Using LMHOSTS with Dynamic Name Resolution

Specifying Remote ~~Servers~~Sewers 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 ~~astrict~~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~~SewerB 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 ~~aworkstation~~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. ~~Ifthis~~lf this fails, the LMHOSTS file is used. ~~If~~lf 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~~LIVIHOSTS file can represent Windows NT Workstation computers, Windows NT Server computers, ~~lAN~~LAN Manager servers, or ~~Windows~~\Mndows for Workgroups 3.11 computers running Microsoft TCP/IP. There is no need to distinguish between different ~~platforms~~ptatforms 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~~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~~. Ifyou~~ lf 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~~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~~tne #PRE
keyword. Use nbtstat to remove or correct preloaded entries that may have been
mistyped or
any names cached by successful broadcast resolution~~.~~,
Setting Up LNIHOSTS 6of8
102.54.94.91 accounting
102.54.94.94 payroll
102.54.94.97 stockquote
102.54.94. 102 printqueue
#accounting server
#payroll server
#PRE #stock quote server
#print server in Bldg 10

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~~PDCS) and
backup domain
controllers (~~BDCs~~BDCS) maintain the user account security database and manage
other
network-related services. Because large Windows NT domains can span multiple
~~IP~~lP 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, ~~acolon~~a colon, and the domain in which the
domain controller
participates. For example:

102.54.94.97 treydc #DOM:treycorp #~~The treycorp~~Thetreycorp PDC

Using the #DOM keyword to designate domain controllers adds entries to a special ~~internet~~infernef group name cache that is used to limit internetwork distribution of requests intended for the local domain controller. When domain controller activity such as ~~alogon~~a logon request occurs, the request is sent on the special internet group name. ~~In~~ln 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~~fonivard 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 ~~aWindows~~a Windows NT computer that is ~~amember~~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.

l 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 ~~abackup~~a backup to primary domain controller status does not affect the ability to offer all services to members of the domain.

~~Iftrust~~l 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~~LMHQSTS files should contain at least the name and IP address mapping for ~~the~~tile 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, ~~asingle~~a singie common LMHOSTS
Setting up LN|HosTs 7of8

file usually satisfies ~~all~~al! 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.
~~Chapter 6 Setting Up LMHOSTS~~
Names that appear with #~~DOMin~~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<IC~~DOMAlN<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~~Controllers
whose names are entered in LMHOSTS files should have their ~~IP~~lP addresses reserved as static
addresses in the DHCP database rather than running as DHCP clients.
Also, all Windows NT Advanced ~~Server~~Sewer 3.1 computers in a domain and its trusted domains ~~should~~
shouid 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 \~~s'ystemroot~~sysfemroof
\SYSTEM32\~~DRIVERS~~DRlVERS\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~~sen/ice to distribute multiple copies of the global ~~file~~flle(s) to multiple servers for reliable access.

To provide a redundant list of servers maintaining copies of the same LMHOSTS file, use the #~~BEGIN~~BEGlN_ALTERNATE and #END_ALTERNATE keywords. This is known as a block inclusion, which allows multiple servers to be searched for a valid copy of ~~aspecific~~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): ~~c;\PR1v/-\TE directory):

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

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

~~#BEGIN_ALTERNATE~~

```
#BEGINALTERNATE
#INCLUDE \\treydc\public\lmhosts #source for global file
#INCLUDE \\treybdc\public\lmhosts #backup source
#INCLUDE \\~~localsvr\public~~localsv1.\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~~ LMHCDSTS 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 ~~alocal~~ a local LMHOSTS file located in the C:\~~PRIVATE~~PRlVATE 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. ~~Ifno~~lf 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.

~~CHAPTER 7~~
, Setting Up LNIHOSTS 8of8
102.54.94.97 treydc #PRE #DOM:treycorp
102.54.94.99 treybdc #PRE #DOM:treycorp
102.54.94.98 localsvr #PRE #DOM:treycorp
#primary DC
#backup DC in domain
#INCLUDE c:\private\lmhostS #include a local lmhosts

~~Using~~Usmg the ~~Microsoft~~Mlcrosoft FTP Server ~~Service~~
Servlce
The Microsoft ~~FfP~~FTP Server service allows other computers using the ~~FfP~~FTP
utility to connect to
this computer and transfer files. The ~~FfP~~FTP Server service supports ~~all~~ell
Windows NT ftp client
commands. Non-Microsoft versions of ~~FfP~~FTP clients may contain commands that
are not
supported. The ~~FfP~~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 ~~FfP~~FTP Server service is integrated with the Windows NT security model.
Users connecting to
the ~~FfP~~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 ~~FfP~~FTP
Server service be installed on an NTFS partition so that the ~~fLies~~files and
directories made available
via ~~FfP~~FTP can be secured.
~~Caution~~CauUon
The ~~FfP~~FTP Server protocol relies on the ability to pass user passwords over
the network without
data encryption. ~~Auser~~A user with physical access to the network could examine
user passwords
during the ~~FfP~~FTP validation process.
The following topics are included in this chapter:
~~•~~' Installing the ~~FfP~~FTP Server service
~~•~~l Configuring the ~~FfP~~FTP Server service
~~•~~l Administering the ~~FfP~~FTP Server service
~~•~~' Advanced configuration parameters for ~~FfP~~FTP Server ~~service~~ser\/ice
For information about using performance counters to monitor ~~FfP~~FTP Server
traffic, see
Chapter 8, "Using Performance Monitor with ~~TCPIIP~~TCP/IP Services."
~~Installing the FTP Server Service~~
. Chapter 7 1of12

_'les H4
®
||Ili|||||i lillilli
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 ~~FfP~~FTP Server ~~service~~sen/ice.
~~.,_~~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 ~~TCPIIP~~TCP/IP Protocol And Related Components, and then
choose the Continue button. When the Windows NT TCP~~I~~/IP Installation Options dialog box
appears, check the ~~FfP~~FTP Server Service option, and then choose the OK button.
4. When the message prompts you to ~~confmn~~confirm that you are familiar with ~~FfP~~FTP security, choose
the Yes button to continue with ~~FfP~~FTP Server service installation.

~~- WindowsNT~~
The ~~File T 1 ansfe1 P10tocol 1elies on the ability to pass use1~~ FTP Service supports the FTP protocol as described
~~passw01ds ove1 the netwmk without data enayption. A~~
in HFC 353. The FTP protocol transmits passwords over
the network in cleartext [e.g., unencryptedl. By running
this service on this system, you are opening the
~~use1~~possibility of a user with physical access to ~~the netw01k may be able~~ your network
to examine ~~usen' passwmds dwing FTP validation. A1e~~users' passwords as they are sent on the wire.
Are you~~(])~~ ~~sule~~sure you want to continue installing this service?
5. ~~When~~Wnen prompted for the ~~full~~ful! 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 ~~compute r~~computer, the ~~FfP~~FTP Service dialog box appears
so that you can continue with the configuration procedure as described in the next section.
The ~~FfP~~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 ~~FfP~~FTP Server tool in ~~the~~tne Control Panel as described in
the following section.
~~Chapter 7~~ Using the Microsoft FTP Server Service
Installing the FTP Server Service
2of12

~~Configuring~~After the FTP ~~Server Service After the FfP Server service~~Sewer sen/ice software is installed on your computer, you must configure it to operate. When you configure the ~~FfP~~FTP Server service, your settings result in one of the
following:
~~1~~' No anonymous ~~FfP~~FTP connection allowed. In this case, each user must provide a valid

Windows NT ~~usemame~~username and password. To configure the ~~FfP~~FTP Server
service for this, make
sure the Allow Anonymous Connection box is cleared in the ~~FfP~~FTP Service dialog
box.
~~1~~l Allow both anonymous and Windows NT users to connect. ~~In~~ln this case, ~~ausera~~a
user can choose
to use either an anonymous connection or ~~aWindows~~a Windows NT ~~usemame~~username
and password. To
configure the ~~FfP~~FTP Server service for this, make sure only the Allow
Anonymous
Connection box is checked in the ~~FfP~~FTP Service dialog box.
~~1~~l Allow only anonymous ~~FfP~~FTP connections. In this case, a user cannot connect
using a
Windows NT ~~usemame~~username and password. To configure the ~~FfP~~FTP Server
service for this, make
sure both the Allow Anonymous Connections and the Allow Anonymous Connections
Only
boxes are checked in the ~~FfP Service~~FTP Sen/ice dialog box.
If anonymous connections are allowed, you must supply the Windows NT
~~usemame~~username and
password to be used for anonymous ~~FfP~~FTP. When an anonymous ~~FfP~~FTP transfer
takes place,
Windows NT will check the ~~usemame~~username assigned in this dialog box to
determine whether access
is allowed to the files.
~~. . , .~~To configure or reconfigure the ~~FfP Server~~FTP Sewer service
1. The FTP Service dialog box appears automatically after the FTP Server
service software is
installed on your computer.
~~-~~Or~~ If~~
lf you are ~~reconfiguring~~reoonfiguring the FTP Server service, choose the
Network option in Control
Panel. In the ~~Installed~~lnstalied Network Software box, select FTP
~~Server~~Sen/er, and then choose the
Configure button.

Using the Microsoft FTP Server Service
Configuring the FTP Sewer Service
3of12

20 1U
C:"\users
~~Maximum Connections: -!die Timeout (min): -~~ guest
Home ~~.Qirector.11: '-lc_:_us_er_s____________J~~ Qireclury:
~~!!.sername: "'lg_ue_st__________'~~
~~fassword: I●●●●●●●● ●●● ●●●~~
nnnu nnnnnnnununnnnn n nu n un nn nu
'
lT! lln u n n u n
Username:
Password:
~~DAllow .Qnl.l' AnonJimous~~Allow Qnly Anonymous Connections
~~IBBIJ~~
The FTP Service dialog box displays the following options:

Item
Maximum Connections
Idle Timeout
Description

Specifies the maximum number of ~~FfP~~FTP users who can connect to the system simultaneously. The default value is ~~20;~~20, the maximum is 50. ~~Avalue~~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 ~~FfP~~FTP server, any subsequent attempts to connect ~~will~~wilt receive messages defined by the administrator~~.~~, For information about defining custom messages, see "Advanced Configuration Parameters for ~~FfP~~FTP Server Service" later in this chapter.

Specifies how many minutes an inactive user can remain connected to the ~~FfP~~FTP Server service. The default value is 10 minutes; the maximum is 60 minutes. ~~Ifthe~~lf the value is ~~0,~~0. users are never automatically disconnected.

Maximum Connections: idle Timeout (min):

~~Chapter 7 Using the Microsoft FTP Server Service~~
~~Item Description~~

Home Directory
Allow Anonymous
Connections
Username
Password
Allow Only Anonymous
Connections

Specifies the initial directory for users.

~~Allow Anonymous~~ Enables users to connect to the ~~FfP~~FTP Server using the user
~~Connections~~ name
anonymous (or ftp, which is ~~asynonym~~a synonym for anonymous). ~~Apassword~~A password is not necessary, but the user ~~will~~Will be prompted to supply a mail address as the password. By default, anonymous connections are not allowed. Notice that you cannot use a Windows NT user account with the name anonymous with the ~~FfP~~ FTP Server. The anonymous user name is reserved in the ~~FfP~~FTP Server for the anonymous logon function. Users ~~logging~~iogging on with the username anonymous receive permissions based on the ~~FfP~~FTP Server configuration for anonymous Iogons.

~~Username~~ Specifies which local user account to use for ~~FfP~~FTP Server users who log on under anonymous. Access permissions for the anonymous ~~FfP~~FTP user will be the same as the specified local user account. The default is the standard Guest system account. ~~If~~lf 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~~ Allows only the user name anonymous to be accepted.
~~Connections~~ This
option is useful if you do not want users to log on using their own user names and passwords because ~~FfP~~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 ~~FfP~~FTP Service dialog box and return
to the Network
Settings dialog box.
4.   To complete initial ~~FfP~~FTP Server service installation and
configuration, choose the OK
button.
~~Amessage~~A message reminds you that you must restart the computer so that the
changes you made
will take effect.
Note

ag!m1nlstr.atur.. ...1.8.2.:.1..-.8fE:.3..§4...
ernesta 142.1 24.1 ?1 U:UU: 42
Close
§..¢cui.:t_u
Refresh
Hyip
Qffw 34. 4.? 4 Disconnect All
When you first install the ~~FfP~~FTP Server service, you must also complete the
security ~~configuration~~
confi uration as described in ~~the following procedure~~tue foliowin rocedure
for users to access g p volumes on ~~your~~our
computer.
~~11J!> ~~To configure ~~FfP~~FTP Server security
1.   After the ~~FfP~~FTP Server has been installed and you have restarted Control
Panel, start the ~~FfP~~
FTP Server option in Control Panel. Windows NT Server users can also use the
~~FfP~~FTP menu
in Server Manager.
~~zJ   FTP User Sessions~~
1| | \
~~.!;_onnecled~~Connected Users From Time
~~............................ J.4.?J. .?.-.1..-.4...... Q:Q- ?§ ....~~
~~142.1.24.171 000:42~~
~~11111\1~~
~~P-RiJ~~
~~I E!t''V\ltft~~
=.niii';i=i"i"'W. *=i=i""
2.   In the ~~FfP~~FTP User Sessions dialog box, choose the Security button.
1'1"

... ¢ nn ml
~~·   FTP Server Security ~~Security ccass
~~Securil.l' Access   ,~~
~~P.artition: jo: II [gl Allow Read~~
Eartitiun: F3 afkllnw _l3_ead
File ~~S.Pslem T.11pe: NTFS [gl :-.li.ti.·-:.·-;_i-- 1 ~~System Type: HTF3 8
~~Chapter 7 Using the Microsoft FTP Server Service~~
D
I

~~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 ~~fmished~~finished setting security access on partitions.
The changes take effect immediately. The FTP ~~Server~~Sen/er service is now ready to operate.
J

~~Administering the~~ FTP Server ~~Service~~
After initial installation ~~is~~ss complete, the FTP Server service is automatically started ~~FTP Server in~~ln the
background each time the computer is started. Remote computers can initiate ~~-~~an ~~FfP~~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 ~~amember~~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~~Sen/er service is configured to allow anonymous ~~logons~~Iogons.
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 ~~FfP~~FTP Server ~~service~~sen/ice
~~•~~ ° Use the Services option in Control Panel, or at the ~~command~~commend 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."

Using the Microsoft FTP Server Sewice
Administering the FTP Server Service
4of12

Administering the FTP Sewer Service

Using FTP Commands at the Command Prompt

When you install the FTP service, ~~aset~~a set of ftp commands are automatically ~~installed~~Installed that you can use at the command prompt. For ~~asummary~~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.~~

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.

Using the Microsoft FTP Server Service 50f12

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~~Sen/er computers, the same dialog box can be reached from ~~Server~~Sen/er Manager by choosing the FTP menu command.

~~In~~ln 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. ~~Ifthe~~lf the user name contained a mail host name (for example, ernesta@trey-research.com) only the username (~~ernesta~~emesta) 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.

~~Chapter 7 Using the Microsoft FTP Server Service~~

The ~~FfP~~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 ~~FfP~~FTP Service Security dialog box, where you can set Read and Write permissions for each partition on the ~~FfP~~FTP Server, as described earlier in this chapter. You must set the permissions for each partition you want ~~FfP~~FTP users to have access to. ~~Ifyou~~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 ~~FfP Server~~FTP Sewer partition security, if a user logs on using a Windows NT account, access permissions for that account are in effect.

. Using the Microsoft FTP Server Service 6of12

Administering the FTP Sewer Service

Controlling the FTP Server and User Access

~~Anetwork~~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 ~~avalue~~a value between 0 and 50. Any value from 1 to 50 restricts concurrent FTP sessions to the value specified. ~~Avalue~~A value of 0 allows unlimited connections to be established to the ~~FfP~~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~~iater in this chapter.

Using the Microsoft FTP Server Service 7of12

Administering the FTP Server Service

Annotating Directories

You can add directory descriptions to inform ~~FfP~~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~~Sen/er Service" later in this chapter.
. Using the Microsoft FTP Sewer Service 8of12

Administering the FTP Server Service
Changing Directory Listing Format
Some ~~FfP~~FTP client software makes assumptions based on the formatting of
directory list
information. The Windows NT ~~FfP~~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-~~DOS style~~DOSstyle (the default)
and UNIX-style listings. On
most ~~FfP~~FTP client implementations (including the Windows NT ~~FfP~~FTP client),
users type ~~acommand~~a
command at the command prompt similar to quote site dirstyle to get this
effect.
You can set the ~~default~~defautt style for directory ~~listing~~iisting format by
setting ~~avalue~~a value for MsDosDirOutput
in the Registry, as described in "Advanced Configuration Parameters for ~~FfP~~FTP
Server Service"
later in this chapter.
Using the Microsoft FTP Sewer Service 9of12

Administering the FTP Sewer Service
Customizing Greeting and Exit Messages
You can create customized greeting and exit messages by setting values for
GreetingMessage and ~~ExitMessage~~ExitNlessage in the Registry, as described in
"Advanced Configuration
Parameters for ~~FfP~~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 ~~FfP~~FTP

Server. When you create custom messages, you can add multiline messages of
your choice.
Using the Microsoft FTP Server Service 10 Of12

Administering the FTP Sewer Service
Logging FTP Connections
You can log incoming ~~FfP~~FTP connections in the System event log by setting
values for
LogAnonymous and LogNonAnonymous in the Registry, as described in "Advanced
Configuration Parameters for ~~FfP~~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~~tog entries are made for both anonymous and
nonanonymous
users connecting to the ~~FfP~~FTP Server. You can view such entries in the System
event log by
using Event Viewer.
~~Chapter 7~~. Using the Microsoft FTP ~~Server~~Sewer Service 11 of12

Advanced Configuration Parameters for
FTP ~~Server Service~~ Sewer Sen/ice
This section presents configuration parameters that affect the behavior of
the ~~FfP~~FTP Server
service and that can be modified only through Registry Editor. After you modify
any of these
value entries, you must restart the ~~FfP~~FTP Server ~~service~~sen/ice 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 ~~FfP~~FTP Server service configuration using
Registry Editor
1. Run ~~REGEDT32.EXE~~REGEDTSZEXE 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~~F1 to get Help on
how to make
changes in Registry Editor.
2. In Registry Editor, click the window titled HKEY__LOCAL_~~MACHINE~~MACH1NE
On Local Machine,
and then ~~click~~Click the icons for the SYSTEM subtree until you reach this
subkey:
.. \SYSTEM\~~CurrentControlSet~~CurrentContro1
Set\Services\~~ftpsvc\Parameters~~ftp svc\Paramete1's
All of the parameters described here are located under this Registry subkey.

The following describes the value entries for ~~FfP~~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~~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 ~~FfP~~FTP users of the contents of a directory on the server. The directory description is saved in a file named ~~-FfPSVC-~~ ~FTPSVC~.CKM, which is usually a hidden file. When this value is 1, directory annotation is on.

~~ExitMessage~~ Exitlvlessage

Data type = REG_~~sz~~SZ

Range = String

Default = "Goodbye."

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

~~GreetingMessage~~

GreetingNlessage

Using the Microsoft FTP Sewer Service 12 of12

Data type = REG_~~MULTI~~MULT|_ 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~~( ),~~ 0, this greeting message is not sent.

LogAnonymous

Data type = REG_DWORD

Range = ~~0or~~0 or 1

Default = 0 (false-that is, do not log successful anonymous logons)

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

LogNonAnonymous

Data type = REG_DWORD

Range =~~0or~~ 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.

~~Chapter 7 Using the Microsoft FTP Server Service~~

LogFileAccess

Data type = REG__DWORD

Range = 0 or 1
Default = 0 (do not log file accesses to ~~FfPSVC.LOG~~FTPSVOLOG)
If this value is non-zero, all file accesses are logged to ~~the~~tne file
~~FfPSVC.LOG~~FTPSVGLOG in the ~~service~~
servioe's current directory (typically \~~systemroot~~<:ysfemroof\SYSTEM32).
For each file opened by the ~~FfP~~
FTP Server, ~~FfPSVC.LOG~~FTPSVOLOG will contain a single line entry in the
following format:
~~IPAddress~~lPAddress username action path ~~date_time~~dafe_fime
~~•~~
'_ip_address is the client computer's IP address
~~•~~l username is the user's name (or password for anonymous ~~logons~~Iogons)
~~•~~' action is either "opened," "created," or "appended"
~~•~~l path is the fully qualified path of the file acted upon

~~•~~
~~date~~'_dafe_time is the date and time the action took place
Entries are also written to the log whenever the ~~FfP~~FTP Server starts or stops.
For example:
~~*~~>l<************* FTP SERVER SERVICE STARTING Fri Apr 29 10:28:49 1994
~~11.101.199.173~~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~~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~~lf
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~~Hag has no ~~effect when~~effectwhen
retrieving listings on HPFS
or NTFS partitions.
~~MaxClientsMessage~~MaxClientsNlessage
Data type = REG_~~sz~~SZ
Range = String
Default ~~=~~: "Maximum clients reached~~, service~~. sen/ice unavailable."
This value entry specifies the message to be sent to an ~~FfP~~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 ~~FfP Service~~FTP Sewice dialog box or the
MaxConnections value in

the Registry).
MsdosDirOutput
Data type = REG_ _DWORD
Range = 0 or 1
Default = 1 (true-~~that~~tliat is, directory listings ~~will~~Will look like MS-DOS)
This value entry specifies the default behavior for whether the output of the list command ~~will~~
Will look like the output of the MS-DOS dir command or the output of the UNIX Is
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~~Will
contain backward slashes (\). ~~If~~lf 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 ~~FfP~~
FTP Server service in the Network Settings dialog box:
AllowAnonymous
AnonymousOnly
AnonymousUsername
ConnectionTimeout
HomeDirectory ~~MaxConnections~~
NlaxConnections
The following Registry parameters can be set using the options available when you select the ~~FfP~~
FTP Server icon in Control Panel and then choose the Security button:
~~ReadAccessMask~~ReadAccessNlask
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 ~~FfP~~
FTP Server service dialog boxes to set these values.
~~CHAPTER 8~~

Using Performance ~~Monitor~~Nlonitor with ~~TCP/IP~~
TCPIIP Services
wwf
l i
This chapter describes the ~~perfonnance~~performance counters that can be charted in ~~Perfonnance~~Performance Monitor
so you can track ~~perfonnance~~performance of the IP ~~protocols, FfP~~protocois, FTP Server service traffic, and ~~WINS~~ WiNS
servers.
The ~~perfonnance~~performance counters are described in the following topics in this chapter:
~~•~~" Using ~~Perfonnance~~Performance Monitor with TCP/IP
~~•~~' Monitoring TCP/IP ~~perfonnance~~performance

~~•~~
' Monitoring ~~FfP~~FTP Server service traffic

~~•~~' Monitoring WINS server ~~perfonnance~~performance
important
~~Important~~ To use the TCP/IP ~~perfonnance~~performance counters in
~~Perfonnance~~Performance Monitor, you must install the SNMP
service, as described in Chapter 2, "Installing and Configuring Microsoft
TCP/IP and SNMP."
Chapter 8 1of10

Qumputer:
Ugiect: instance:
Enunleri
Colug: § cale: idth S kyle
Euugter Definition
'M-APEAHS
FTP Server
u Flles Tutal
, ~ ~ ,
Haximum Anonymous Users
Maximum Connections
Maximum Nonhnonymous Users
Total Anonymous Users
Default
LéJt1nrf.8.ttem I || mattern 1- 1- - -~~¢ u....|' I. theFTPSe|'-wer
533
~~Using Performance Monitor with TCPnP~~ I*
After elements of Microsoft TCP~~!~~/IP are installed, you can use ~~Perfonnance~~
~~Mont-Gf~~Performance Monitor to track
performance.
~~._.~~ To use Performance Monitor with ~~TCP/IP~~TCPIIP
1.
2.
3.
4.
5.
6.
For
~~In~~ln the Administrative Tools group in Program Manager, double-click
~~Perfonnance~~Performance Monitor.

~~2.~~
From the Edit menu, choose Add To Chart.

~~. Add to Chart~~
~~hOIIIIJUler: I\\A APEAAS LJ Oi"i{i~~
~~O!!ject: IFTP Server !j !nstance:~~
~~1M~~

~~Counter: Files Total ..~~
~~IsM~~
~~-lril',: . ;,1~~

~~Maxillutl AIIOII,.nDUI Users MaxiiUII Connections r I M}l Ma. . NonA-Users~~
~~Total Anon9110US Usera -~~

~~Co-: J ij icale: JDelault [!J 't[idth:J --[iJ St1le: I --IJ~~
~~-I~~

~~3.~~
In the Computer list in the Add To Chart dialog box, select the computer you ~~want~~Want to
monitor.

~~4.~~
In the Object list, select the TCP/IP-related process you want to monitor: ~~FI'P~~FTP Server,
ICMP, IP, Network Interface, TCP, UDP, ~~or WINS~~orWlNS 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 tabies
~~defmition tables~~ later in this chapter.
~~6.~~ When you have selected all the counters you want for ~~aparticulara~~a particular chart~~. chou''~~, choose the Done
button.
~~For~~ more information about using Performance Monitor, see Chapter 19, ~~''Perfonnance Monitor," in the Windows NT Server~~"Performance
Using Performance Monitor with TCP/IP Services
Using Performance Monitor with TCP/IP
2of10

Monitor," in tlwe WndowsNT Sewer System Guide.

5:2
≥
~~Chapter 8~~ Using Performance Monitor with ~~TCP/IP Services~~TCPIIP Sewices s of10
Monitoring TCPIIP 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
Intedace, TCP, or UDP in the Object list.
The counters for each of these object types are described in the following sections.
:

. * 1
L1
Monitoring TCP/IP Performance

~~I xil til the dilferenl elements that make up the TCP/IP protocol suite L';Jil he~~

~~1lltillitored separ;ilclv in PerlornLJilCL' M(111i1or il SNMP scr\ ices arc ilhl;illcd on tile~~

~~, , 1111puter.~~

~~Ill l'o \iew cmmtcrs spt•l'itk to TCP/IP prorcsses~~

~~•   In tile ,\dd Tn ('hart di;ilo~ h()\ 111 Perlunnance :VInnitor. ..elect I(\W W \ict\\ork iltlni;Jcc. I CP. till 'I)!> in the Ohjcclli..,t.~~

~~Ihe L'Olllllers lor caL·il nltlic..,c nhiL'L'IIvpes ;1rc descr1hcd in the lollowin~ seL·tiulb.~~

~~I(1.1P Performance Counters~~ ICMP Performance Counters

~~l'he IUviP Ohjcel 1\ IlL' includes those Ulllltlcrs thalcberihc the rate" thallnlcmct ('unlrol Mcss;1ge ProtoL·ul (I('MP) mess<~~es arc received ami sent hy :1 cert;1i11 L'lllily u .ing the I('MP prui(IL'lli. II al .o desuihe.., v;1riou.., error L·ounls lor tile I(·r~..1P protocol.~~

~~ICMP prrformann counter \1ranin~ :~~

~~I he numhcr ol I('MP lllL'Ssa~cs Ihal this L'lllitv did Jltil ~,end hec:111Se ol pruhlc11h discovncd within I('MP. ' liCit as l:1ck ul hullL'IS. I his \:due ~,lwuld IHII include L'ITllrs discuvercd tlllisidc the ICiviP 1:1\ cr. such :1s the i11:1hilitv ol IP tu ruute the rL·stdtant dat:1~ram. In Sllllle implcmentatioiiS. there 111:1v he notvpes til error th:11 L'tlntrihute to this cuunter\ \:due.~~

~~The nunthL·r nl ICMP messa~cs that the entitv rL·ceived. hut determined as h:1vin~ eiT(Hs !lwll(M1> checksums. 1\HIIcn~th. ;1nd so on).~~

The ICMP Object Type includes tnose counters that describe the rates that Internet Control ~~The rate :11 \\hich ICtviP messages :tre received hy the~~ Message Protocol (ICMP) messages are received and sent by a certain entity using the ICMP ~~<'lltity. The r:1te includes those ntess:l_l!.L'S 1weived in error.~~

~~f"he LIIL' :tt \\ hich 1('\[P mess:1ges :II\' :IIIL'Illpted to be ·<nth\ !he entitv. l"hL' r:1te includes tht1se mess:1~es sent lllL'rror.~~

~~l"he total rate at \vhich IUvlP n1cs ..:1~es are recein·d :111d 'L'ilt hv the L'nlitv. I he r:1te inl'iudes tilil SL' mess:I\!L'S receivL·d m sent in error.~~

~~lhe number uiiCt\IP :\dd1·es~ i'v1:isk Request llll'\S:I_!,!es r~.:ceived.~~ protocol. lt also describes various error counts for the ICMP protocol.

ICMP performance counter

Messages Outbound Errors

Messages Received Errors

Messages Received/Second

Messages Sent/Second

Messages/Second

Received Address Mask

Received Address Mask Reply

Received Destination Unreachable

Received Echo Reply/Second

Received Echo/Second

Received Parameter Problem

Received Redirect/Second

Received Source Quench

Received Time Exceeded

Received Timestamp

Reply/Second

Received Timestamp/Second

Sent Address Mask

Sent Address Mask ~~Reply~~Repiy
Sent Destination Unreachable
Sent Echo Reply/Second
Sent Echo/Second
Sent Parameter Problem
~~Sent Redirect/Second Sent Source Quench Sent Time Exceeded Sent Timestamp Reply/Second Sent Timestamp/Second~~
Meaning
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 lP to route the resultant datagram. ln some implementations, there may be no types of error that contribute to this counter's value.
The number of ICMP messages that the entity received, but determined as having errors (bad ICMP checksums, bad length, and so on).
The rate at which ICMP messages are received by the entity.
The rate includes those messages received in error.
The rate at which ICMP messages are attempted to be sent by the entity. The rate includes those messages sent in error.
The total rate at which ICMP messages are received and sent by the entity. The rate includes those messages received or sent in error.
True number of ICMP Address Mask Request messages received.
The number of ICMP Address Mask Reply messages received.
The number of ICMP Destination Unreachable messages received.
The rate of ICMP Echo Reply messages received.
The rate of ICMP Echo messages received.
The number of ICMP Parameter Problem messages received.
The rate of ICMP Redirect messages received.
The number of ICMP Source Quench messages received.
The number of ICMP Time Exceeded messages received.
The rate of ICMP Timestamp Reply messages received.
The rate of ICMP Timestamp (request) messages received.
The number of ICMP Address Mask Request messages sent.
The number of ICMP Address Mask Reply messages sent.
The number of ICMP Destination Unreachable messages sent.
The rate of ICMP Echo ~~Reply~~Repiy messages sent.
The rate of ICMP Echo messages sent.
The number of ICMP Parameter ~~Problem~~Probiem messages sent.

Using Performance Monitor with TCP/IP Sen/ices 4of10

Sent Redirect/Second The rate of ICMP Redirect messages sent.

Sent Source Quench The number of ICMP Source Quench messages sent.
~~The number of ICMP~~
Sent Time Exceeded ~~messages sent.~~
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.

~~Chapter 8 Using~~Monitoring TCP/IP Performance ~~Monitor with TCPnP Services~~
IP Performance Counters
The IP Object Type includes those counters that describe the rates that
Internet Protocol (IP)
datagrams are received and sent by ~~acertain~~a certain computer using the IP
protocol. It also describes
various error counts for the IP protocol.
IP performance counter Meaning
Datagrams Forwarded/Second
~~Datagrams Outbound Discarded~~
~~Datagrams Outbound No Route~~
~~Datagrams Received Address Errors~~
~~Datagrams Received Delivered/Second~~
~~Datagrams Received Discarded~~
~~Datagrams Received Header Errors~~
~~Meaning~~ The rate of input datagrams for which this entity was not their ~~finalIP~~
final IP destination that resulted in an attempt to find a route to ~~forward~~
fon/vard them to that final destination. ~~In~~ln 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.
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.
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~~fonmard datagrams,
this counter includes datagrams discarded because the
destination address was not a local address.
The rate at which input datagrams are successfully delivered to
IP user protocols (including ICMP).
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.
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.
The number of locally addressed datagrams received

successfully but discarded because of an unknown or
unsupported protocol.
The rate at which IP datagrams are received from the
interfaces, including those in error.
Datagrams Outbound No Route
Datagrams Received Address
Errors
Datagrams Received
Delivered/Second
Datagrams Received Discarded
Datagrams Received Header
Errors
Datagrams Received Unknown
Protocol
Datagrams Received/Second
counter does not include any datagrams counted in Datagrams
Using Performance Monitor with TCP/IP Sewices 5of10
Datagrams Sent/Second The rate at which IP datagrams are supplied to IP for
transmission by Iocai IP user protocols (including ICMP). This

Datagrams/Second
Fragment Re-assembly Failures
Fragmentation Failures
Fragmented Datagrams/Second
Fragments Created/Second
Fragments
Re-assembled/Second
Fragments Received/Second
~~Meaning~~
~~The number of locally addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.~~
~~The rate at which IP datagrams are received from the interfaces, including those in error.~~
~~The rate at which IP datagrams are supplied to IP for transmission by local IP user protocols (including 1CMP). This~~ counter does not include any
datagrams counted in Datagrams
Forwarded.
The rate at which IP datagrams are received from or sent to the
interfaces, including those in error. Any ~~forwarded~~fonNarded datagrams
are not included in this rate.
The number of failures detected by the IP reassembly
algorithm (for whatever reason: timed out, errors, and so on).
This is not necessarily ~~acount~~a count of discarded IP fragments,
because some algorithms (notably RFC ~~SIS~~815) can lose track of
the number of fragments by combining them as they are
received.
The number of IP datagrams that have been discarded
because they needed to be fragmented at this entity ~~hut~~but could
not be, for example, because their "Don't Fragment" flag was
set.
The rate at which datagrams are successfully fragmented at
this entity.
The rate at which ~~1P~~IP datagram fragments have ~~heen~~been generated
as a result of fragmentation at this entity.

The rate at which ~~IP fragmenl'l are~~IP fragments are successfully reassembled.
The rate at which IP fragments that need to ~~he reassembled~~be reassembied at this entity are received.

~~Chapter 8 Using~~Monitoring TCPIIP Performance ~~Monitor with TCPnP Services~~
Network Interface Performance Counters for TCP/IP
The Network Interface ~~Ohject~~Object Type includes those counters that ~~descrihe~~describe the rates at which
bytes and packets are received and sent over a network TCP/IP connection. ~~It~~it also describes
various error counts for the same connection.
The rate at wnich bytes are received on the interface, including framing characters.
The rate at which bytes are sent on the interface, including
~~Network Interface counter~~ framing characters.
Bytes Received/Second
Bytes Sent/Second
Bytes Total/Second
Current Bandwidth
Output Queue Length
Packets Outbound Discarded
Packets Outbound Errors ~~Packets Received Discarded~~
~~Meaning~~
~~The rate at which bytes are received on the interface, including framing characters.~~
Packeis Received Discarded
Packets Received Errors
Packets Received
Non-Unicast/Second
Packets Received
Unicast/Second
Packets Received Unknown
Packets Received/Second
Packets Sent
~~The rate at which bytes are sent on the interface, including framing characters.~~ Non-Unicast/Second
The rate at which bytes are sent and received on the interface, including framing characters.
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.
The length of the output packet queue (in packets.) ~~If~~lf 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.
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~~possibie reason for discarding such a packet could be to free up buffer space.
The number of outbound packets that could not be transmitted because of errors.
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~~protocol. One possible
reason for discarding such a packet could be to free up buffer
space.
The number of inbound packets tnat contained errors
preventing them from being deliverable to a higher-layer
protocol.
The rate at wlmich non-unicast (that is, subnet broadcast or
subnet multicast) packets are delivered to a higher-layer
protocol.
The rate at which (subnet) unicast packets are delivered to a
higher-layer protocol.
The number of packets received via the interface that were
discarded because of an unknown or unsupported protocol.
The rate at which packets are received on the network
interface.
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 intcludes the
. Using Performance Monitor with TCP/IP Services 60f10
Network Interface counter Meaning
~~Packets Received Errors~~
~~Packets Received Non Unicast/Second~~
~~Packets Received Unicast/Second~~ ~~Packets Received Unknown~~
~~Packets Received/Second~~
~~Packets Sent Non-Unicast/Second~~

Packets Sent Unicast/Second
Packets Sent/Second
Packets/Second
~~Meaning~~
~~The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.~~
~~The rate at which non unicast (that is, subnet broadcast m subnet multicast) packets are delivered to a higher-layer protocol.~~
~~The rate at which (subnet) unicast packets are delivered In a higher layer protocol.~~
~~The number of packets received via the interface that wen: discarded because of an unknown or unsupported protocol.~~
~~The rate at which packets are received on the network interface.~~
~~The rate at which packets are requested to be transmitted to non-unicast (that is, subnet broadcast or subnet multicast)~~ addresses by higher-level protocols. The rate includes the
packets that were discarded or not sent.
The rate at which packets are requested to be transmitted to
subnet-unicast addresses by higher-level protocols. The rate
includes the packets ~~that~~mat were discarded or not sent.
The rate at which packets are sent on the network interface.
The rate at which packets are sent and received on the
network interface.

:S
~~Chapter 8 Using~~Monitoring TCP/IP Performance ~~Monitor with TCP/IP Services~~
TCP Performance Counters

The TCP Object Type includes those counters that describe the rates that Transmission
Control Protocol (TCP) segments are received and sent by a certain entity using the TCP
protocol. ~~In~~ln addition, it describes the number of TCP connections that are in each of the
possible TCP connection states.
TCP performance counter~~ Meaning~~
Connection Failures~~ The number of times TCP connections have made a direct transition to the CLOSED state from the SYN-SENT state or the SYN-RCVD state. plus the number of times TCP connections have made a direct transition to the LISTEN state from the SYN RCVD state.~~
Connections Active~~ The number of times TCP connections have made a direct transition to the SYN SENT state from the CLOSED 'itate.~~
Connections Established
Connections Passive
Connections Reset
Segments Received/Second
Segments Retransmitted/Second
Segments Sent/Second
Segments/Second
Meaning
The number of times TCP connections have made a direct
transition to the CLOSED state from the SYN-SENT state or
the SYN-RCVD state, plus the number of times TCP
connections have made a direct transition to the LISTEN state
from the SYN-RCVD state.
Tne number of times TCP connections have made a direct
transition to the SYN-SENT state from the CLOSED state.
The number of TCP connections for which the current state is
either ESTABLISHED or CLOSE-WAIT.
~~Connections Passive~~ The number of times TCP connections have made ~~a~~e direct
transition to the SYN-RCVD state from the LISTEN state.
~~Connections Reset~~ The number of times TCP connections have made a direct
transition to the CLOSED state from either the ~~ESTABLISHED~~ESTABUSHED
state or the CLOSE-WAIT state.
~~Segments Received/Second~~ The rate at which segments are received, including those
received in error. This count includes segments received on
currently established connections.
~~Segments Retransmitted/Second~~ The rate at which segments are retransmitted, that is~~.~~,
segments transmitted containing one or more previously
transmitted bytes.
~~Segments Sent/Second~~ The rate at which segments are sent, including those on
current connections, but excluding those containing only
retransmitted bytes.
~~Segments/Second~~ The rate at which TCP segments are sent or received using the
TCP protocol.
. Using Performance Monitor with TCP/IP Services 7of10

,I 4ii

Monitoring TCP/IP Performance
UDP Performance Counters
The UDP Object Type includes those counters that describe the rates that User Datagram
Protocol (UDP) ~~datagrarns~~datagrams are received and sent by ~~acertain~~a certain entity ~~usinK~~using the UDP protocol. It
also describes various error counts for the UDP protocol.
UDP ~~perfonnance~~performance counter ~~Meaning~~
Datagrams No Port/Second
Datagrems Received Errors
Datagrams Received/Second
Datagrams Sent/Second
Datagrams/Second
Meaning
The rate of received UDP datagrams for which there was no
application at the destination port.
~~Datagrams Received Errors~~ The number of received UDP datagrams that could not ~~he~~be
delivered for reasons other than the lack of an application at
the destination port.
~~Datagrams Received/Second~~ The rate at ~~which~~whicrm UDP datagrams are delivered to UDP users.
~~Datagrams Sent/Second~~ The rate at which UDP datagrams are sent from the entity.
~~Datagrams/Second~~ The rate at which UDP datagrams are sent or received by the entity.
Using Performance Monitor with TCP/IP Services 80f10

r .1
Eg* i
~~Monitoring FTP Server Traffic~~ >
When you install the ~~FfP~~FTP Server services, the necessary software is also installed so that you
can monitor and graph various ~~FfP~~FTP Server statistics using Performance Monitor. Using
Performance Monitor to view activity on remote Windows NT systems makes ~~FfP~~FTP Server
administration more convenient when you are administering multiple Windows NT ~~FfP Servers~~FTP Sewers.
~~Chapter 8 Using Performance Monitor with TCPnP Services~~
~~IJl>~~ To view counters specific to the FTP ~~Server~~Sewer service

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

The FTP Server performance counters ~~are~~are cleared each time you start and stop the FTP
Server service.
FTP performance counter
Bytes Received/Second
Bytes Sent/Second
Bytes Total/Second
Connection Attempts
Current Anonymous Users
Current Connections
Current NonAnonymous Users
Files Received

Files Sent
Files Totai
Logon Attempts
Maximum Anonymous Users
Maximum Connections
Maximum NonAnonymous Users
Total Anonymous Users
Total NonAnonymous Users
~~FI'P performance counter~~ Meaning
~~Bytes Received/Second~~ The rate at which data ~~hytes are~~bytes are received ~~hy the FrP~~by tbe FTP Server. ~~Bytes Sent/Second~~
The rate at ~~which~~whicb data bytes ~~are~~are sent by the FTP Server.
~~Bytes Total;Second~~ The sum of Bytes Sent/Second and Bytes
Received/Second.
This is the total rate of bytes transferred by the FTP ~~Server~~Sewer.
~~Connection Attempts~~ The ~~numher~~number of connection attempts that have
been made to
the FTP Server.
~~Current Anonymous Users~~ The number of anonymous users currently
connected to the
FTP Server.
~~Current Connections~~ The current number of connections to the ~~-TP~~FTP Server.
~~Current NonAnonymous~~ The number of nonanonymous users ~~currenrly~~currently
connected ~~Users~~ to
the FTP Server.
~~Files Received~~ The total number of files received by the FTP Server.
~~Files Sent~~ The total number of files sent by the FTP Server.
~~Files Total~~ The sum of Files Sent and Files Received. This is the total
number ~~of files~~offiles transferred by the FTP Server. ~~Logon Attempts~~
The number of logon attempts that have been made to the FTP
Server.
~~Maximum Anonymous~~ The maximum number of anonymous users ~~Users~~ simultaneously
connected to the FTP Server. ~~Maximum Connections~~
The maximum number of simultaneous connections to the FTP
Server.
~~Maximum NonAnonvmous~~ The maximum number of ~~nonanonvmous~~nonanonymous users
~~Users~~ simultaneously
connected to the FTP Server.
~~Total Anonymous Users~~ The total number of anonymous users that have ever
connected to the FTP Server. ~~Total NonAnonymous Users~~
The total number of nonanonymous users that have ever
connected to the FTP Server.
Using Performance Monitor with TCP/IP Sewices
Monitoring ~~WINS Server Performance~~ FTP Sewer Traffic

~~-~~
9of10

I*
When you install ~~aWINS~~a WINS server and SNMP services, counters are
automatically installed so
that you can use ~~Perfonnance~~Performance Monitor to view WINS Server service
~~perfonnance~~performance.
To view counters specific to the WINS ~~Server~~Sewer service

~~• In the Perfonnance Monitor window, select WINS Server in the Object list.~~
WINS performance counter
Failed Queries/Second
Failed Releases/Second ~~Group Conflicts/Second Group Registrations/Second Group Renewals/Second Queries/Second Releases/Second Successful Queries/Second Successful Releases/Second Total Number of Conflicts/Second Total Number of Registrations/Second Total Number of Renewals/Second Unique Conflicts/Second Unique Registrations/Second Unique Renewals/Second~~ Meaning
The total number of failed queries per second.
The total number of failed releases per second.
The rate at which group registrations received by the WINS server resulted in conflicts with records in the database.
Group Conflicts/Second
The rate at which group registrations are received by the WINS server.
The rate at which group renewals are received by the WINS server.
The total number of queries per second, which is the rate at which queries are received by the WINS server.
The total number of releases per second, which is the rate at which releases are received by the WINS server.
The total number of successful queries per second.
The total number of successful releases per second.
The sum of the Unique and Group ~~1.'ontlicts~~conflicts per second, which is the total rate at which ~~contlicts~~conflicts were seen by the WINS server.
The sum of the Unique and Group registrations per second.
This is the total rate at which registrations are received by the WINS server.
The sum of the Unique and Group registrations per second, which is the total rate at which renewals are received by the WINS server.
The rate at which unique registrations and renewals received by the WINS server ~~resulted~~resuited in conflicts with records in the database.
The rate at which unique registrations are received by the WINS server.
The rate at which unique renewals are received by the WINS server.

~~18:~~
Group Registrations/Second
Group Renewals/Second
Queries/Second
Releases/Second
Successful Queries/Second
Successful Releases/Second
Total Number of Conflicts/Second
Total Number of Registrations/Second
Total Number of Renewals/Second
Unique Confiicts/Second