:

```
rcp remote1.user1:file1 remote2.user2:file2 remotedest.destuser:directory
```

To copy from a remote system using an IP address to a local computer (where the username is mandatory because a period is used in the remote system name):

```
rcp 11.101.12.1.user:filename filename
```



rexec

This connectivity command runs commands on remote hosts running the **rexecd** service. **Rexec** authenticates the user name on the remote host by using a password, before executing the specified command.

Syntax
rexec *host* [-l *username*] [-**n**] *command*

Parameters
host
Specifies the remote host on which to run *command*.

-l *username*
Specifies the user name on the remote host.

-n
Redirects the input of **rexec** to NUL.

command
Specifies the command to run.

Notes
Rexec prompts the user for a password and authenticates the password on the remote host. If the authentication succeeds, the command is executed.

Rexec copies standard input to the remote command, standard output to its standard output, and standard error to its standard error. Interrupt, quit, and terminate signals are propagated to the remote command. **Rexec** normally terminates when the remote command does.

Use quotation marks around redirection symbols to redirect onto the remote host. If quotation marks are not used, redirection occurs on the local computer. For example, the following command appends the remote file *remotefile* to the local file *localfile*:

```
rexec otherhost cat remotefile >> localfile
```

The following command appends the remote file *remotefile* to the remote file *otherremotefile*:

```
rexec otherhost cat remotefile ">>" otherremotefile
```

Using Interactive Commands

You cannot run most interactive commands. For example, **vi** or **emacs** cannot be run using **rexec** . Use **telnet** to run interactive commands.

route

This diagnostic command manipulates network routing tables.

Syntax
route [**-f**] [*command* [*destination*] [**MASK** *netmask*] [*gateway*]]

Parameters
-f
Clears the routing tables of all gateway entries. If this parameter is used in conjunction with one of the commands, the tables are cleared prior to running the command.

command
Specifies one of four commands.

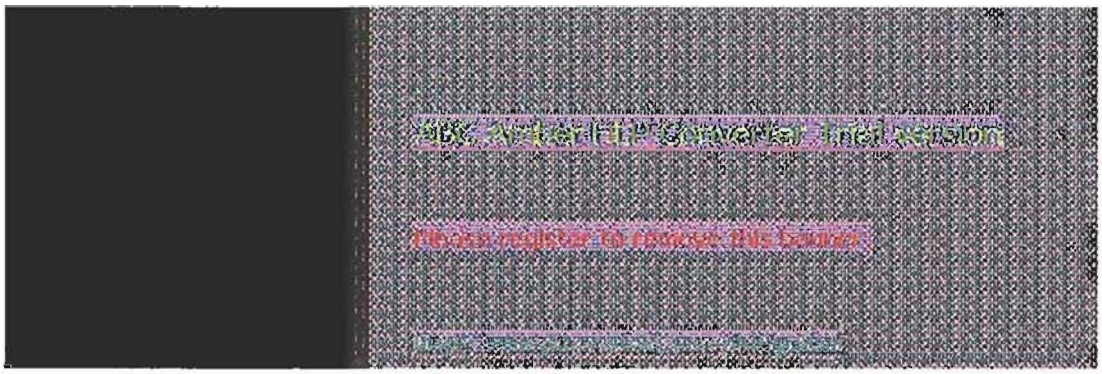
Command	Purpose
print	Prints a route
add	Adds a route
delete	Deletes a route
change	Modifies an existing route

destination
Specifies the host to send *command*.

MASK
Specifies, if present, that the next parameter be interpreted as the *netmask* parameter.

netmask
Specifies, if present, the subnet mask value to be associated with this route entry. If not present, this parameter defaults to 255.255.255.255.

gateway
Specifies the gateway.



rsh

This connectivity command runs commands on remote hosts running the RSH service. For information about the .r .sts file, see the Rcp command.

Syntax

rsh *host* [-l *username*] [-n] *command*

Parameters

host

Specifies the remote host on which to run *command*.

-l *username*

Specifies the user name to use on the remote host. If omitted, the logged on user name is used.

-n

Redirects the input of **rsh** to NUL.

command

Specifies the command to run.

Notes

Rsh copies standard input to the remote *command*, standard output of the remote *command* to its standard output, and the standard error of the remote *command* to its standard error. **Rsh** normally terminates when the remote command does.

Using Redirection Symbols

Use quotation marks around redirection symbols to redirect onto the remote host. If quotation marks are not used, redirection occurs on the local computer. For example, the following command appends the remote file *remotefile* to the local file *localfile*:

```
rsh otherhost cat remotefile >> localfile
```

The following command appends the remote file *remotefile* to the remote file *otherremotefile*:

```
rsh otherhost cat remotefile ">>" otherremotefile
```

Using Rsh on a Windows NT Server Domain

If the user is logged on to a Windows NT Server domain, the domain controller must be available to resolve the currently logged on name, because the logged on name is not cached on the local computer. Because the *username* is required as part of the **rsh** protocol, the command will fail if the *username* cannot be obtained.

telnet

This connectivity command starts terminal emulation with a remote system running a Telnet service. Telnet provides DEC™ VT 100, DEC VT 52, or TTY emulation, using connection-based services of TCP.

To provide terminal emulation from a Windows NT computer, the foreign host must be configured with the TCP/IP program, the Telnet server program or daemon, and a user account for the Windows NT computer.

Note
Microsoft does not provide the Telnet server daemon (**telnetd**).

Syntax
telnet [*host* [*port*]]

Parameters
host
Specifies the host name or IP address of the remote system you want to connect to, providing compatibility with applications such as Gopher and Mosaic.

port
Specifies the remote port you want to connect to, providing compatibility with applications such as Gopher and Mosaic. The default value is specified by the **telnet** entry in the SERVICES file. If no entry exists in the SERVICES file, the default connection port value is decimal 23.

Notes
The Telnet application is found in the Accessories program group after you install the TCP/IP connectivity utilities. Telnet is a Windows Sockets-based application that simplifies TCP/IP terminal emulation with Windows NT.

To use Telnet

1. Double-click the Telnet icon in the Accessories program group.

   Or

   At the command prompt, type **telnet** and press ENTER.

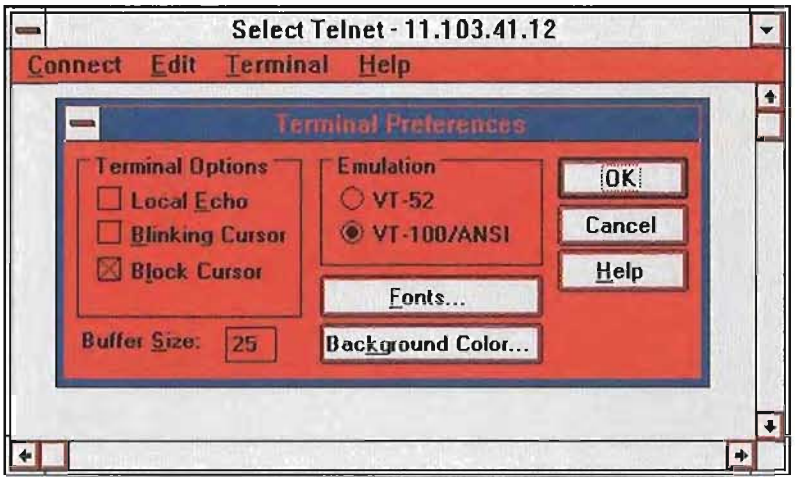
2. From the Connect menu in the Telnet window, choose Remote System.

3. In the Connect dialog box, type the host name you want to connect to, and then choose the Connect button.

   A connection is made, and you can begin a work session.

4. To end a session, choose the Disconnect command from the Connect menu.

You can specify your preferences for items such as emulation options, the screen font, and color by choosing Preferences from the Terminal menu. You can also use commands from the Edit menu to select, copy, and paste text from the Clipboard. For information about Telnet options, see the online Help.


Select Telnet - 11.103.41.12
Connect Edit Terminal Help
Terminal Preferences
Terminal Options
Local Echo
Blinking Cursor
Block Cursor
Emulation
VT-52
VT-100/ANSI
OK
Cancel
Help
Fonts...
Buffer Size: 25
Background Color...

tftp

This connectivity command transfers files to and from a remote computer running the Trivial File Transfer Protocol (TFTP) service. This utility is similar to **ftp**, but it does not provide user authentication, although the files require read and write UNIX permissions.

Syntax

tftp [**-i**] *host* [**get** | **put**] *source* [*destination*]

Parameters

-i

Specifies binary image transfer mode (also called octet). In binary image mode, the file is moved literally byte by byte. Use this mode when transferring binary files.

If -i is omitted, the file is transferred in ASCII mode. This is the default transfer mode. This mode converts the end-of-line (EOL) characters to a carriage return for UNIX and a carriage return/linefeed for personal computers. This mode should be used when transferring text files. If a file transfer is successful, the data transfer rate is displayed.

host

Specifies the local or remote host.

get

Transfers *destination* on the remote computer to *source* on the local computer.

Since the TFTP protocol does not support user authentication, the user must be logged on, and the files must be writable on the remote computer.

put

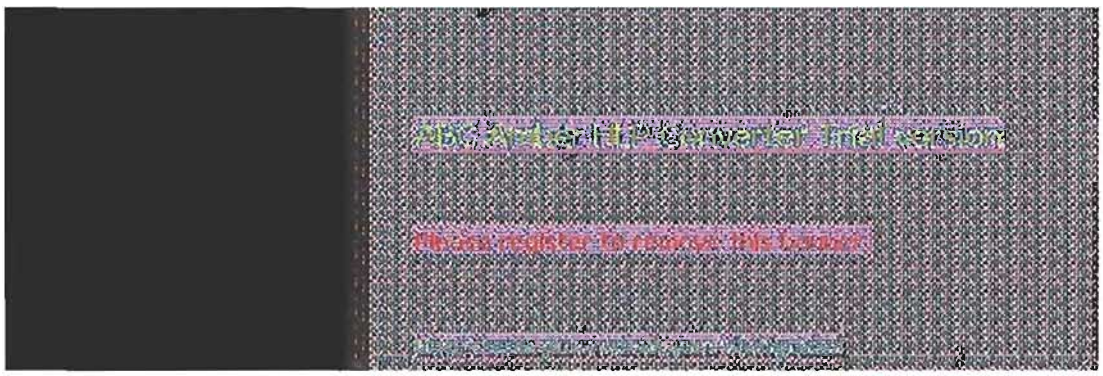
Transfers *source* on the local computer to *destination* on the remote computer.

source

Specifies the file to transfer.

destination

Specifies where to transfer the file.



tracert

This diagnostic utility determines the route taken to a destination by sending Internet Control Message Protocol (ICMP) echo packets with varying Time-To-Live (TTL) values to the destination. Each router along the path is required to decrement the TTL on a packet by at least 1 before forwarding it, so the TTL is effectively a hop count. When the TTL on a packet reaches 0, the router is supposed to send back an ICMP Time Exceeded message to the source system. **Tracert** determines the route by sending the first echo packet with a TTL of 1 and incrementing the TTL by 1 on each subsequent transmission until the target responds or the maximum TTL is reached. The route is determined by examining the ICMP Time Exceeded messages sent back by intermediate routers. Notice that some routers silently drop packets with expired time-to-live (TTLs) and will be invisible to **tracert**.

Syntax
tracert [-d] [-h *maximum_hops*] [-j *host-list*] [-w *timeout*] *target_name*

Parameters
-d
Specifies not to resolve addresses to hostnames.

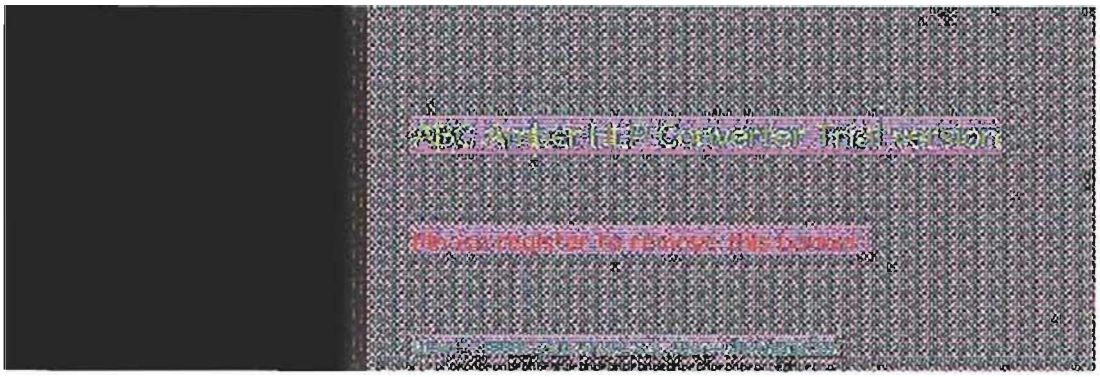
-h *maximum_hops*
Specifies maximum number of hops to search for target.

-j *host-list*
Specifies loose source route along *host-list*.

-w *timeout*
Waits the number of milliseconds specified by *timeout* for each reply.

Notes
The following shows sample output for **tracert**. The first column is the hop number, which is the Time To Live (TTL) value set in the packet. The next three columns are the round-trip times in milliseconds for three attempts to reach the destination with that TTL value. An asterisk (*) means that the attempt timed out. The fourth column is the hostname (if it was resolved) and IP address of the responding system.

```
C:\>tracert ds.internic.net

Tracing route to ds.internic.net [198.49.45.10]
over a maximum of 30 hops:

1  <10 ms <10 ms  *   [131.107.1.100]
2  10 ms <10 ms  10 ms seattle1-gw.nwnet.net [192.80.12.82]
3   *    10 ms  10 ms enss143-cnet.nwnet.net [192.35.180.2]
4  20 ms  *    10 ms t3-3.seattle-cnss8.t3.ans.net [140.222.88.4]
5  30 ms  30 ms  20 ms t3-0.los-angeles-cnss8.t3.ans.net [140.222.8.1
6  70 ms  70 ms  80 ms t3-0.new-york-cnss24.t3.ans.net [140.222.24.1]
7  80 ms  81 ms  80 ms t3-0.denver-cnss40.t3.ans.net [140.222.40.1]
8  100 ms  91 ms  90 ms t3-1.new-york-cnss32.t3.ans.net [140.222.32.2]
9  90 ms  90 ms  91 ms mf-0.new-york-cnss36.t3.ans.net [140.222.32.196]
10 100 ms  90 ms  91 ms t1-0.enss222.t3.ans.net [140.222.222.1]
11 140 ms  191 ms  100 ms ds.internic.net [198.49.45.10]

Trace complete.
```



MIB Object Types for Windows NT

This appendix lists the objects in the LAN Manager MIB II, DHCP MIB, and WINS MIB, and provides a brief description of each.

The following MIB objects are listed in this appendix:

- LAN Manager MIB II for Windows NT objects, including Common group, Server group, Workstation group, and Domain group
- Microsoft DHCP objects
- Microsoft WINS objects

This appendix assumes that you are familiar with network management, TCP/IP, and SNMP. It also assumes that you are familiar with the concept of a *management information base* (MIB). If you are not familiar with TCP/IP or the Internet MIB 2, see *Internetworking with TCP/IP* by Douglas E. Comer (Prentice Hall, 1991) and *The Simple Book* by Marshall T. Rose (Prentice Hall, 1991).

LAN Manager MIB II for Windows NT Objects

The LAN Manager MIB II for Windows NT contains a set of objects specifically designed to support computers running Windows NT Notice that there are fewer objects in the LAN Manager MIB II for Windows NT than the LAN Manager MIB II for OS/2 because of differences in the operating system.

All LAN Manager MIB II objects apply to computers running Windows NT Workstation and Windows NT Server

LAN Manager MIB II for Windows NT Objects

Common Gr~up

comVersionMaj {common 1}
The major release version number of the Windows NT software.

comVersionMin {common 2}
The minor release version number of the Windows NT software.

comType {common 3}
The type of Windows NT software this system is running.

comStatStart {common 4}
The time, in seconds, since January 1, 1970, at which time the Windows NT statistics on this node were last cleared. The **comStatStart** object applies to the following statistical objects:

comStatNumNetIOs	svStatErrorOuts	wkstaStatSessStarts
comStatFiNetIOs	svStatPwErrors	wkstaStatSessFails
comStatFcNetIOs	svStatPermErrors	wkstaStatUses
svStatOpens	svStatSysErrors	wkstaStatUseFails
svStatDevOpens	svStatSentBytes	wkstaStatAutoRecs
svStatJobsQueued	svStatRcvdBytes	
svStatSOpens	svStatAvResponse	

comStatNumNetIOs {common 5}
The number of network I/O operations submitted on this node.

comStatFiNetIOs {common 6}
The number of network I/O operations on this node that failed issue.

comStatFcNetIOs {common 7}
The number of network I/O operations on this node that failed completion.

LAN Manager MIB II for Windows NT Objects

Server Group

svDescription {server 1}
A comment describing the server.

svSvcNumber {server 2}
The number of network services installed on the server.

svSvcTable {server 3}
A list of service entries describing the network service installed on the server.

svSvcEntry {svSvcTable 1}
The names of the network services installed on the server.

svSvcName {svSvcEntry 1}
The name of a Windows NT network service.

svSvcInstalledState {svSvcEntry 2}
The installation status of a network.

svSvcOperatingState {svSvcEntry 3}
The operating status of a network service.

svSvcCanBeUninstalled {svSvcEntry 4}
Indicates whether the network service specified by this entry can be removed.

svSvcCanBePaused {svSvcEntry 5}
Indicates whether the network service specified by this entry can be paused.

svStatsOpen {server 4}
The total number of files that were opened on the server.

svStatDevOpens {server 5}
The total number of communication devices that were opened on the server.

svStatQueuedJobs {server 6}
The total number of print jobs that were spooled on the server.

svStatSOpens {server 7}
The number of sessions that were started on the server.

svStatErrorOuts {server 8]
The number of sessions disconnected because of an error on the server.

svStatPwErrors {server 9}
The number of password violations encountered on the server.

svStatPermErrors {server 10}
The number of access-permission violations encountered on the server.

svStatSysErrors {server 11}
The number of system errors encountered on the server.

svStatSentBytes {server 12}
The number of bytes sent by the server.

svStatRcvdBytes {server 13}
The number of bytes received by the server.

svStatAvResponse {server 14}
The mean number of milliseconds it took the server to process a workstation I/O request (for example, the average time an NCB sat at the server).

svSecurityMode {server 15}
The type of security running on the server.

svUsers {server 16}

The number of concurrent users the server can support.

svStatReqBufsNeeded {server 17}
The number of times the server requested allocation of additional buffers.

svStatBigBufsNeeded {server 18}
The number of times the server needed but could not allocate a big buffer while processing a client request.

svSessionNumber {server 19}
The number of sessions on the server.

svSessionTable {server 20}
A list of session entries corresponding to the current sessions that clients have with the server.

svSessionEntry {svSessionTable 1}
A session that is currently established on the server.

svSesClientName {svSessionEntry 1}
The name of the remote computer that established the session.

svSesUserName {svSessionEntry 2}
The number of connections to server resources that are active in the current session.

svSesNumConns {svSessionEntry 3}
The number of connections to server resources that are active in the current session.

svSesNumOpens {svSessionEntry 4}
The number of files, devices, and pipes that are open in the current session.

svSesTime {svSessionEntry 5}
The length of time, in seconds, since the current session began.

svSesIdleTime {svSessionEntry 6}
The length of time, in seconds, that the session has been idle.

svClientType {svSessionEntry 7}
The type of client that established the session.

svSesState {svSessionEntry 8}
The state of the current session. (Setting the state of an active session to **deleted** with **netSessionDel** deletes the client session. The session state cannot be set to **active**.)

svAutoDisconnects {server 21}
The number of sessions that the server automatically disconnected because of inactivity.

svDisConTime {server 22}
The number of seconds the server waits before disconnecting an idle session.

svAuditLogSize {server 23}
The maximum size, in kilobytes, of the server's audit log.

svUserNumber {server 24}
The number of users who have accounts on the server.

svUserTable {server 25}
A table of active user accounts on the server.

svUserEntry {svUserTable 1}
A user account on the server.

svUserName {svUserEntry 1}
The name of a user account.

svShareNumber {server 26}
The number of shared resources on the server.

svShareTable {server 27}
A table of the shared resources on the server.

svShareEntry {svShareTable 1}
A table corresponding to a single shared resource on the server.

svShareName {svShareEntry 1}
The name of a shared resource.

svSharePath {svShareEntry 2}

The local name of a shared resource.

svShareComment {svShareEntry 3}
A comment associated with a shared resource.

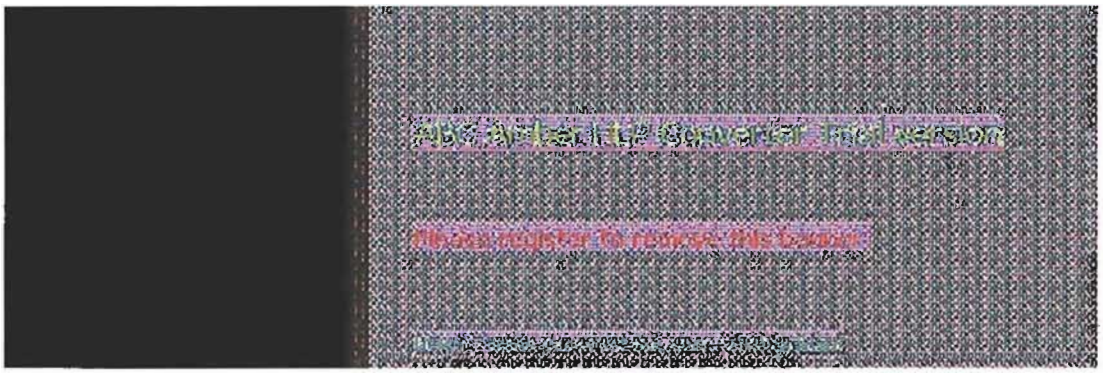
svPrintQNumber {server 28}
The number of printer queues on the server.

svPrintQTable {server 29}
A table of the printer queues on the server.

svPrintQEntry {svPrintQTable 1}
A table entry corresponding to a single printer queue on the server.

svPrintQName {svPrintQEntry 1}
The name of a printer queue.

svPrintQNumJobs {svPrintQEntry 2}
The number of jobs currently in a printer.



LAN Manager MIB II for Windows NT Objects

Workstation Group

wkstaStatSessStarts {workstation 1}
The number of sessions the workstation initiated.

wkstaStatSessFails {workstation 2}
The number of failed sessions the workstation had.

wkstaStatUses {workstation 3}
The number of connections the workstation initiated.

wkstaStatUseFails {workstation 4}
The number of failed connections the workstation had.

wkstaStatAutoRecs {workstation 5}
The number of sessions that were broken and then automatically reestablished.

wkstaErrorLogSize {workstation 6}
The maximum size, in kilobytes, of the workstation error log.

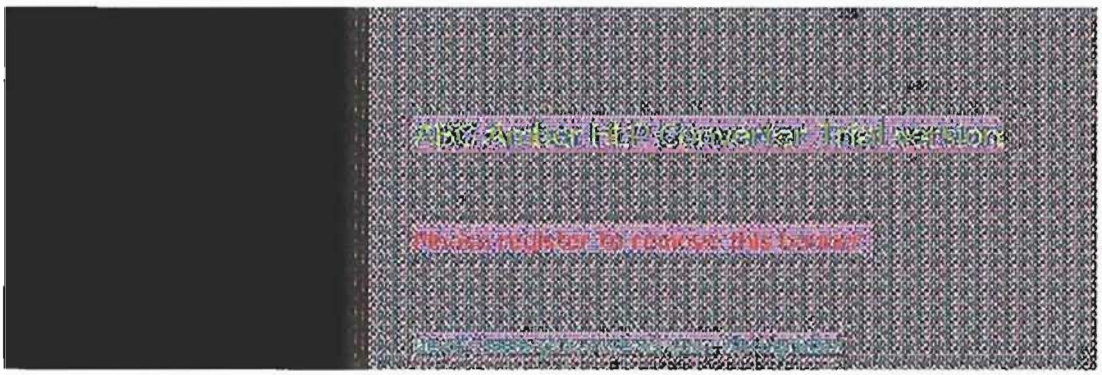
wkstaUseNumber {workstation 7}
This object will always return the value 0.

LAN Manager MIB II for Windows NT Objects

Domain Group

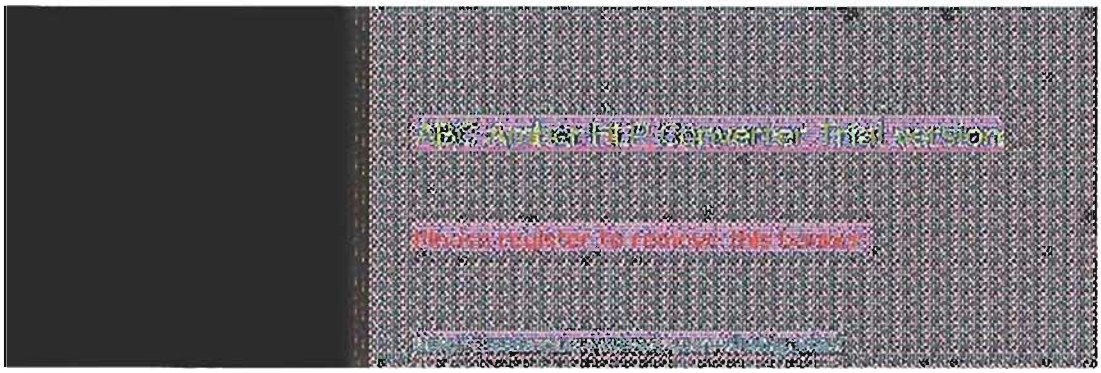
domPrimaryDomain {domain 1}

The name of the primary domain to which the computer belongs.



Microsoft DHCP Objects

Enterprises are defined in RFC 1155-SMI. Object Type is defined in RFC 1212. DisplayString is defined in RFC 1213.



Microsoft DHCP Objects

DHCP MIB Parameters

ParDhcpStartTime {DhcpPar 1}
DHCP Server start time.

ParDhcpTotalNoOfDiscovers {DhcpPar 2}
Indicates the number of discovery messages received.

ParDhcpTotalNoOfRequests {DhcpPar 3}
Indicates the number of requests received.

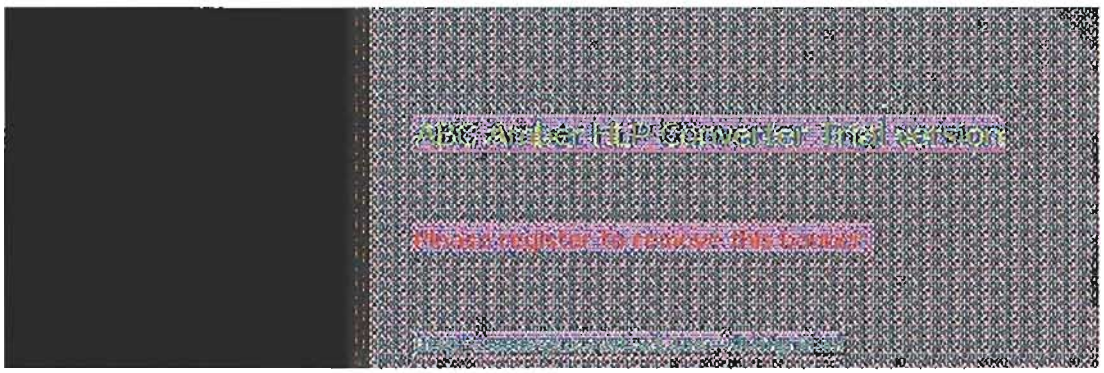
ParDhcpTotalNoOfReleases {DhcpPar 4}
Indicates the number of releases received.

ParDhcpTotalNoOfOffers {DhcpPar 5}
Indicates the number of offers sent.

ParDhcpTotalNoOfAcks {DhcpPar 6}
Indicates the number of acknowledgments sent.

ParDhcpTotalNoOfNacks {DhcpPar 7}
Indicates the number of negative acknowledgments sent.

ParDhcpTotalNoOfDeclines {DhcpPar 8}
Indicates the number of declines received.



Microsoft DHCP Objects

DHCP Scope Group

ScopeTable {DhcpScope 1}
A list of subnets maintained by the server.

sScopeTableEntry {ScopeTable 1}
The row corresponding to a subnet.

SubnetAdd {sScopeTableEntry 1}
The subnet address.

NoAddInUse {sScopeTableEntry 2}
The number of addresses in use.

NoAddFree {sScopeTableEntry 3}
The number of free addresses available.

NoPendingOffers {sScopeTableEntry 4}
The number of addresses currently in the offer state - that is, those that are used temporarily.

Microsoft WINS Objects

Enterprises are defined in RFC 1155-SMI. Object Type is defined in RFC 1212. DisplayString is defined in RFC 1213.

Microsoft WINS Objects

WINS Parameters

ParWinsStartTime {Par 1}
WINS start time.

ParLastPScvTime {Par 2}
Most recent date and time at which planned scavenging took place. Planned scavenging happens at intervals specified in the Registry. Scavenging involves changing owned nonrenewed entries to the released state. Further, released records may be changed to extinct records, extinct records may be deleted, and revalidation of old replicas may take place.

ParLastATScvTime {Par 3}
Most recent date and time at which scavenging took place as a result of administrative action.

ParLastTombScvTime {Par 4}
Most recent date and time at which extinction scavenging took place.

ParLastVerifyScvTime {Par 5}
Most recent date and time at which revalidation of old active replicas took place.

ParLastPRplTime {Par 6}
Most recent date and time at which planned replication took place. Planned replication happens at intervals specified in the Registry.

ParLastATRplTime {Par 7}
Most recent date and time at which administrator-triggered replication took place.

ParLastNTRplTime {Par 8}
Most recent date and time at which network-triggered replication took place. Network-triggered replication happens as a result of an update notification message from a remote WINS.

ParLastACTRplTime {Par 9}
Most recent date and time at which address change-triggered replication took place. Address change-triggered replication happens when the address of an owned name changes because of a new registration.

ParLastInitDbTime {Par 10}
Most recent date and time at which the local database was generated statically from one or more data files.

ParLastCounterResetTime {Par 11}
Most recent date and time at which the local counters were initialized to zero.

ParWinsTotalNoOfReg {Par 12}
Indicates the number of registrations received.

ParWinsTotalNoOfQueries {Par 13}
Indicates the number of queries received.

ParWinsTotalNoOfRel {Par 14}
Indicates the number of releases received.

ParWinsTotalNoOfSuccRel {Par 15}
Indicates the number of releases that succeeded.

ParWinsTotalNoOfFailRel {Par 16}
Indicates the number of releases that failed because the address of the requestor did not match the address of the name.

ParWinsTotalNoOfSuccQueries {Par 17}
Indicates the number of queries that succeeded.

ParWinsTotalNoOfFailQueries {Par 18}
Indicates the number of queries that failed.

ParRefreshInterval {Par 19}
Indicates the Renewal interval in seconds (sometimes called the refresh interval).

ParTombstoneInterval {Par 20}
Indicates the Extinct interval in seconds.

ParTombstoneTimeout {Par 21}
Indicates the Extinct timeout in seconds.

ParVerifyInterval {Par 22}
Indicates the Verify interval in seconds.

ParVersCounterStartVal_LowWord {Par 23}
Indicates the Low Word of the version counter that WINS should start with.

ParVersCounterStartVal_HighWord {Par 24}
Indicates the High Word of the version counter that WINS should start with.

ParRplOnlyWCnfPnrs {Par 25}
Indicates whether replication is allowed with nonconfigured partners. If not set to zero, replication will be done only with partners listed in the Registry (except when an update notification comes in).

ParStaticDataInit {Par 26}
Indicates whether static data should be read in at initialization and reconfiguration time. Update of any MIB variable in the parameters group constitutes reconfiguration.

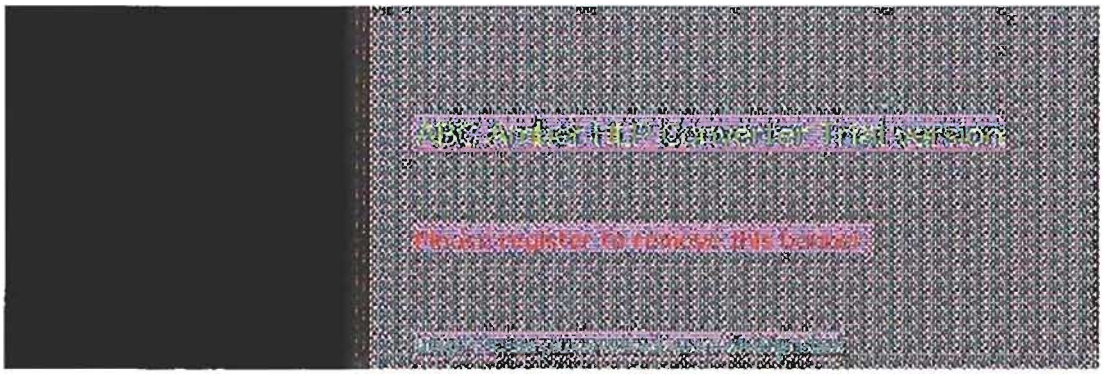
ParLogFlag {Par 27}
Indicates whether logging should be done. Logging is the default behavior.

ParLogFileName {Par 28}
Specifies the path to the log file.

ParBackupDirPath {Par 29}
Specifies the path to the backup directory.

ParDoBackupOnTerm {Par30}
Specifies whether WINS should perform a database backup upon termination. Values can be 0 (no) or 1 (yes). Setting this value to 1 has no meaning unless **ParBackupDirPath** is also set.

ParMigration {Par 31}
Specifies whether static records in the WINS database should be treated as dynamic records during conflict with new name registrations. Values can be 0 (no) or 1 (yes).



Microsoft WINS Objects

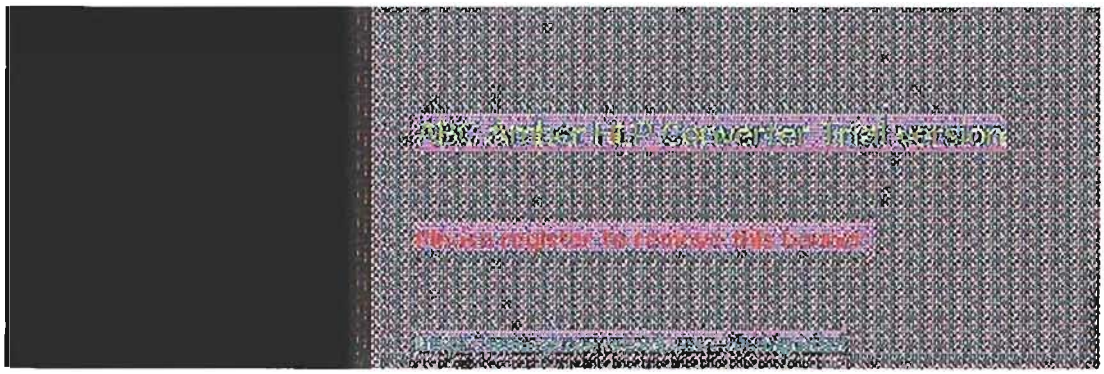
WINS Datafiles Group

DFDatafilesTable {Datafiles 1}
A list of datafiles specified under the \Datafiles key in the Registry. These files are used for static initialization of the WINS database.

dDFDatafileEntry {DFDatafilesTable 1}
Data file name record.

dFDatafileIndex {dDFDatafileEntry 1}
Used for indexing entries in the datafiles table. It has no other use.

dFDatafileName {dDFDatafileEntry 2}
Name of the datafile to use for static initialization.



Microsoft WINS Objects

WINS Pull Group

PullInitTime {Pull 1}
Indicates whether pull should be done at WINS invocation and at reconfiguration. If any pull or push group's MIB variable is set, that constitutes reconfiguration.

PullCommRetryCount {Pull 2}
Specifies the retry count in case of communication failure when doing pull replication. This is the maximum number of retries to be done at the interval specified for the partner before WINS stops for a set number of replication-time intervals before trying again.

PullPnrTable {Pull 3}
A list of partners with which pull replication needs to be done.

pPullPnrEntry {PullPnrTable 1}
The row corresponding to a partner.

PullPnrAdd {pPullPnrEntry 1}
The address of the remote WINS partner.

PullPnrSpTime {pPullPnrEntry 2}
Specifies the specific time at which pull replication should occur.

PullPnrTimeInterval {pPullPnrEntry 3}
Specifies the time interval for pull replication.

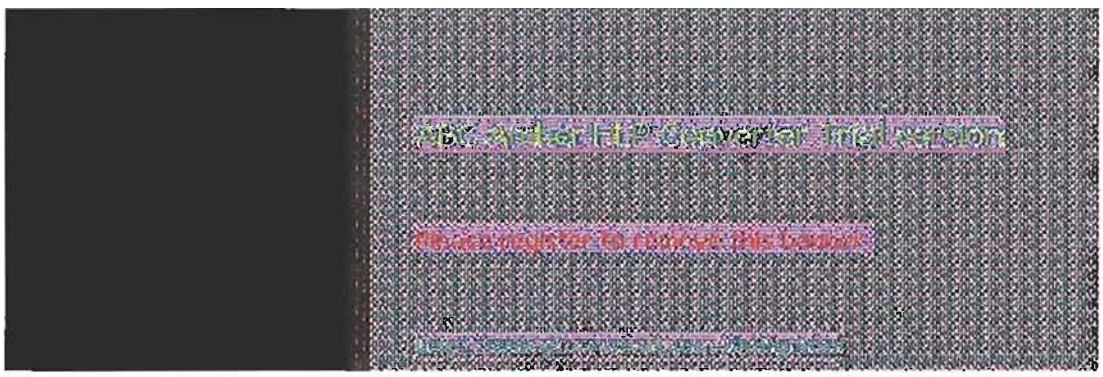
PullPnrMemberPrec {pPullPnrEntry 4}
The precedence to be given to members of the special group pulled from the WINS. The precedence of locally registered members of a special group is more than any replicas pulled in.

PullPnrNoOfSuccRpls {pPullPnrEntry 5}
The number of times replication was successful with the WINS after invocation or reset of counters.

PullPnrNoOfCommFails {pPullPnrEntry 6}
The number of times replication was unsuccessful with the WINS because of communication failure (after invocation or reset of counters).

PullPnrVersNoLowWord {pPullPnrEntry 7}
The Low Word of the highest version number found in records owned by this WINS.

PullPnrVersNoHighWord {pPullPnrEntry 8}
The High Word of the highest version number found in records owned by this WINS.



Microsoft WINS Objects

WINS Push Group

PushInitTime {Push 1}
Indicates whether a push (that is, notification message) should be done at invocation.

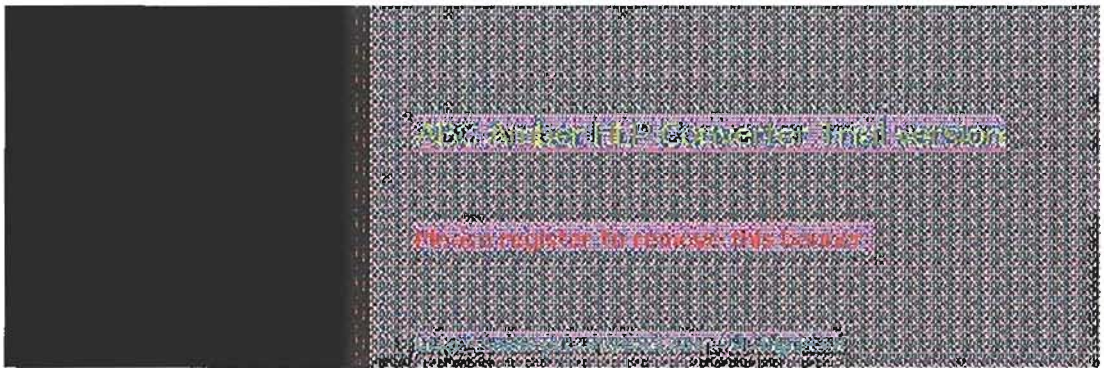
PushRplOnAddChg {Push 2}
Indicates whether a notification message should be sent when an address changes.

PushPnrTable {Push 3}
A list of WINS partners with which push replication is to be initiated.

pPushPnrEntry {PushPnrTable 1}
The row corresponding to the WINS partner.

PushPnrAdd {pPushPnrEntry 1}
Address of the WINS partner.

PushPnrUpdateCount {pPushPnrEntry 2}
Indicates the number of updates that should result in a push message.



Microsoft WINS Objects

WINS Cmd Group

CmdPullTrigger {Cmd 1}
This variable when set will cause the WINS to pull replicas from the remote WINS server identified by the IP address.

CmdPushTrigger {Cmd 2}
If set, causes WINS to push a notification message to the remote WINS server identified by the IP address.

CmdDeleteWins {Cmd 3}
If set, causes all information pertaining to a WINS server (data records, context information) to be deleted from the local WINS server . Use this only when the owner-address mapping table is nearing capacity. Deleting all information pertaining to the managed WINS is not permitted.

CmdDoScavenging {Cmd 4}
If set, causes WINS to do scavenging.

CmdDoStaticInit {Cmd 5}
If set, WINS will do static initialization using the file specified as the value. If 0 is specified, WINS will do static initialization using the files specified in the Registry (filenames can be read and written to using the Datafile table).

CmdNoOfWrkThds {Cmd 6}
Reads the number of worker threads in WINS.

CmdPriorityClass {Cmd 7}
Reads the priority class of WINS to normal or high.

CmdResetCounters {Cmd 8}
Resets the counters. Value is ignored.

CmdDeleteDbRecs {Cmd 9}
If set, causes all data records pertaining to a WINS server to be deleted from the local WINS server. Only data records are deleted.

CmdDRPopulateTable {Cmd 10}
Retrieves records of a WINS server whose IP address is provided. When this variable is set, the following table is generated immediately.

CmdDRDataRecordsTable {Cmd 11}
The table that stores the data records. The records are sorted lexicographically by name. The table is cached for a certain time (to save overhead on WINS). To regenerate the table, set the **CmdDRPopulateTable** MIB variable.

CmdDRRecordEntry {CmdDRDataRecordsTable 1}
Data record owned by the WINS server whose address was specified when **CmdDRPopulateTable** was set.

CmdDRRecordName {cCmdDRRecordEntry 1}
Name in the record.

CmdDRRecordAddress {cCmdDRRecordEntry 2}
Address(es) of the record. If the record is a multihomed record or an internet group, the addresses are returned sequentially in pairs. Each pair comprises the address of the owner WINS server followed by the address of the computer or of the internet group member. The records are always returned in network byte order.

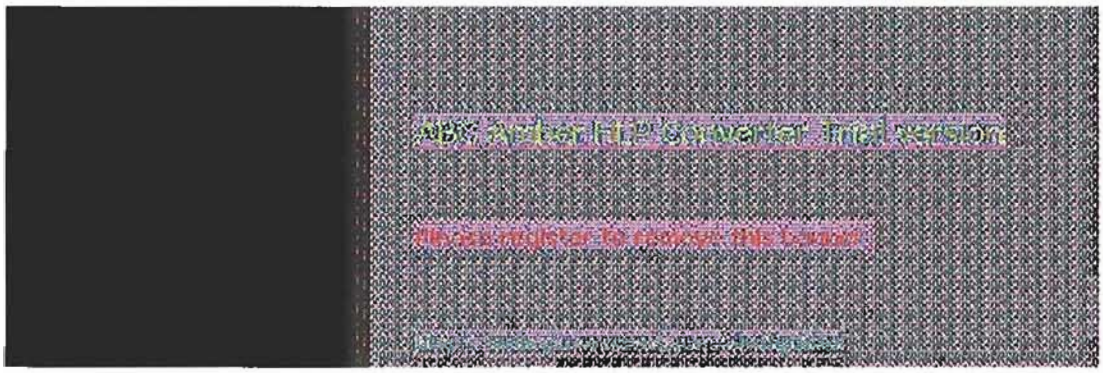
CmdDRRecordType {cCmdDRRecordEntry 3}
Type of record as unique, multihomed, normal group, or internet group.

CmdDRRecordPersistenceType {cCmdDRRecordEntry 4}
Persistence type of the record as static or dynamic.

CmdDRRecordState {cCmdDRRecordEntry 5}
State of the record as active, released, or extinct.

CmdWinsVersNoLowWord {Cmd 12}
The Low Word of the version number counter of the record.

CmdWinsVersNoHighWord {Cmd 13}
The High Word of the version number counter of the record.



Windows Sockets Applications

Vendors

AGE Logic, Inc.
9985 Pacific Heights Blvd.
San Diego, CA 92121
Phone: (619) 455-8600
Fax: (619) 597-6030
X Window software

American Computer & Electronics Corp.
209 Perry Parkway
Gaithersburg, MD 20877
Phone: (301) 258-9850
Fax: (301) 921-0434
Network management

Attachmate Corporation
3617 131st Avenue SE
Bellevue, WA 98006-9930
Phone: (800) 426-6283
Fax: (206) 747-9924
Terminal emulation

Beame and Whiteside
P.O. Box 8130
Dundas, Ontario L9H 5E7
CANADA
Phone: (416) 765-0822
Fax: (416) 765-0815
Terminal emulation, file transfer, remote process execution, e-mail, NFS, network printing
Digital Equipment Corporation
Attn: Lori Heron
2 Results Way
MR02-2/D10
Marlboro, MA 01752-3011
Phone: (508) 467-7855
Fax: (508) 467-1926
eXcursion, X Window server and client libraries

Distinct Corporation
14395 Saratoga Ave. Suite 120
Saratoga, CA 95070
Phone: (408) 741-0781
Fax: (408) 741-0795
Terminal emulation, file transfer, X Window, remote process execution, e-mail, NFS, ONC/RPC

Esker, Inc.
1181 Chess Drive, Suite C
Foster City, CA 94404
Phone: (415) 341-9065
Fax: (415) 341-6412
Terminal emulation, file transfer, X Window, remote process execution, NFS

Executive Systems/XTree Company
4115 Broad Street Bldg. #1
San Luis Obispo, CA 93401-7993
Phone: (805) 541-0604
Fax: (805) 541-4762
Network management
Frontier Technologies Corporation
10201 North Port Washington Road
Mequon, Wisconsin 53092
Phone: (414) 241-4555
Fax: (414) 241-7084
Terminal emulation, file transfer, remote process execution, e-mail, NFS, NNTP, TelnetD, network printing

Gallagher & Robertson A/S
Postboks 1824, Vika
0123 OSLO
NORWAY
Phone: (+47) 2 41 85 51
Fax: (+47) 2 42 89 22
Terminal emulation, file transfer

Genisys Comm, Inc.
314 S. Jay Street
Rome, NY 13440
Phone: (315) 339-5502
Fax: (315) 339-5528
Terminal emulation, file transfer

Gradient Technologies, Inc.
577 Main Street, Suite 4
Hudson, MA 01749
Phone: (508) 562-2882
Fax: (508) 562-3549
DCE (OSF distributed computing environment)

Hummingbird Communications Ltd.
2900 John Street, Unit 4
Markham, Ontario L3R 5G3
CANADA
Phone: (416) 470-1203
Fax: (416) 470-1207
File transfer, remote process execution, terminal emulation, X Window

Hypercube, Inc.
Unit 7-419 Phillip Street
Waterloo, Ontario N2L 3X2
CANADA
Phone: (519) 725-4040
Fax: (519) 725-5193
Modeling software, remote process execution

I-Kinetics, Inc.
19 Bishop Allen Drive
Cambridge, MA 02139
Phone: (617) 661-8181
Fax: (617) 661-8625
Middleware, remote process execution

John Fluke Mfg. Co.

P.O. Box 9090
Everett, WA 98206
Phone: (206) 356-5847
Fax: (206) 356-5790
Instrument control software

JSB Computer Systems Ltd.
Cheshire House, Castle Street
Macclesfield, Cheshire
ENGLAND SK11 6AF
Phone: (+44) 625-433618
Fax: (+44) 625-433948

JSB Corporation [USA]
Suite 115, 108 Whispering Pines Drive
Scotts Valley, CA 95066
Phone: (408) 438-8300
Fax: (408) 438-8360
Terminal emulation, file transfer, X Window, remote process execution, virtual sockets library

Lanera Corporation
516 Valley Way
Milpitas, CA 95035
Phone: (408) 956-8344
Fax: (408) 956-8343
Terminal emulation, file transfer, X Window, remote process execution, NFS, SNMP

Microdyne Corp.
239 Littleton Road
Westford, MA 01886
Phone: (508) 392-9953
Fax: (508) 392-9962
File transfer

NetManage, Inc.
20823 Stevens Creek Blvd.
Cupertino, CA 95014
Phone: (408) 973-7171
Fax: (408) 257-6405
Terminal emulation, file transfer, X Window, e-mail, NFS, TN3270, BIND, SNMP

Network Computing Devices
9590 SW Gemini
Beaverton, OR 97005
Phone: (503) 641-2200
Fax: (503) 643-8642
X Window

Spry, Inc.
1319 Dexter Ave. N
Seattle, WA 98109
Phone: (206) 286-1412
Fax: (206) 286-1722
Terminal emulation, file transfer, e-mail, network printing

SunSelect
2 Elizabeth Drive
Chelmsford, MA 01824-4195
Phone: (508) 442-2300
Fax: (508) 250-2300

E-mail

TurboSoft Pty Ltd.
248 Johnston Street
Annandale, NSW 2038
AUSTRALIA
Phone: (+612) 552-1266
Fax: (+612) 552-3256
Terminal emulation, file transfer, network printing

Unipalm Ltd.
216, Science Park, Milton Road
Cambridge, Cambridgeshire
CB4 4WA ENGLAND
Phone: (+44) 223-420002
Fax: (+44) 223-426868
E-mail

VisionWare UK
57 Cardigan Lane
Leeds, ENGLAND LS4 2LE
Phone: (+44) 532-788858
Fax: (+44) 532-304676

VisionWare USA
1020 Marsh Road
Suite 220
Menlo Park, CA 94025
Phone: (415) 325-2113
Fax: (415) 325-8710
Terminal emulation, file transfer, X Window, remote process execution

VisiSoft
430 10th Street NW, Suite S008
Atlanta, GA 30318
Phone: (404) 874-0428
Fax: (404) 874-6412
Network management

Walker Richer & Quinn, Inc.
1500 Dexter Ave. N.
Seattle, WA 98109
Phone: (206) 217-7500
Fax: (206) 217-0293
Terminal emulation, file transfer, X Window

XSoft
3400 Hillview Ave.
Palo Alto, CA 92304
Phone: (800) 428-2995
Fax: (415) 813-7028
Document management

Internet Sources for Applications

Celloftp.law.cornell.edu/pub/LII/Cellocello.zip, lview31.zip, gswin.zip, cellofaq.zip, wingif14.zip, wplny09b.zip

Cookie Serversunsite.unc.edu/pub/micro/pc-stuff /ms-windows/winsock/appscooksock.zip

EINet Wais Clientftp.cica.indiana.edu/pub/pc/win3/winsockewais154.zip

Finger Daemonsunsite.unc.edu/pub/micro/pc-stuff /ms-windows/winsock/appsfingerd.zip

Finger31ftp.cica.indiana.edu/pub/pc/win3/winsockfinger31.zip

GopherBookftp.cica.indiana.edu/pub/pc/win3/winsockgophbk11.zip

GopherSemwac.ed.ac.uk/pub/gophersgsi386.zip or gsalpha.zip

HGopherftp.cica.indiana.edu/pub/pc/win3/winsockhgoph24.zip
HTTPSemwac.ed.ac.uk/pub/httpshsi386.zip or hsalpha.zip

Internet Help Fileftp.ccs.queensu.ca/pub/msdos/tcpipipwin.zip

Micro X-Winbart.starnet.com/pubxwindemo.exe or xwin287b.exe

Mosaicftp.ncsa.uiuc.edu/PC/Mosaicwmos20a1.zip

NCSA Telnetftp.cica.indiana.edu/pub/pc/win3/winsockwintelb3.zip

PCEudoraftp.qualcomm.com/pceudora/windowseudora14.exe

QWS3270ftp.ccs.queensu.ca/pub/msdos/tcpipqws3270.zip

SerWebftp.cica.indiana.edu/pub/pc/win3/winsockserweb03.zip

Text Serversunsite.unc.edu/pub/micro/pc-stuff /ms-windows/winsock/appstxtsrv.zip

TimeSyncftphost.cac.washington.edu/pub/winsocktsync1_4.zip

Trumpet for Windowsftp.utas.edu.au/pub/trumpet/wintrumpwtwsk10a.zip

Trumpet Telnetpetros.psychol.utas.edu.au/pc/trumpet/trmpteltrmptel.exe

Trumpet Winsockftp.utas.edu.au/pc/trumpet/wintrumpwinsock.zip

USGS WAIS Clientridgisd.er.usgs.gov/software/waiswwais23.zip

Wais Managerftp.cnidr.org/pub/NIDR.tools/wais/pc/windowswaisman3.zip

WFTPDsunsite.unc.edu/pub/micro/pc-stuff/ms-windows/winsock/appswftpd18b.zip

Windows SMTPsunsite.unc.edu/pub/micro/pc-stuff /ms-windows/winsock/appswsmtpd16.zip

WinFSPftp.cica.indiana.edu/pub/pc/win3/winsockwinfsp12.zip
WinIRCdorm.rutgers.edu (ftp.utas.edu.au)/pub/msdos/trumpet/irc

/pc/trumpet/irc/winirc-betawinirc.exe, winirc.doc

WinLPRsunsite.unc.edu/pub/micro/pc-stuff /ms-windows/winsock/appswinlpr10.zip

WinQVT/Netsunsite.unc.edu/pub/micro/pc-stuff /ms-windows/winsock/appsqvtne394.zip

WinQVT/Net for NTsunsite.unc.edu/pub/micro/pc-stuff /ms-windows/winsock/appsqvtnt394.zip

WinQVTNetbiochemistry.cwru.edu/pub/qvtnetqvtws396.zip

WinTalkelf.com/pub/wintalkwintalk.zip

WinVNtitan.ksc.nasa.gov/pub/win3/winvnwinvnstd90_2.zip

WS Gophersunsite.unc.edu/pub/micro/pc-stuff /ms-windows/winsock/appswsg-09g.exe

WS_Fingersunsite.unc.edu/pub/micro/pc-stuff /ms-windows/winsock/appswsfinger.zip

WS_FTPftp.usma.edu/pub/msdosws_ftp.zip

WS_FTPbsunsite.unc.edu/pub/micro/pc-stuff /ms-windows/winsock/appsws_ftpb zip, view.zip

WSArchieftp.demon.co.uk/pub/ibmpc/winsock/apps/wsarchiewsarchie.zip