

---

## Administering DHCP Clients

After you have established the scope and defined the range of available and excluded IP addresses, DHCP-enabled clients can begin using the service for automatic TCP/IP configuration.

You can use DHCP Manager to manage individual client leases, including creating and managing reservations for clients.

---

### Tip

You can use the **ipconfig** utility to troubleshoot the IP configuration on computers that use DHCP, as described in Chapter 11, "Utilities Reference." You can also use **ipconfig** on TCP/IP-32 clients on Windows for Workgroups 3.11 computers and on computers running Microsoft Network Client version 2.0 for MS-DOS.

---

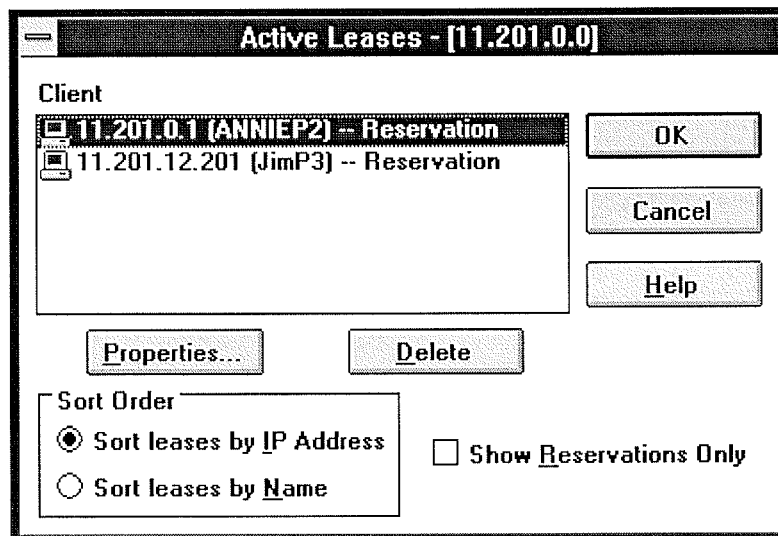
## Administering DHCP Clients

### Managing Client Leases

The lease for the IP address assigned by a DHCP server has an expiration date, which the client must renew if it is going to continue to use that address. You can view the lease duration and other information for specific DHCP clients, and you can add options and change settings for reserved DHCP clients.

#### ► To view client lease information

1. In the DHCP Servers list in the DHCP Manager window, select the scope for which you want to view or change client information.
2. From the Scope menu, choose Active Leases.



3. In the Active Leases dialog box, select the computer whose lease you want to view in the IP Address list, and then choose the Properties button.

If you want to view only clients that use reserved IP addresses, check the Show Reservations Only box.

4. In the Client Properties dialog box, you can view the unique identifier and other client information, including the lease expiration date.

**Client Properties**

IP Address: 11 .201.0 .1

Unique Identifier: 2340897432

Client Name: ANNIEP2

Client Comment: Net admin machine

Lease Expires: 1994/09/16 20:53

OK Cancel Help Options

---

**Note**

You can only edit the name, unique ID, and comment, or choose the Options button in the Client Properties dialog box for clients with reserved IP addresses.

---

For information about the Options button in this dialog box, see "Defining Options for Reservations" earlier in this chapter.

You can cancel the DHCP configuration information for a DHCP client that is no longer using an IP address or for all clients in the scope. This has the same effect as if the client's lease expired-the next time that client computer starts, it must enter the rebinding state and obtain new TCP/IP configuration information from a DHCP server.

---

**Important**

Delete only entries for clients that are no longer using the assigned DHCP configuration. Deleting an active client could result in duplicate IP addresses on the network, because deleted addresses will be assigned to new active clients.

You can use **ipconfig /release** at the command prompt for a DHCP client computer to delete an active client entry and safely free its IP address for reuse.

---

► **To cancel a client's DHCP configuration**

1. Make sure the client is not using the assigned IP address.
2. In the IP Client list of the Active Leases dialog box, select the client you want to cancel, and then choose the Delete button.

## Administering DHCP Clients

### Managing Client Reservations

You can reserve a specific IP address for a client. Typically, you will need to reserve addresses in the following cases:

- For domain controllers if the network also uses LMHOSTS files that define IP addresses for domain controllers
- For clients that use IP addresses assigned using another method for TCP/IP configuration
- For assignment by RAS servers to non-DHCP clients
- For DNS servers

If multiple DHCP servers are distributing addresses in the same scope, the client reservations on each DHCP server should be identical. Otherwise, the DHCP reserved client will receive different IP addresses, depending on the responding server.

#### Important

The IP address and static name specified in WINS take precedence over the IP address assigned by the DHCP server. For such clients, create client reservations with the IP address that is defined in the WINS database.

#### ► To add a reservation for a client

1. From the Scope menu, choose Add Reservations.

The screenshot shows a dialog box titled "Add Reserved Clients". It has a standard Windows-style title bar with a close button on the left. The dialog contains four input fields, each with a label and a text box:

- IP Address:** The text box contains "11 .105.41 .25".
- Unique Identifier:** The text box contains "08002b2b3308".
- Client Name:** The text box contains "MIKEMAS1".
- Client Comment:** The text box is empty.

At the bottom of the dialog, there are four buttons: "Add", "Close", "Help", and "Options".

2. In the Add Reserved Clients dialog box, type information to identify the first reserved client:
  - IP Address specifies an address from the reserved address pool. You can specify any reserved, unused IP address. DHCP Manager checks and warns you if a duplicate or nonreserved address is entered.
  - Unique Identifier usually specifies the media access control (MAC) address for the client computer's network adapter card. You can determine this address by typing **net config wksta** at the command prompt on the client computer.
  - Client Name specifies the computer name for this client. This is used for identification purposes only and does not affect the actual computer name for the client. This is not

available for MS-DOSbased clients; in this case, only the Unique Identifier appears.

- Client Comment is any optional text that you enter to describe this client.

3. Choose the Add button to add the reservation to the DHCP database. You can continue to add reservations without dismissing this dialog box.
4. When you have added all reservations, choose the Close button.

After the IP address is reserved in DHCP Manager, the client computer must be restarted to be configured with the new IP address.

If you want to change a reserved IP address for a client, you have to remove the old reserved address and add a new reservation. You can change any other information about a reserved client while keeping the reserved IP address.

▶ **To change the reserved IP address**

1. Make sure the reserved client is not using the old IP address. To do this, shut down the client computer immediately after issuing the **ip config/release** command on that client computer.
2. In the Active Leases dialog box, select the reserved IP address in the Client list, and choose the Delete button. Then choose the OK button.
3. From the Scope menu, choose Add Reservations, and then enter information for a new reservation as described earlier in this section.

▶ **To change basic information for a reserved client**

1. From the Scope menu, choose Active Leases.
2. In the Client list of the Active Leases dialog box, select the address of the reserved client that you want to change, and then choose the Properties button.
3. In the Client Properties dialog box, change the unique identifier, client name, or comment, and then choose the OK button.

---

**Note**

You can only change values in the Client Properties dialog box for reserved clients.

---

You can also view and change the options types that define configuration parameters for selected reserved clients by choosing the Options button in the Client Properties dialog box. Changing options for a reserved client follows the same procedure as use to originally define options, as described in "Defining Options for Reservations" earlier in this chapter.

---

### Managing the DHCP Database Files

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

- DHCP.MDB is the DHCP database file.
- DHCP.TMP is a temporary file that DHCP creates for temporary database information.
- JET.LOG and the JET\*.LOG files contain logs of all transactions done with the database. These files are used by DHCP to recover data if necessary.
- SYSTEM.MDB is used by DHCP for holding information about the structure of its database.

---

#### **Caution**

The DHCP.TMP, DHCP.MDB, JET.LOG, and SYSTEM.MDB files should not be removed or tampered with.

---

The DHCP database and related Registry entries are backed up automatically at a specific interval (15 minutes by default), based on the value of Registry parameters (as described later in this chapter). You can also forced database backup while working in DHCP Manager.

### Troubleshooting DHCP

The following error conditions can appear to indicate potential problems with the DHCP server:

- The administrator can't connect for a DHCP server using DHCP Manager. The message that appears might be, "The RPC server is unavailable."
- DHCP clients cannot renew the leases for their IP addresses. The message that appears on the client computer is, "The DHCP client could not renew the IP address lease."
- The DHCP Client service or Microsoft DHCP Server service may be down and cannot be restarted.

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

#### ► To ensure the DHCP services are running

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

In the Services dialog box for the client computer, Started should appear in the Status column for the DHCP Client service. For the DHCP server itself, the Started should appear in the Status column for the Microsoft DHCP Server service.

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

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

#### ► To restart a DHCP 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 log on under an account with Administrator rights.
3. At the command prompt, type **net start dhcpcserver** and press Enter.

---

#### Note

Use Event Viewer to find the possible source of problems with DHCP services.

---

## Troubleshooting DHCP

### Restoring the DHCP Database

If you ascertain that the DHCP services are running on both the client and server computers but the error conditions described earlier persist, then the DHCP database is not available or has become corrupted. If a DHCP server fails for any reason, you can restore the database from the automatic backup files.

▶ **To restore a DHCP database**

- Restart the DHCP server. If the DHCP database has become corrupted, it is automatically restored from the DHCP backup directory specified in the Registry, as described later in this chapter.

▶ **To force the restoration of a DHCP database**

- Set the value of **RestoreFlag** in the Registry to 1, and then restart the computer. For information about this parameter, see "Registry Parameters for DHCP Servers" later in this chapter.

▶ **To manually restore a DHCP database**

- If the two restore methods described earlier do not work, manually copy all DHCP database files from the backup directory to the \DHCP working directory. Then restart the Microsoft DHCP Server service.



### **Troubleshooting DHCP**

#### **Backing up the DHCP Database onto Another Computer**

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

▶ **To move a DHCP database**

- Use the Replicator service to copy the contents of the DHCP backup directory to the new computer.

## Advanced Configuration Parameters for DHCP

This section presents configuration parameters that affect the behavior of DHCP servers and clients, and that can be modified only through Registry Editor. For the changes to take effect after you modify any of these value entries, you must restart the Microsoft DHCP Server service for server parameters or the DHCP Client service for client parameters.

---

### Caution

You can impair or disable Windows NT if you make incorrect changes in the Registry while using Registry Editor. Whenever possible, use DHCP 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 the DHCP server or client 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 subkey for the specific parameter, as described in the following sections.

The following sections describe the value entries for parameters for DHCP servers and clients that can be set only by adding an entry or changing their values in Registry Editor.

## Advanced Configuration Parameters for DHCP

### Registry Parameters DHCP Servers

When you change any of these parameters except **RestoreFlag**, you must restart the computer for the changes to take effect. For the **RestoreFlag** parameter, you must restart the Microsoft DHCP Server service.

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

..SYSTEM\current\currentcontrolset\services\DHCPServer\Parameters

#### APIProtocolSupport

Data type = REG\_DWORD  
Range = 0x1, 0x2, 0x4, 0x5, 0x7  
Default = 0x1

Specifies the supported protocols for the DHCP server. You can change this value to ensure that different computers running different protocols can access the DHCP server. The values for this parameter can be the following:

0x1	For RPC over TCPIP protocols
0x2	For RPC over named pipes protocols
0x4	For RPC over local procedure call (LPC) protocols
0x5	For RPC over TCPIP and RPC over LPC
0x7	For RPC over all three protocols (TCP/IP, named pipes, and LPC)

#### BackupDatabasePath

Data type = REG\_EXPAND\_SZ  
Range = *filename*  
Default = %SystemRoot%\system32\dhcp\backup

Specifies the location of the backup database file where the database is backed up periodically. The best location for the backup file is on another hard drive, so that the database can be recovered in case of a system drive crash. Do not specify a network drive, because DHCP Manager cannot access a network drive for database backup and recovery.

#### BackupInterval

Data type = REG\_DWORD  
Range = no limit  
Default = 15 minutes

Specifies the interval for backing up the database.

#### DatabaseCleanupInterval

Data type = REG\_DWORD  
Range = No limit  
Default = 0x15180 (864,000 minutes - 24 hours)

Specifies the interval for cleaning up expired client records from the DHCP database,

freeing up those IP addresses for reuse.

### **DatabaseLoggingFlag**

Data type = REG\_DWORD  
Range = 0 or 1  
Default = 1 (true-that is, database logging is enabled)

Specifies whether to record the database changes in the JET.LOG file. This log file is used after a system crash to recover changes that have not been made to the database file defined by **DatabaseName**. Database logging affects system performance, so **DatabaseLogging** can be turned off if you believe the system is highly stable and if logging is adversely affecting system performance.

### **DatabaseName**

Data type = REG\_SZ  
Range = *filename*  
Default = dhcp.mdb

Specifies the name of the database file to be used for the DHCP client information database.

### **DatabasePath**

Data type = REG\_EXPAND\_SZ  
Range = *pathname*  
Default = %SystemRoot%\System32\dhcp

Specifies the location of the database files that have been created and opened.

### **RestoreFlag**

Data type = REG\_DWORD  
Range = 0 or 1  
Default = 0 (false-that is, do not restore)

Specifies whether to restore the database from the backup directory. This flag is reset automatically after the successful restoration of the database.

## Advanced Configuration Parameters for DHCP Registry Parameters for DHCP Clients

The Registry parameters for DHCP clients are specified under the following key:

```
..SYSTEM\current\currentcontrolset\services\DHCP\Parameter\<option#>
```

The *Option#* keys are a list of DHCP options that the client can request from the DHCP server.

For each of the default options, the following values are defined:

### RegLocation

Data type = REG\_SZ

Default = Depends on the Registry location for the specific option

Specifies the location in the Registry where the option value is written when it is obtained from the DHCP server. The "?" character expands to the adapter name for which this option value is obtained.

### KeyType

Data type = REG\_DWORD

Default = 0x7

Specifies the type of Registry key for the option.

---

## **Guidelines for Setting Local Policies**

This section provides some suggestions for setting lease options, dividing the free address pool among DHCP servers, and avoiding DNS naming problems.

## Guidelines for Setting Local Policies

### Guidelines for Managing DHCP Addressing Policy

Allocation of IP addresses for distribution by DHCP servers can be done dynamically or manually. These methods use the same DHCP client-server protocol, but the network administrator manages them differently at the DHCP server.

#### Dynamic Allocation of IP Addresses

Dynamic allocation allows a client to be assigned an IP address from the free address pool. The lease for the address has a lease duration (expiration date), before which the client must renew the lease to continue using that address. Depending on the local lease policies defined by the administrator, dynamically allocated addresses can be returned to the free address pool if the client computer is not being used, if it is moved to another subnet, or if its lease expires. Any IP addresses that are returned to the free address pool can be reused by the DHCP server when allocating an IP address to a new client. Usually the local policy ensures that the same IP address is assigned to a client each time that system starts and that addresses returned to the pool are reassigned.

After the renewal time of the lease time has passed, the DHCP client enters the *renewing* state (as described in Chapter 3, "Networking Concepts for TCP/IP"). The client sends a request message to the DHCP server that provided its configuration information. If the request for a lease extension fits the local lease policy, the DHCP server sends an acknowledgment that contains the new lease and configuration parameters. The client then updates its configuration values and returns to the bound state.

When the DHCP client is in the renewing state, it must release its address immediately in the rare event that the DHCP server sends a negative acknowledgment. The DHCP server sends this message to inform a client that it has incorrect configuration information, forcing it to release its current address and acquire new information.

If the DHCP client cannot successfully renew its lease, the client enters a *rebinding* state. At this stage, the client sends a request message to all DHCP servers in its range, attempting to renew its lease. Any server that can extend the lease sends an acknowledgment containing the extended lease and updated configuration information. If the lease expires or if a DHCP server responds with a negative acknowledgment, the client must release its current configuration and return to the initializing state. (This happens automatically, for example, for a computer that is moved from one subnet to another.)

If the DHCP client uses more than one network adapter to connect to multiple networks, this protocol is followed for each adapter that the user wants to configure for TCP/IP. Windows NT allows multihomed systems to selectively configure any combination of the system's interfaces. You can use the **ipconfig** utility to view the local IP configuration for a client computer.

When a DHCP-enabled computer is restarted, it sends a message to the DHCP server with its current configuration information. The DHCP server either confirms this configuration or sends a negative reply so that the client must begin the initializing stage again. System startup might therefore result in a new IP address for a client computer, but neither the user nor the network administrator has to take any action in the configuration process.

#### Manual Allocation of IP Addresses

Manual allocation follows the policy used in most current TCP/IP implementations. With this method, the network administrator defines the IP address and other configuration options that

the DHCP servers will provide for a particular computer. The DHCP servers respond based on the client's unique identifier, which is the network adapter's MAC-layer address. Any IP addresses assigned in this way cannot be allocated by DHCP servers to other clients using either automatic or dynamic allocation. The address has a permanent lease.

For example, for the range of IP addresses to be provided through RAS servers, these addresses should be manually excluded from the range of dynamically allocated addresses.



## Guidelines for Setting Local Policies

### Guidelines for Lease Options

To define appropriate values for lease duration, you should consider the frequency of the following events for your network:

- Changes to DHCP options and default values
- Network interface failures
- Computer removals for any purpose
- Subnet changes by users because of office moves, laptop computers docked at different workstations, and so on

All of these types of events cause IP addresses to be released by the client or cause the leases to expire at the DHCP server. Consequently, the IP addresses will be returned to the free address pool to be reused.

If many changes occur on your internetwork, you should assign short lease times, such as two weeks. This way, the addresses assigned to systems that leave the subnet can be reassigned quickly to new DHCP client computers requesting TCP/IP configuration information.

Another important factor is the ratio between connected computers and available IP addresses. For example, the demand for reusing addresses is low in a network where 40 systems share a class C address (with 254 available addresses). A long lease time such as two months would be appropriate in such a situation. However, if 230 computers share the same address pool, demand for available addresses is much greater, so a lease time of a few days or weeks is more appropriate.

Notice, however, that short lease durations require that the DHCP server be available when the client seeks to renew the lease. So backup servers are especially important when short lease durations are specified.

## Guidelines for Setting Local Policies

### Guidelines for Partitioning the Address Pool

You will probably decide to install more than one DHCP server, so the failure of any individual server will not prevent DHCP clients from starting. However, DHCP does not provide a way for DHCP servers to cooperate in ensuring that assigned addresses are unique. Therefore, you must divide the available address pool among the DHCP servers to prevent duplicate address assignment.

A typical scenario is a local DHCP server that maintains TCP/IP configuration information for two subnets. For each DHCP server, the network administrator allocates 70 percent of the IP address pool for local clients and 30 percent for clients from the remote subnet, and then configures a relay agent to deliver requests between the subnets.

This scenario allows the local DHCP server to respond to requests from local DHCP clients most of the time. The remote DHCP server will assign addresses to clients on the other subnet only when the local server is not available or is out of addresses. This same method of partitioning among subnets can be used in a multiple subnet scenario to ensure the availability of a responding server when a DHCP client requests configuration information.

## Guidelines for Setting Local Policies

### Guidelines for Avoiding DNS Naming Conflicts

DNS can be used to provide names for network resources, as described in Chapter 3, "Networking Concepts for TCP/IP." However, DNS configuration is static. With DHCP, a host can easily have a different IP address if its lease expires or for other reasons, but there is no standard for updating DNS servers dynamically when IP address information changes. Therefore, DNS naming conflicts can occur if you are using DHCP for dynamic allocation of IP addresses.

This problem will primarily affect systems that extend internetworking services to local network users. For example, a server acting as an anonymous FTP server or as an e-mail gateway might require users to contact it using DNS names. In such cases, such clients should have reserved leases with an unlimited duration..

For workstations in environments that do not require the computers to register in the DNS name space, DHCP dynamic allocation can be used without problems.

## Guidelines for Setting Local Policies

### Using DHCP with Diskless Workstations

If your network includes diskless workstations or X terminal BOOTP clients that need configuration information to use TCP/IP, you must build profiles. (BOOTP is the internetworking Bootstrap Protocol used to configure systems across internetworks. DHCP is an extension of BOOTP.)

You might decide to continue to manage these workstations using your existing BOOTP servers. If so, you must be sure to exclude these addresses from the free address pool maintained by the DHCP server.

## Planning a Strategy for DHCP

This section describes how to develop strategies for placing DHCP servers on small-scale and large-scale installations. Most network administrators implementing DHCP will also be planning a strategy for implementing WINS servers. The planning tasks described here also apply for WINS servers, and in fact, the administrator will probably want to plan DHCP and WINS implementation in tandem.

The following describes the general planning tasks:

1. Compile a list of a requirements, including:
  - Client support (numbers and kinds of systems to be supported)
  - Interoperability with existing systems, especially requirements for mission-critical accounting, personnel, and similar information systems
  - Hardware support and related software compatibility (including routers, switches, and servers)
  - Network monitoring software, including SNMP requirements and other tools
2. Isolate the areas of the network where processes must continue uninterrupted, and target these areas for the last stages of implementation.
3. Review the geographic and physical structure of the network to determine the best plan for defining logical subnets as segments of the internetwork.
4. Define the components in the new system that require testing, and develop a phase plan for testing and adding components.

For example, the plan could define units of the organization to be phased into using DHCP, and the order for types of computers to be phased in (including Windows NT servers and workstations, Microsoft RAS servers and clients, Windows for Workgroups computers, and MS-DOS clients).

5. Create a pilot project for testing. Be sure that the pilot project addresses all the requirements identified in Task #1.
6. Create a second test phase, including tuning the DHCP (and WINS) server-client configuration for efficiency. This task can include determining strategies for backup servers and for partitioning the address pool at each server to be provided to local versus remote clients.
7. Document all architecture and administration issues for network administrators.
8. Implement a final phase for bringing all organizational units into using DHCP.

While planning, remember that the actual placement of the servers in the physical network need not be a major planning issue. DHCP servers (and WINS servers) do not participate in the Windows NT Server domain model, so domain membership is not an issue in planning for server placement. Because most routers can forward DHCP configuration requests, DHCP servers are not required on every subnet in the internetwork. Also, because these servers can be administered remotely from any Windows NT Server computer that is DHCP- or WINS-enabled, location is not a major issue in planning for server placement.

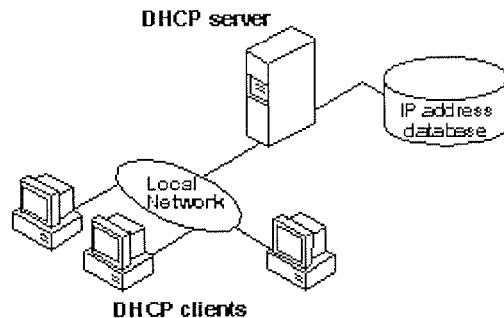
## Planning a Strategy for DHCP

### Planning a Small-Scale Strategy for DHCP Servers

For a small LAN that does not include routers and subnetting, the server needs for the network can probably be provided with a single DHCP server.

Planning in this case includes determining the following:

- The hardware and storage requirements for the DHCP server
- Which computers can immediately become DHCP clients for dynamic addressing and which should keep their static addresses
- The DHCP option types and their values to be predefined for the DHCP clients

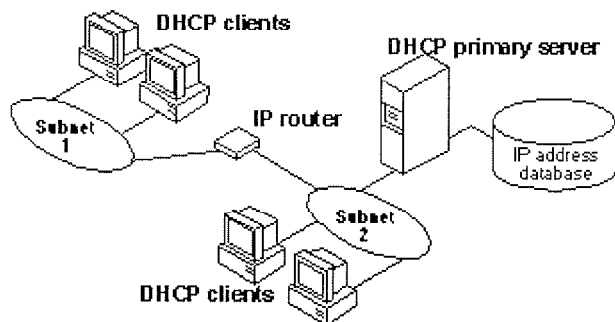


A Single Local Network Using Automatic TCP/IP Configuration with DHCP

### Planning a Strategy for DHCP

#### Planning a Large-Scale Strategy for DHCP Servers

The network administrator can use relay agents implementing RFC 1542 (usually IP routers) so that DHCP servers located on one node of the internetwork can respond to TCP/IP configuration requests from remote nodes. The relay agent forwards requests from local DHCP clients to the DHCP server and subsequently relays responses back to the clients.



#### An Internetwork Using Automatic TCP/IP Configuration with DHCP

The additional planning issues for a large enterprise network includes:

- Compatibility of hardware and software routers with DHCP, as described at the beginning of this chapter.
- Planning the physical subnetting of the network and relative placement of DHCP servers. This includes planning for placement of DHCP (and WINS servers) among subnets in a way that reduces b-node broadcasts across routers.
- Specifying the DHCP option types and their values to be predefined per scope for the DHCP clients. This may include planning for scopes based on the needs of particular groups of users. For example, for a marketing group that uses portable computers docked at different stations, or for a unit that frequently moves computers to different locations, shorter lease durations can be defined for the related scopes. This way, frequently changed IP addresses can be freed for reuse.

As one example, the segmenting of the WAN into logical subnets could match the physical structure of the internetwork. Then one IP subnet can serve as the backbone, and off this backbone each physical subnet would maintain a separate IP subnet address.

In this case, for each subnet a single computer running Windows NT Server could be configured as both the DHCP and WINS server. Each server would administer a defined number of IP addresses with a specific subnet mask, and would also be defined as the default gateway. Because the server is also acting as the WINS server, it can respond to name resolution requests from all systems on its subnet.

These DHCP and WINS servers can in turn be backup servers for each other. The administrator can partition the address pool for each server to provide addresses to remote clients.

There is no limit to the maximum number of clients that can be served by a single DHCP server. However, your network may have practical constraints based on the IP address class and server configuration issues such as disk capacity and CPU speed.

# Installing and Configuring WINS Servers

A WINS server is a Windows NT Server computer running Microsoft TCP/IP and the Windows Internet Name Service (WINS) server software. WINS servers maintain a database that maps computer names to IP addresses, allowing users to easily communicate with other computers while gaining all the benefits of TCP/IP.

This chapter describes how to install WINS servers and how to use WINS Manager to manage these servers. The topics include the following:

- WINS benefits
- Installing and administering WINS servers
- Configuring WINS servers and replication partners
- Managing static mappings
- Setting preferences for WINS Manager
- Managing the WINS database
- Troubleshooting WINS
- Advanced configuration parameters for WINS
- Planning a strategy for WINS servers

For an overview of how WINS works, see "Windows Internet Name Service and Broadcast Name Resolution" in Chapter 3, "Networking Concepts for TCP/IP."

---

**Note**

WINS can also be configured and monitored using SNMP. All configuration parameters can be set using SNMP, including configuration parameters that can otherwise only be set by editing the Registry. For a list of WINS MIB object types, see Appendix A, "MIB Object Types for Windows NT."

You can also use Performance Monitor to track WINS server performance, as described in Chapter 8, "Using Performance Monitor with TCP/IP Services."

---



---

## WINS Benefits

Using WINS servers can offer these benefits on your internetwork:

- Dynamic database maintenance to support computer name registration and name resolution. Although WINS provides dynamic name services, it offers a NetBIOS namespace, making it much more flexible than DNS for name resolution.
- Centralized management of the computer name database and the database replication policies, alleviating the need for managing LMHOSTS files.
- Dramatic reduction of IP broadcast traffic in Microsoft internetworks, while allowing client computers to easily locate remote systems across local or wide area networks.
- The ability for clients on a Windows NT Server network (including Windows NT, Windows for Workgroups, and LAN Manager 2.x) to browse domains on the far side of a router without a local domain controller being present on the other side of the router.
- A scalable design, making it a good choice for name resolution for medium to very large internetworks.

---

### Note

WINS client software is part of the Microsoft TCP/IP-32 for Windows for Workgroups and the Microsoft Network Client 2.0 software that is included on the Windows NT Server compact disc. For information about installing these clients, see the *Windows NT Server Installation Guide*.

---

## Installing WINS Servers

You install a WINS server as part of the process of installing Microsoft TCP/IP in Windows NT Server. These instructions assume you have already installed the Windows NT Server operating system on the computer.



You must be logged on as a member of the Administrators group to install a WINS server.

### ► To install a WINS server

1. Choose the Network options in Control Panel. When the Network Settings dialog box appears, choose the Add Software button.
2. In the Network Software list in the Add Network Software dialog box, select TCP/IP Protocol And Related Components, and then choose the Continue button.
3. In the Windows NT TCP/IP Installation Options dialog box, check the appropriate options to install, including at least the following:
  - WINS Server Service
  - SNMP Service (for configuring and monitoring WINS using SNMP or Performance Monitor)
4. Choose the OK button. Windows NT Setup displays a message asking for the full path to the Windows NT Server distribution files. Type the appropriate location, and choose the Continue button.

All necessary files are copied to your hard disk.

5. 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.

All the appropriate TCP/IP and WINS server software is ready for use after you reboot the computer.

The Windows Internet Name Service is a Windows NT service running on a Windows NT computer. The supporting WINS client software is automatically installed for Windows NT Server and for Windows NT computers when the basic operating system is installed.

### ► To start and stop the WINS service on any Windows NT computer

1. In Control Panel, choose the Services icon.

Or

In Server Manager, choose Services from the Computer menu.

2. In the Services dialog box, select the Windows Internet Name Service, and choose the Start or Stop button. Then choose the Close button.

You can start and stop the WINS service at the command prompt using the commands **net start wins** or **net stop wins**.



## 5 Installing and Configuring WINS Servers

4 of 27

### Administering WINS Servers

When you install a WINS server, an icon for WINS Manager is added to the Network Administration group in Program Manager. You can use this tool to view and change parameters for any WINS server on the internetwork. To administer a WINS server remotely, you can run WINS Manager on a Windows NT Server computer that is not a WINS server.



You must be logged on as a member of the Administrators group for a WINS server to configure that server.

#### ► To start WINS Manager



1. Double-click the WINS Manager icon in Program Manager.

Or

At the command prompt, type **start winsadm** and press Enter. You can include a WINS server name or IP address with the command, for example, **start winsadm 11.103.41.12** or **start winsadm myserver**.

2. If the Windows Internet Name Service is running on the local computer, that WINS server is opened automatically for administration. If the Windows Internet Name Service is not running when you start WINS, the Add WINS Server dialog box appears, as described in the following procedure.

WINS Manager - (Local)	
Server View Mappings Options Help	
WINS Servers	Statistics
1.101.4.162	Server Start Time: 5/19/94 1:38:45 PM
11.103.41.12	Database Initialized: -- --
	Statistics Cleared: -- --
	Last Replication Times:
	Periodic: -- --
	Admin Trigger: -- --
	Net Update: -- --
	Total Queries Received: 34589
	Successful: 34001
	Failed: 488
	Total Releases: 345
	Successful: 321
	Failed: 24
	Total Registrations: 33456

Ready

---

**Note**

If you specify an IP address when connecting to a WINS server, the connection is made using TCP/IP. If you specify a computer name, the connection is made over NetBIOS. The list that appears in the WINS Server window shows the IP address first if you connected using TCP/IP, or the computer name first, if the connection was made over NetBIOS.

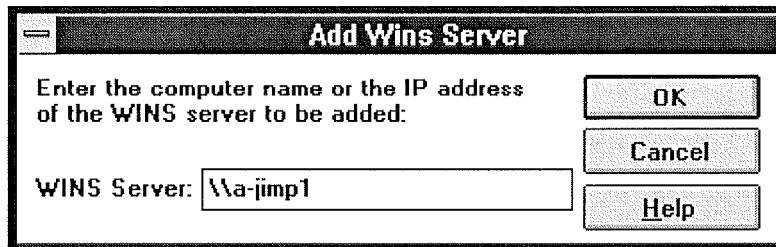
---

► **To connect to a WINS server for administration**

- In the WINS Manager window, select a server in the WINS Servers list. This list contains all WINS servers that you previously connected to or that have been reported by partners of this WINS server.

Or

1. If you want to select another server that you have not previously connected to, choose the Add WINS Server command from the Server menu.



2. In the WINS Server box of the Add WINS Server dialog box, type the IP address or computer name of the WINS server you want to work with, and then choose the OK button. (You do not have to include double backslashes before the name. WINS Manager will add these for you.)

The title bar in the WINS Manager window shows the IP address or computer name for the currently selected server, depending on whether you used the address or name to connect to the server. WINS Manager also shows some basic statistics for the selected server, as described in the following table. Additional statistics can be displayed by choosing the Detailed Information command from the Server menu.

**Statistics in WINS Manager**

<b>Statistic</b>	<b>Meaning</b>
Database Initialized	The time when this WINS database was initialized.
Statistics Cleared	The time when statistics for the WINS server were last cleared with the Clear Statistics command from the View menu.
Last Replication Times	The times at which the WINS database was last replicated.
Periodic	The last time the WINS database was replicated based on the replication interval specified in the Preferences dialog box.
Admin Trigger	The last time the WINS database was replicated because the administrator chose the Replicate Now button in the Replication Partners dialog box.
Net Update	The last time the WINS database was replicated as a result of a network request, which is a push notification message that requests propagation.
Total Queries Received	The number of <i>name query request</i> messages received by this WINS server. Successful indicates how many names were successfully matched in the database, and Failed indicates how many names this WINS server could not resolve.

Total Releases	The number of messages received that indicate a NetBIOS application has shut itself down. Successful indicates how many names were successfully released, and Failed indicates how many names this WINS server could not release.
Total Registrations	The number of messages received that indicate name registrations for clients.

► **To refresh the statistical display in WINS Manager**

- From the View menu, choose the Refresh Statistics command, or press F5.

Or

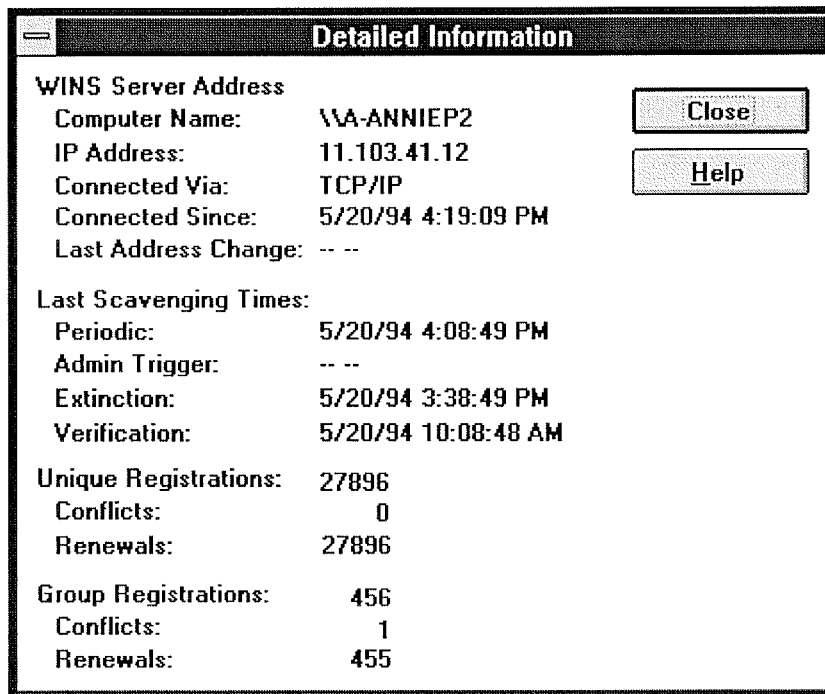
From the View menu, choose the Clear Statistics command to reset all statistical counters.

Or

Use automatic screen refreshing, based on the interval you specify in the Preferences dialog box, as described in "Setting Preferences for WINS Manager" later in this chapter.

► **To see information about the current WINS server**

1. From the Server menu, choose the Detailed Information command.



The Detailed Information dialog box shows information about the selected WINS server, as described in the table below.

2. To dismiss the Detail Information dialog box, choose the Close button.

**Detailed Information Statistics for WINS Manager**

Statistic	Meaning
Last Address Change	Indicates the time at which the last WINS database change was replicated.
Last Scavenging Times	The last times that the database was cleaned for specific types

Last Scavenging Times	The last times that the database was cleaned for specific types of entries. (For information about database scavenging, see "Managing the WINS Database" later in this chapter.
Periodic	Indicates when the database was cleaned based on the renewal interval specified in the WINS Server Configuration dialog box.
Admin Trigger	Indicates when the database was last cleaned because the administrator chose the Initiate Scavenging command.
Extinction	Indicates when the database was last cleaned based on the Extinction interval specified in the WINS Server Configuration dialog box.
Verification	Indicates when the database was last cleaned based on the Verify interval specified in the WINS Server Configuration dialog box.
Unique Registrations	The number of <i>name registration requests</i> that have been accepted by this WINS server.
Unique Conflicts	The number of conflicts encountered during registration of unique names owned by this WINS server.
Unique Renewals	The number of renewals received for unique names.
Group Registrations	The number of registration requests for groups that have been accepted by this WINS server. For information about groups, see "Managing Special Names" later in this chapter.
Group Conflicts	The number of conflicts encountered during registration of group names.
Group Renewals	The number of renewals received for group names.

For descriptions of the related intervals, see "Configuring WINS Servers" later in this chapter.

---

## Configuring WINS Servers and Replication Partners

You will want to configure multiple WINS servers to increase the availability and balance the load among servers. Each WINS server must be configured with at least one other WINS server as its replication partner.

Configuring a WINS server includes specifying information about when database entries are replicated between partners. A *pull partner* is a WINS server that pulls in replicas of database entries from its partner by requesting and then accepting replicas. A *push partner* is a WINS server that sends update notification messages to its partner when its WINS database has changed. When its partner responds to the notification with a replication request, the push partner sends a copy of its current WINS database to the partner.

For information about configuring preferences, see "Setting Preferences for WINS Manager" later in this chapter.



## Configuring WINS Servers and Replication Partners

### Configuring WINS Servers

For each WINS server, you must configure threshold intervals for triggering database replication, based on a specific time, a time period, or a certain number of new records. If you designate a specific time for replication, this occurs one time only. If a time period is specified, replication is repeated at that interval.

► **To configure a WINS server**

1. From the Server menu, choose the Configuration command.

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

2. To view all the options in this dialog box, choose the Advanced button.

3. For the configuration options in the WINS Server Configuration dialog box, specify time intervals using the spin buttons, as described in the following list.

Configuration option	Meaning
Renewal Interval	Specifies how often a client reregisters its name. The default is five hours.

Extinction Interval	Specifies the interval between when an entry is marked as <i>released</i> and when it is marked as <i>extinct</i> . The default is four times the renewal interval.
Extinction Timeout	Specifies the interval between when an entry is marked <i>extinct</i> and when the entry is finally scavenged from the database. The default is the same as the renewal interval.
Verify Interval	Specifies the interval after which the WINS server must verify that old names it does not own are still active. The default is 20 times the extinction interval.

The replication interval for this WINS server's pull partner is defined in the Preferences dialog box, as described in "Setting Preferences for WINS Manager" later in this chapter.

4. If you want this WINS server to pull replicas of new WINS database entries from its partners when the system is initialized or when a replication-related parameter changes, check Initial Replication in the Pull Parameters options, and then type a value for Retry Count.

The retry count is the number of times the server should attempt to connect (in case of failure) with a partner for pulling replicas. Retries are attempted at the replication interval specified in the Preferences dialog box. If all retries are unsuccessful, WINS waits for a period before starting replication again. For information about setting the start time and replication interval for pull and push partners, see "Setting Preferences for WINS Manager" later in this chapter.

5. To inform partners of the database status when the system is initialized, check Initial Replication in the Push Parameters group. To inform partners of the database status when an address changes in a mapping record, check Replicate On Address Change.
6. Set any Advanced WINS Server Configuration options, as described in the following table.
7. When you have completed all changes in the WINS Server Configuration dialog box, choose the OK button.

#### Advanced WINS Server Configuration Options

Configuration option	Meaning
Logging Enabled	Specifies whether logging of database changes to JET.LOG should be turned on.
Log Detailed Events	Specifies whether logging events is verbose. (This requires considerable system resources and should be turned off if you are tuning for performance.)
Replicate Only With Partners	Specifies that replication will be done only with WINS pull or push partners. If this option is not checked, an administrator can ask a WINS server to pull or push from or to a non-listed WINS server partner. By default, this option is checked.
Backup On Termination	Specifies that the database will be backed up automatically when WINS Manager is closed.
Migrate On/Off	Specifies that static unique and multihomed records in the database are treated as dynamic when they conflict with a new registration or replica. This means that if they are no longer valid, they will be overwritten by the new registration or replica. Check this option if you are upgrading non-Windows NT systems to Windows NT. By default, this option is not checked.
Starting Version Count	Specifies the highest version ID number for the database. Usually, you will not need to change this value unless the database becomes corrupted and needs to start fresh. In such a case, set this value to a number higher than appears as the version number

this value to a number higher than appears as the version number counter for this WINS server on all the remote partners that earlier replicated the local WINS server's records. This value can be seen in the View Database dialog box in WINS Manager.

Database Backup Path

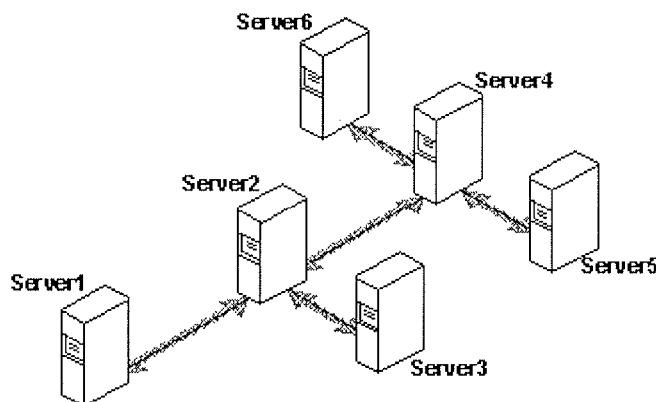
Specifies the directory where the WINS database backups will be stored. WINS uses this directory to perform an automatic restoration of the database in the event that the database is found to be corrupted when WINS is started. Do not specify a network directory.

## 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.

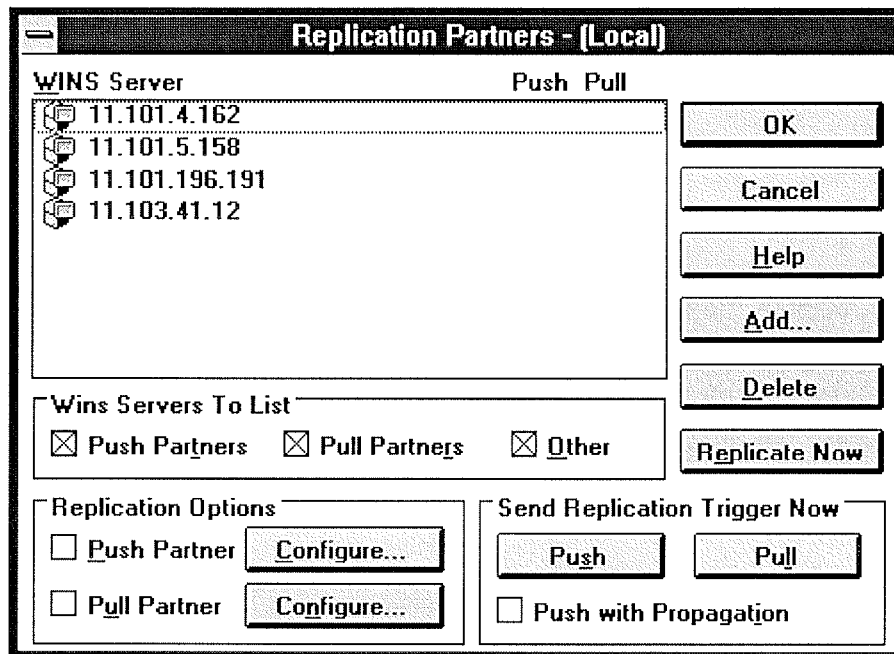
- If Server2, for example, needs to perform pull replications with ServerB, make sure it is a push partner of Server3.
- If Server2 needs to push replications to Server3, it should be a pull partner of WINS ServerB.

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.

The screenshot shows a dialog box titled "Pull Partner Properties". It contains the following elements:

- Pull Partner:** 11.103.41.12
- Start Time:** 11:30
- Replication Interval (h:m:s):** 3 : 00 : 00
- Buttons:** OK, Cancel, Help, and Set Default Values.

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.

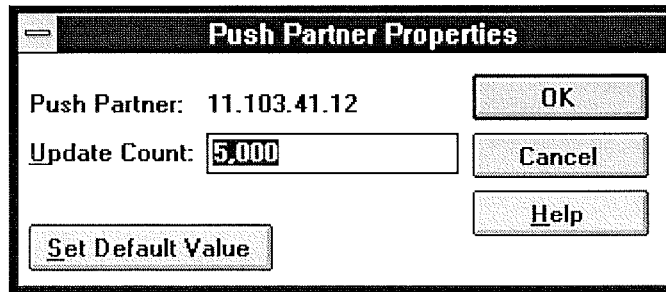
If you want to return to the values specified in the Preferences dialog box, choose the Set Default Values button.

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

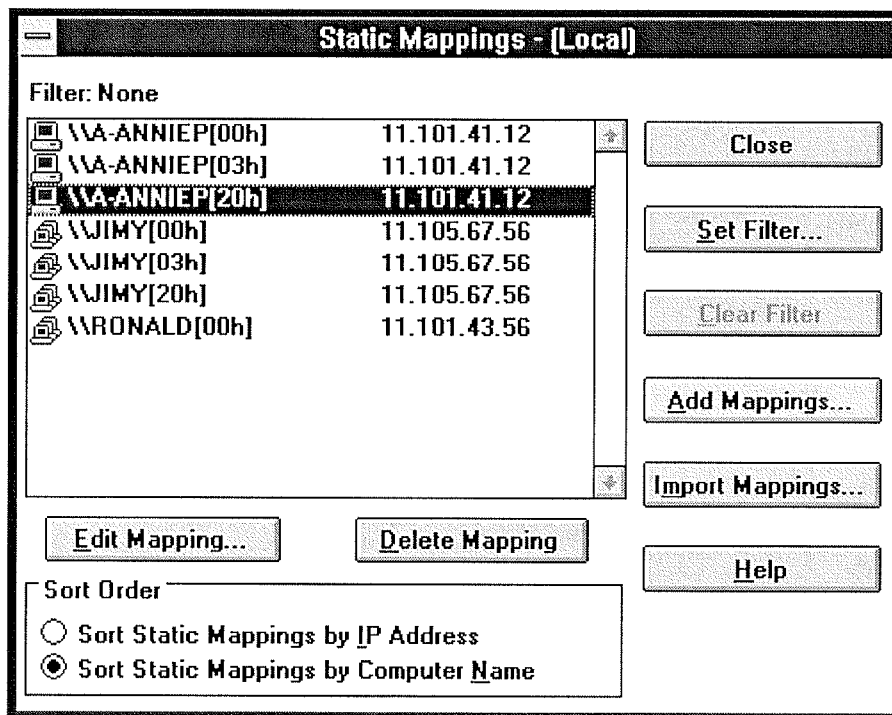
Static mappings are permanent lists of computer name-to-IP address mappings that cannot be challenged or removed, except when the administrator removes the specific mapping. You use the Static Mappings command in WINS Manager to add, edit, import, or delete static mappings for clients on the network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

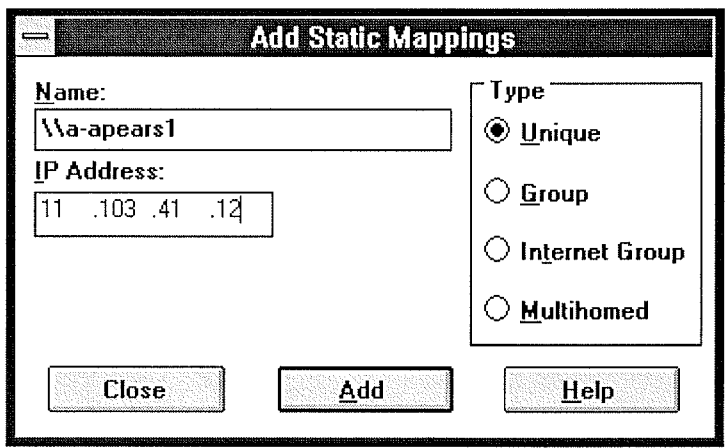
### Adding Static Mappings

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

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.

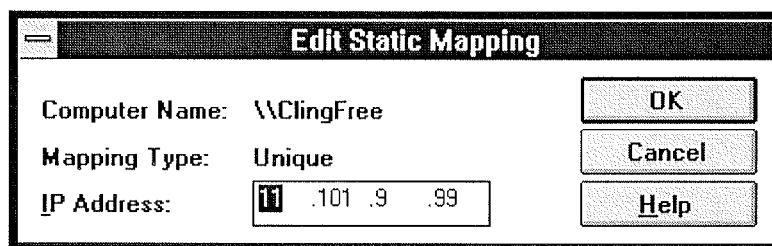
# Managing Static Mappings

## 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

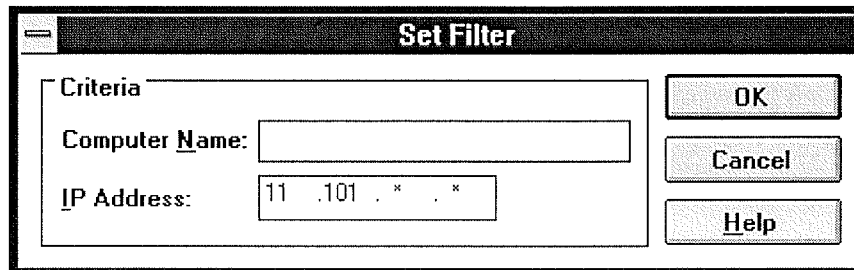
### Filtering the Range of Mappings

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 **nbstat -n** at the command prompt. This table shows the 16th byte for special names, plus the type (unique or group).

Name		Type	Status
<0C29870B>		UNIQUE	Registered
ANNIEP5	<20>	UNIQUE	Registered
ANNIEP5	<00>	UNIQUE	Registered

ANNIEPDOM	<00>	GROUP	Registered
ANNIEPDOM	<1C>	GROUP	Registered
ANNIEPDOM	<1B>	UNIQUE	Registered
ANNIEP5	<03>	UNIQUE	Registered
ANNIEP5	<1E>	GROUP	Registered
ANNIEP5	<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 <i>released</i>
Owned released name for which the Extinct interval has expired	Marked <i>extinct</i>
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.

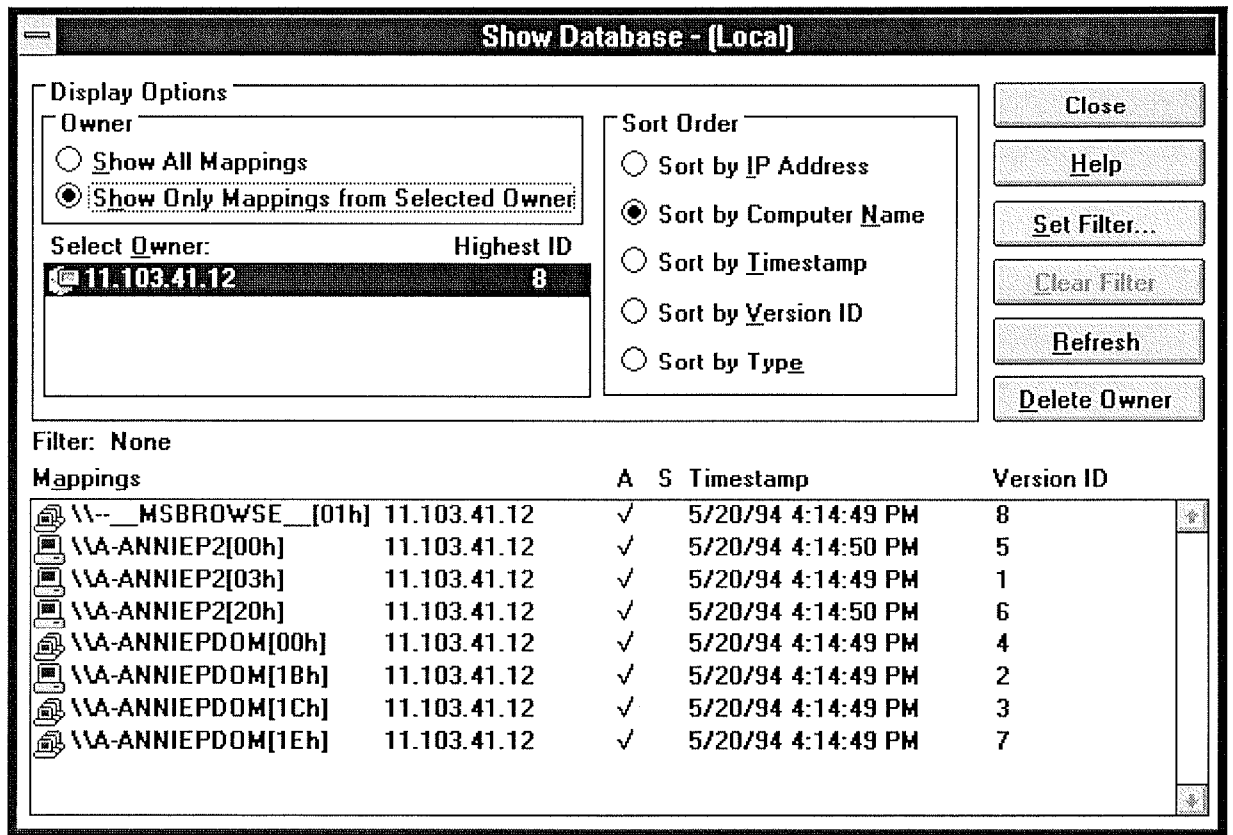
# Managing the WINS Database

## 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.

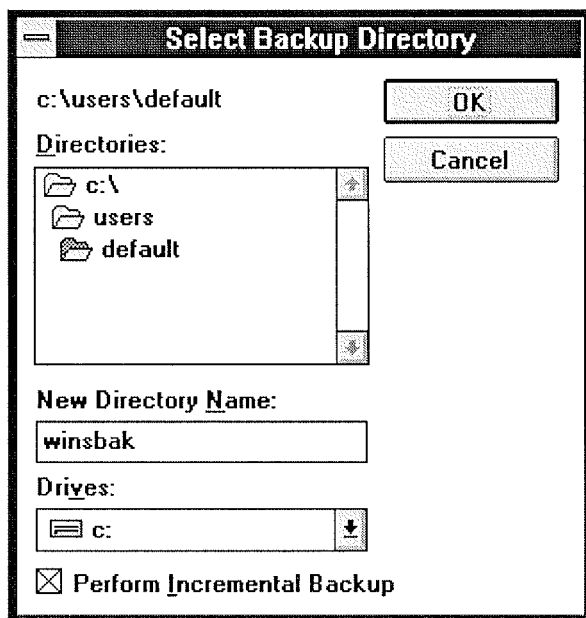
# Managing the WINS Database

## 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 troubleshooting 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 become 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.

---

## 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\

**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.

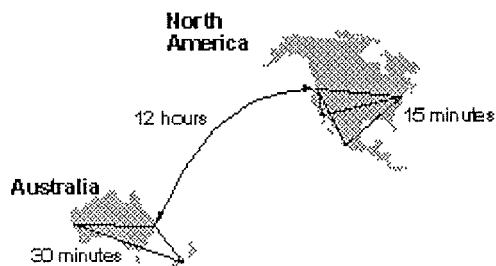
## Planning a Strategy for WINS Servers

### 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.
\0xnn	Support for nonprinting characters in NetBIOS names. Enclose the NetBIOS name in double quotation marks and use \0xnn



the NetBIOS name in double quotation marks and use `\0xnn` 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.

### 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

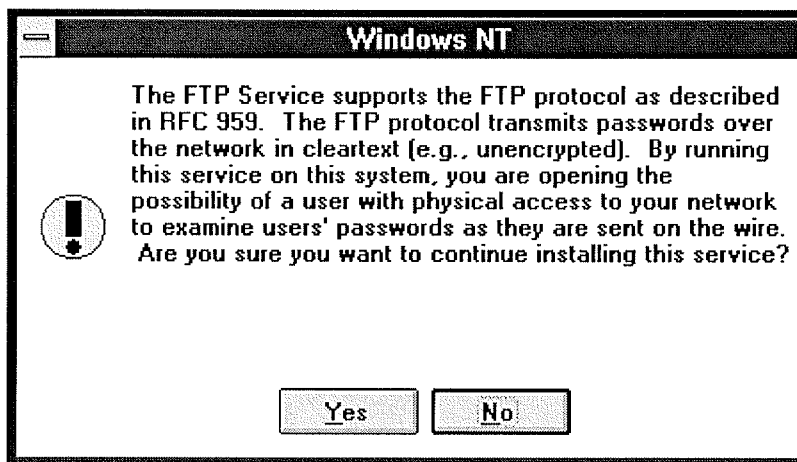
These procedures assume that you have installed any necessary devices and device drivers.



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.

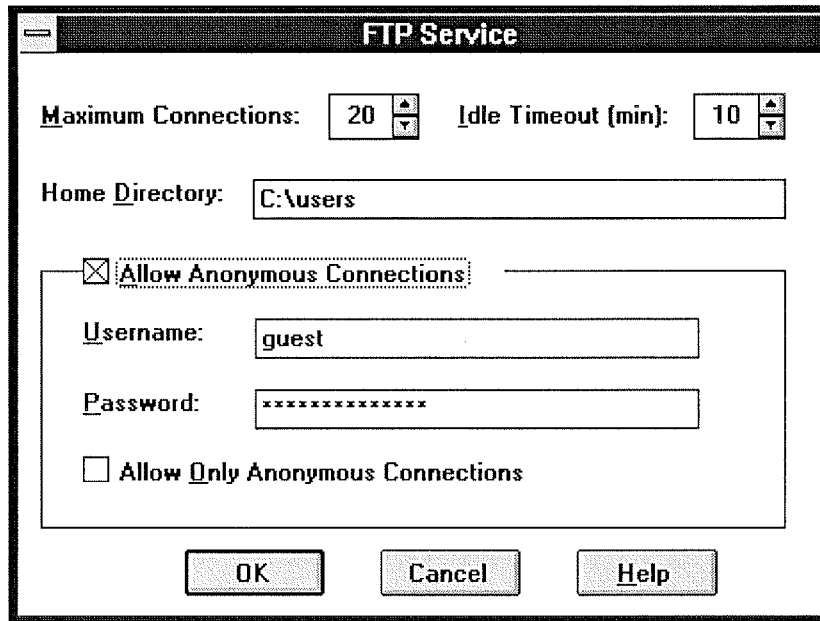
If anonymous connections are allowed, you must supply the Windows NT username and password to be used for anonymous FTP. When an anonymous FTP transfer takes place, Windows NT will check the username assigned in this dialog box to determine whether access is allowed to the files.

### ► 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 <b>anonymous</b> (or <b>ftp</b> , which is a synonym for <b>anonymous</b> ). 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 <b>anonymous</b> with the FTP Server. The <b>anonymous</b> user name is reserved in the FTP Server for the anonymous logon function. Users logging on with the username <b>anonymous</b> 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 <b>anonymous</b> . 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 <b>anonymous</b> 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.

---

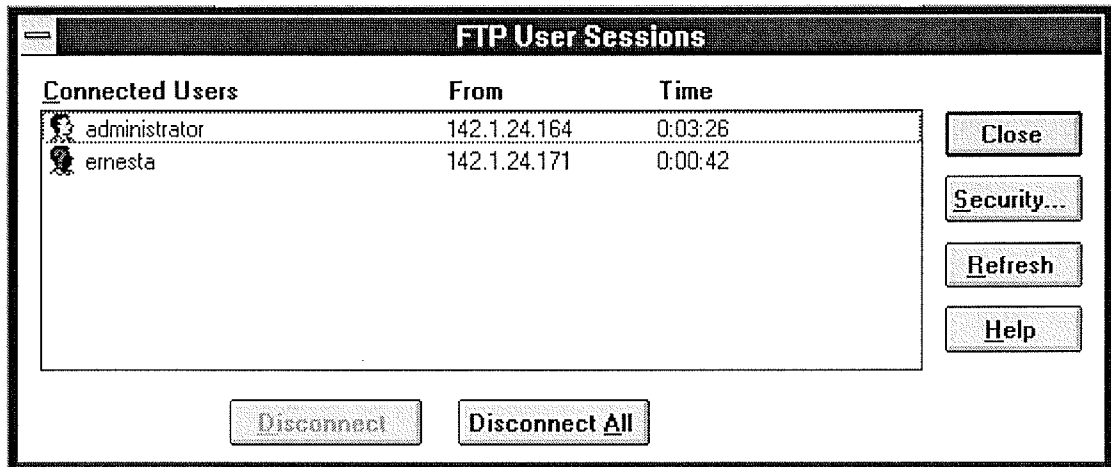
**Note**

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.

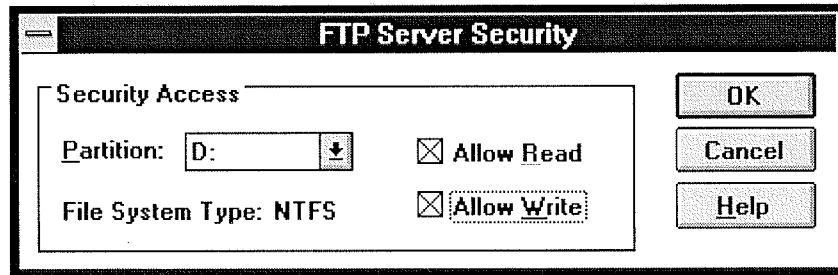
---

► **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



FTP Server

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\tst.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 1  
Default = 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."

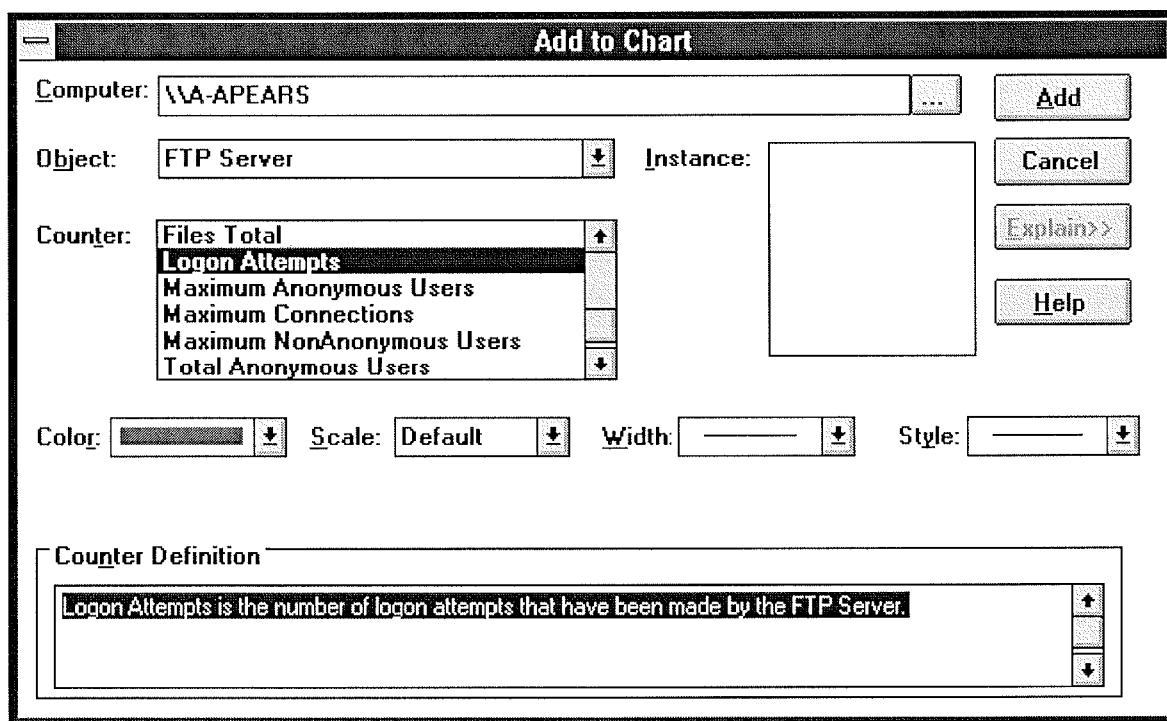
---

## 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



	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