

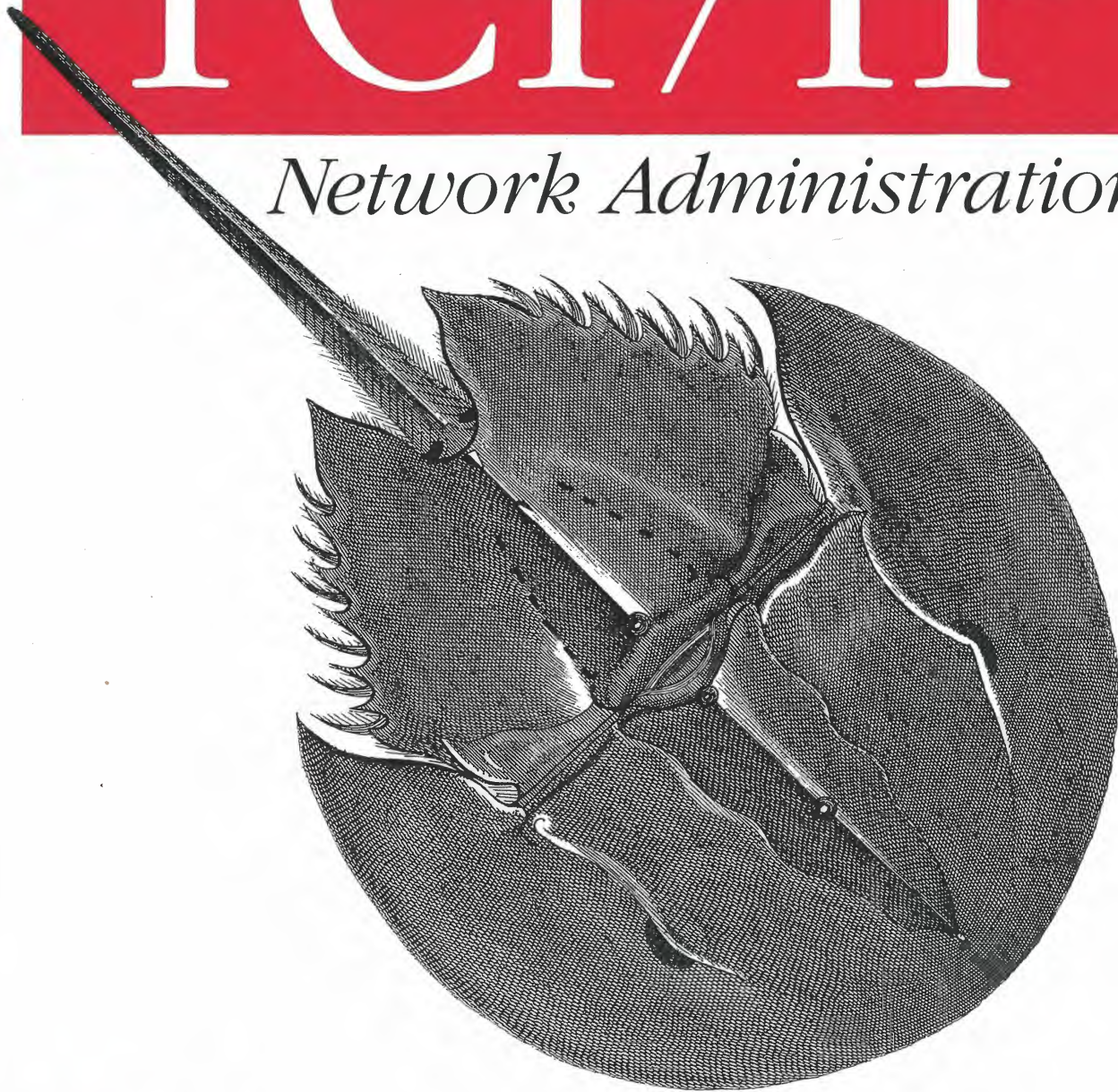
Help for Windows NT System Administrators

Prep
for
MCSE

Windows NT

TCP/IP

Network Administration



O'REILLY®

Craig Hunt & Robert Bruce Thompson

Windows NT TCP/IP Network Administration

Craig Hunt and Robert Bruce Thompson

O'REILLY®

Beijing · Cambridge · Farnham · Köln · Paris · Sebastopol · Taipei · Tokyo

Windows NT TCP/IP Network Administration

by Craig Hunt and Robert Bruce Thompson

Copyright © 1998 O'Reilly & Associates, Inc. All rights reserved.
Printed in the United States of America.

Published by O'Reilly and Associates, Inc., 101 Morris Street, Sebastopol, CA 95472.

Editor: Robert Denn

Production Editor: Paula Carroll

Production Service: TIPS Technical Publishing

Printing History:

October 1998: First Edition.

Nutshell Handbook, the Nutshell Handbook logo, and the O'Reilly logo are registered trademarks of O'Reilly & Associates, Inc. The association between the horseshoe crab and the topic of TCP/IP is a trademark of O'Reilly and Associates.

Many of the designations used by manufacturers and sellers to distinguish their products are claimed as trademarks. Where those designations appear in this book, and O'Reilly & Associates, Inc. was aware of a trademark claim, the designations have been printed in caps or initial caps.

While every precaution has been taken in the preparation of this book, the publisher assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained herein.



This book is printed on acid-free paper with 85% recycled content, 15% post-consumer waste. O'Reilly & Associates is committed to using paper with the highest recycled content available consistent with high quality.

ISBN: 1-56592-377-4

[9/99]

Table of Contents

<i>Preface</i>	<i>xi</i>
1. Overview of TCP/IP	1
TCP/IP and the Internet	2
A Data Communications Model	4
TCP/IP Protocol Architecture	7
Network Access Layer	9
Internet Layer	10
Transport Layer	16
Application Layer	20
Summary	21
2. Delivering the Data	23
Addressing, Routing, and Multiplexing	23
The IP Address	25
Subnets	31
The Routing Table	34
Address Resolution	37
Protocols, Ports, and Sockets	38
Summary	44
3. Network Services	46
Names and Addresses	47
The Host Table	49
LMHOSTS	51
Domain Name System	52

Windows Internet Name Service	59
Mail Services	60
Dynamic Host Configuration Protocol	69
Summary	71
4. <i>Getting Started</i>	73
To Connect or Not to Connect	74
Basic Information	76
Planning Routing	83
Planning Naming Service	86
Other Services	90
Informing the Users	91
Summary	92
5. <i>Installing TCP/IP</i>	94
Windows NT Networking	94
Configuring the TCP/IP Protocol	107
Summary	119
6. <i>Using Dynamic Host Configuration Protocol</i>	121
Why DHCP Is Needed	123
How DHCP Works	125
Planning for DHCP	133
Installing the DHCP Server Service	139
Installing and Configuring the DHCP Relay Agent	141
Managing DHCP with DHCP Manager	142
Maintaining and Troubleshooting DHCP Server	154
Summary	156
7. <i>Using Windows Internet Name Service</i>	158
Why WINS Is Needed	159
How WINS Works	163
Installing the WINS Server Service	175
Managing WINS with WINS Manager	176
Troubleshooting WINS	192
Summary	195
8. <i>Configuring DNS Name System</i>	197
The Microsoft DNS Server	199
Planning Your DNS Service	200

Installing the DNS Server	202
The DNS Manager	202
Creating a New Zone	203
Building the DNS Database	207
The DNS Files	209
Using nslookup	218
Summary	222
9. Microsoft Routing and Remote Access Service	223
Routing and Remote Access Service Features	224
Installing Microsoft Routing and RAS	230
Administering Microsoft Routing and RAS	241
Using Dial-Up Networking (DUN)	266
Summary	276
10. Internet Information Server (IIS)	278
IIS Components	279
Installing IIS	281
Configuring IIS	292
Managing IIS	340
Summary	347
11. Troubleshooting TCP/IP	348
Approaching a Problem	348
Diagnostic Tools	351
Testing Basic Connectivity	353
Troubleshooting Network Access	356
Checking Routing	363
Checking Name Service	367
Analyzing Protocol Problems	371
Protocol Case Study	375
Simple Network Management Protocol	378
Summary	380
12. Network Security	382
Security Planning	383
Firewalls	388
Encryption	392
User Authentication	394
Software Security	401

Security Monitoring	403
File Security	407
Words to the Wise	410
Summary	411
13. Information Resources	412
The World Wide Web	412
Anonymous FTP	416
Retrieving RFCs	416
Mailing Lists	418
Newsgroups	420
The White Pages	424
Summary	427
A. PPP Scripting Languages	429
B. DNS Resource Records	443
C. Microsoft DHCP Option Support	458
D. Routing Protocols	465
Index	475

10

In this chapter:

- *IIS Components*
- *Installing IIS*
- *Configuring IIS*
- *Managing IIS*
- *Summary*

Internet Information Server (IIS)

Microsoft jumps into anything they do with both feet. When Microsoft belatedly noticed the Internet phenomenon, they were caught with their collective pants down. Without any products to address the needs of this exploding new market segment, they believed themselves to be in danger of losing market share to the new guys on the block—read Netscape. As anyone familiar with Microsoft might guess, they pulled out all the stops to get competitive products to market as soon as possible. On the client side, they bought rights to a third-party web browser, renamed it Internet Explorer, and turned it into a world-class browser in record time. On the server side, they created a multi-purpose product called Internet Information Server, or IIS for short.

IIS has grown in Internet time. Microsoft cobbled together a quick and dirty IIS 1.0 and released it as an update to Windows NT Server 3.51. It wasn't much more than a placeholder, but at least it got the ball rolling. When Windows NT Server 4.0 was released, it bundled IIS 2.0, a significant upgrade that filled most of the gaping holes and killed most of the bugs in IIS 1.0. Still, the major third-party web server vendors like Netscape and O'Reilly weren't too worried—IIS2 couldn't compete with their feature sets.

When Microsoft shipped IIS3, the third party vendors started to sweat. Microsoft was giving away a product that compared favorably in features and performance with their expensive commercial products. Even worse, Microsoft started to ship free supporting components, like Index Server, that made IIS a complete server-side Internet solution.

At this point, the way things are headed is pretty clear. The release of IIS4 as a part of the Windows NT 4.0 Option Pack, which shipped in Q1 1998, may well be the final nail in the coffin of the commercial web server vendors. The majority of

Internet web servers are now running either IIS or the free Apache server. When you consider private Intranet servers, the proportion running IIS is even higher.

The Web, FTP, and email are where the action is on the Internet today. Depending on whose figures you believe, something close to 99 percent of the current traffic on the Internet is web-, ftp-, or email-related. As IP telephony becomes more popular, that may change, but for now at least it is true. IIS4 provides an excellent no-cost server-side solution for all three of these core Internet services.

NOTE To understate the case, IIS4 is a major application, with supporting applications that are major applications in themselves. Covering IIS thoroughly would require an entire book—or several books. Accordingly, this chapter focuses on getting started with IIS—the essentials of installing and configuring the web, FTP, and SMTP components of IIS at the overview level. For a book-length treatment of this topic, see any of the numerous books devoted to it.

IIS Components

The IIS4 distribution, which is contained within the Windows NT 4.0 Option pack, contains the following major functional IIS components:

World Wide Web (WWW) Service

A standards-compliant HTTP (web) server.

File Transfer Protocol (FTP) Service

A standards-compliant FTP server.

Simple Mail Transfer Protocol (SMTP) Service

A standards-compliant SMTP relay server.

Network News Transport Protocol (NNTP) Service

A standards-compliant NNTP (news) server. The NNTP Service is not installed by default, and we do not cover it in this chapter.

The IIS distribution also includes the following management tools:

Internet Service Manager (ISM)

The main management tool for IIS and the other applications included in the Windows NT 4.0 Option Pack. You can use ISM to manage IIS on the local IIS server, from another computer on the network, or across the Internet. ISM is a snap-in for the Microsoft Management Console (MMC).

NOTE MMC is a Windows NT 5.0 component that provides an application framework for small dedicated utilities—called snap-ins—that perform management functions for a particular application. For example, you use MMC to manage IIS by loading the ISM snap-in into MMC. Windows NT 5.0 will include snap-ins that replace the patchwork quilt of individual management tools, for example, User Manager for Domains and Server Manager, used by Windows NT 4.0. Like Routing and RAS, MMC is a Windows NT 5.0 technology that Microsoft has released as an upgrade to Windows NT 4.0.

Internet Service Manager (HTML)

A browser-based management tool that provides most ISM functions. You can use ISM (HTML) to manage IIS on the local IIS server, from another computer on the network, or across the Internet.

In addition, the Windows NT 4.0 Option Pack distribution includes the following components which are not a part of IIS, but provide supporting functionality:

Certificate Server

Manages the digital certificates used by IIS to provide server and client authentication with the SSL (Secure Sockets Layer) and PCT (Private Communication Technology) protocols.

FrontPage 98 Server Extensions

Server-based extensions that allow FrontPage clients and IIS to operate as a client-server pair.

Internet Connection Services for RAS

Supplements and extends basic RAS with tools that provide a customizable dialer, centralized phone book administration, and RADIUS support.

Microsoft Data Access Components 1.5

Includes ActiveX Data Objects (ADO), Remote Data Service (RDS), the Microsoft OLE DB Provider for ODBC, and Open Database Connectivity (ODBC) components that can be used to provide client/server applications with access to data on remote servers.

Microsoft Index Server

Indexes documents on an IIS web site, and allows client browsers to search the web site by using an HTML query form.

Microsoft Management Console (MMC)

Provides the framework for the application-specific management tools for Option Pack components, including IIS4, Index Server, and Transaction Server. MMC is a general-purpose template manager that uses programs called snap-ins to manage specific components. For example, the Internet Service

Manager (ISM) application is actually a snap-in that runs under the MMC framework. Just think of MMC as the socket wrench and the snap-ins as the sockets. In addition to the MMC-based management tools that can be used locally or across the network, IIS4 and Index Server both include HTML-based tools that allow administrators to use a limited subset of management functions from a web browser.

Microsoft Message Queue (MSMQ)

Allows applications to communicate asynchronously with other applications by sending and receiving messages.

Microsoft Script Debugger

Debugger for ASP pages that contain VBScript, JScript, or Java scripts. You can also use Microsoft Script Debugger to debug scripts written in other scripting languages, for example, Perl or REXX, that support host-independent debugging.

Microsoft Site Server Express

A functionally limited version of the commercial Microsoft Site Server product that provides site and usage analysis, the Posting Acceptor, and the Web Publishing Wizard.

Microsoft Transaction Server (MTS)

A component-based transaction processing system that you can use to develop, deploy, and manage server-based applications. MTS provides a run-time environment and GUI-based administration tool for managing applications.

Windows Scripting Host (WSH)

Allows you to perform common administrative tasks from the command line. WSH is a language-independent scripting host for 32-bit Windows platforms. Presently, WSH uses only the VBScript and JScript scripting engines supplied by Microsoft. However, it is likely that other companies will soon provide Active-X scripting engines for other scripting languages like Perl and REXX.

Installing IIS

Installing IIS4 is a relatively straightforward (albeit time consuming) multi-step process. After you obtain the IIS4 distribution files and prepare your server, you install Internet Explorer 4.01 or higher and then run IIS4 Setup. Because installing IIS4 may require unloading services that may be needed by users and because it requires at least two system restarts, you may want to schedule the installation outside normal working hours unless you are installing IIS4 on a dedicated server. The remainder of this section details the steps necessary to install IIS4.

Configuring IIS

The bulk of this chapter is contained in the following sections, which detail how to configure IIS once you've installed it. This material concentrates on the three major services—the WWW Service, the FTP Service, and the SMTP Service—that are installed when you run IIS Setup using the Typical option. Although the NNTP Service is not covered, configuring it is very similar to configuring the other services.

Using Internet Service Manager (ISM)

Internet Service Manager (ISM) is the main management tool for IIS. ISM runs as a snap-in under the Microsoft Management Console (MMC). To start ISM choose Start → Programs → Windows NT 4.0 Option Pack → Microsoft Internet Information Server → Internet Service Manager. MMC runs and automatically loads the ISM snap-in.

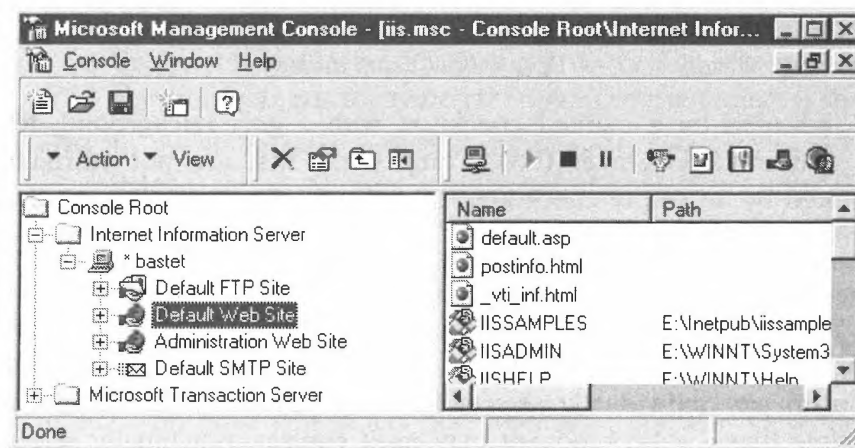


Figure 10-2. The Internet Service Manager

Which toolbar icons and menu choices are available in ISM depend on the object currently selected. For example, Figure 10-2 shows ISM with the Default Web Site object selected. Because we have a web site selected, the toolbar includes three VCR-like icons that you can use to start, stop, or pause the web site. The toolbar also contains icons for Key Manager, Performance Monitor, Event Viewer, Server Manager, and User Manager for Domains, all of which are commonly used when managing a web site. In addition to context-sensitive toolbars, ISM provides the standard context-sensitive menus that you can access by right-clicking an object. We'll use ISM in the following sections to configure settings for the various services installed.

Configuring Computer Properties

Use the Internet Information Server page of the <computer-name> Properties dialog to configure the global IIS properties for the selected computer. To display this dialog, shown in Figure 10-3, log on as an administrator, start Internet Service Manager, right-click the computer name in MMC to display the context-sensitive menu, and choose Properties.

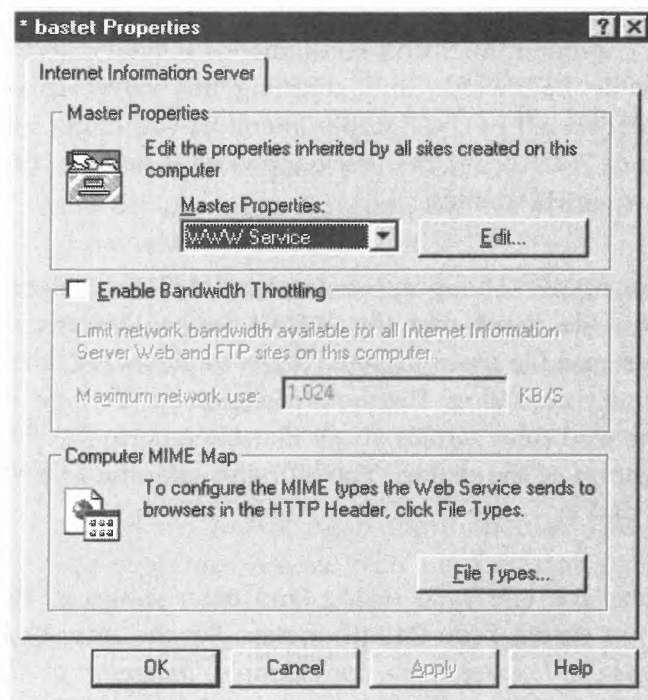


Figure 10-3. Configuring global IIS properties

You use this dialog to set default properties for all Web and FTP sites, control the bandwidth used by all web sites, and set MIME configuration for all sites, as follows:

Master Properties section

Use the Master Properties drop-down list to select a service type—either WWW Service or FTP Service—and click Edit to display the tabbed properties dialog for that service. Using these tabbed properties dialogs is described in the following sections. The settings you make here are the default values that will be used when you create a new Web or FTP site. If these settings are different from those of an existing site, you are given the opportunity to replace the current settings with the new master property settings or to continue to use the existing settings. You can also override these settings later for any particular site. List-formatted properties—for example, access lists, custom error

messages, or filters—are treated as single properties. Changes are not merged with existing list data, but are overwritten by the new data.

Enable Bandwidth Throttling section

Use this section to limit the bandwidth available to all WWW sites on the selected computer. To do so, mark the Enable Bandwidth Throttling checkbox and enter a value in the Maximum network use box. You would typically use this option to limit the availability of bandwidth to the WWW Service on a computer that also provides other bandwidth-consuming services, for example, mail or RAS. On such a computer, Microsoft recommends initially allocating 50 percent of the available bandwidth, and adjusting this value up or down as needed. For example, on a T1 (1.544 Mbps) interface, you might initially set throttling to a value of 772 Kbps. Note that bandwidth throttling controls bandwidth use only by static HTML files.

Computer MIME Map section

Use this section to configure MIME (Multipurpose Internet Mail Extensions) mappings, which specify the file types that the WWW Service returns to browsers. To display the registered file types installed with Windows NT, click File Types to display the File Types dialog. Highlight a registered file type in the Registered file types pane to display details about that file type in the File type details section at the bottom of the dialog. You can also take the following actions in the File Types dialog:

Add a MIME mapping

Click New Type to display the File Type dialog, and enter values in the Associated Extension: and Content Type (MIME): boxes. For the latter box, use the syntax `<mime-type>/<file-extension>`, for example, `image/bmp`.

Remove a MIME mapping

Highlight a registered file type and click Remove.

Edit a MIME mapping

Highlight a registered file type, click Edit to display the File Type dialog, and make the necessary changes to the Associated Extension and/or Content Type (MIME): boxes.

Changing MIME mapping in the master property sheet for the computer changes those properties for all sites, and for the computer itself. You can instead modify MIME mappings for a particular site, which displays only the changed mappings. If you subsequently change the MIME mappings in the master property sheet, the custom mappings for individual sites are overwritten by the new master property sheet mappings.

The pane lists the status of each ISAPI filter (loaded, unloaded or disabled), that filter's name, and the priority assigned to the filter in the DLL. The Details section displays the same information, and adds the name of the executable file that contains the filter. You can modify the ISAPI filter configuration for the web site as follows:

Add an ISAPI filter

Click Add to display the Filter Properties dialog. Enter the Filter Name and Executable, or browse for the executable that contains the filter.

Remove an ISAPI filter

Highlight the filter in the pane and click Remove.

Edit an ISAPI filter

Highlight the filter in the pane and click Edit to display the Filter Properties dialog.

Enable or Disable an ISAPI filter

Highlight the filter in the pane and click Enable to enable a filter that is currently disabled, or click Disable to disable a filter that is currently enabled.

Change the order in which ISAPI filters are loaded

ISAPI filters are loaded in the order that they appear in this pane. To change this order, highlight a filter in the pane and use the up arrow or down arrow to rearrange the list.

ISAPI filters are processed according to the following rules:

- All web sites inherit the ISAPI filters configured in Master Properties for the computer, which are not displayed for the individual web sites.
- When you add filters to an individual web site, those filters are merged with the default filters for the site that are configured in Master Properties for the computer.
- If several filters are registered for the same event, they are called sequentially, as follows:
 - A filter with a higher priority is always processed before any filter with a lower priority.
 - If two filters have the same priority, the global filter set in Master Properties is processed before the local filter defined for the individual web site.
 - If two filters at the same level (global or local) have the same priority, they are processed in the order that they were loaded, which is determined by the order in which they appear in the pane.

Configuring Home Directory properties

Use the Home Directory page of the Web Site Properties dialog to change the location of or modify the properties for the home directory for the web site.

Installing IIS creates the web root directory that you specify, ordinarily `\inetpub\wwwroot`. You can use this dialog to change that location. This is a dynamic dialog, whose contents vary according to the option button you select in the top section, as follows:

A directory located on this computer

Select this option, which is the default, to use a web root directory on the local computer where you installed IIS. Use this page to specify the location, access permissions, and content control for the local directory, as well as application settings. Uses standard drive/directory syntax, for example `C:\web\htmlfiles`.

A share located on another computer

Select this option to use a web root directory located on a network share. The options and settings are similar to those available when the web root directory is on the local computer. Uses UNC syntax in the form `\\servername\share-name`, for example, `\\bastet\htmlfiles`.

A redirection to a URL

When a browser requests the original URL associated with the web site, it is automatically redirected to the URL specified here. You can map requests to another web site by using the fully qualified URL for that web site, for example, `http://www.oreilly.com`. Alternatively, you can map requests to a virtual directory by using a virtual path, for example, `/htmlfiles`. You can use redirection variables and wildcards in the target URL to control how the source URL is mapped to the target URL.

These options are described in the following sections.

A directory located on this computer

Use the Home Directory page of the Web Site Properties dialog shown in Figure 10-6 to change the location of or modify the properties for the home directory for the web site, if that home directory is located on the computer where IIS is installed.

Set the following options:

Local Path

Type the drive and directory for the local path where the home directory resides on the local computer, or browse for the location.

Access Permissions

Use these checkboxes to specify what type of access is allowed to the home directory. If the home directory is located on an NTFS volume, these settings should match the NTFS permissions for that directory. If the settings do not match, the most restrictive settings are used. For example, if you grant Write

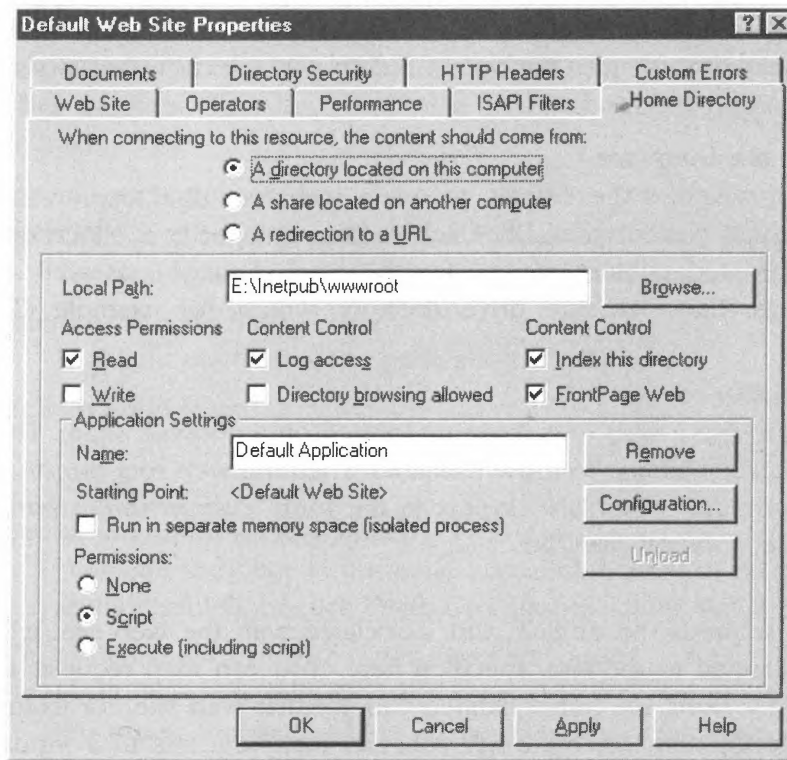


Figure 10-6. The Home Directory page of the Web Site Properties dialog

permission in this dialog, but a particular user has the No Access NTFS permission for the directory, that user will be unable to access the directory.

Read

Mark this checkbox, which is marked by default, to assign Read permission if you want clients to be able to read or download the files contained in the home directory. The WWW Service returns an error if a client attempts to retrieve a file located in a directory for which Read permission has not been granted. Grant Read permission only for directories that contain public information like HTML pages and images. Do not grant Read permission for directories that contain system files, scripts (CGI and ISAPI), and other material that you do not want clients to be able to retrieve.

Write

Mark this checkbox, which is cleared by default, to assign Write permission if you want clients to be able to upload files to the web site, or to change content in files that are write-enabled. Only clients who are using a web browser that supports that HTTP 1.1 put feature can write files.

Content Control

Use these checkboxes to control the behavior of the WWW service for the home directory, as follows:

Log access

Mark this checkbox, which is marked by default, to cause the WWW service to write a log file entry for each visit to this directory. For this setting to be effective, logging must be enabled for the web site in the Web Site properties page, which it is by default

Directory browsing allowed

Mark this checkbox, which is cleared by default, to automatically generate a hypertext directory listing. When this setting is enabled, if a client enters this directory without specifying a file name, and if no default document exists in the directory, the client receives the hypertext directory list, which enables him to navigate the directory tree. Only actual directories are included in the hypertext list. In order to change to a virtual directory, a client must explicitly enter the alias or URL or select a link on another page that points to that virtual directory. This option is disabled by default because enabling it allows a user to navigate the directory structure—a potential security risk.

Index this directory

Mark this checkbox, which is marked by default, to cause Index Server to index the contents of this directory when it does a full-text index of the web site.

FrontPage Web

Mark this checkbox, which is marked by default, to create a FrontPage web for this web site. Clear the checkbox to delete the FrontPage web for this site.

Application Settings

IIS defines an application as all directories and files contained within a directory that is marked as an application starting point, until another application starting point is encountered. If you define the home directory for the web site as an application starting point, all directories (physical and virtual) within that site can participate.

Create/Remove

To define a directory as an application starting point, click Create and name the application. To remove the home directory from the application, click Remove.

Name

Type the name of the application, which appears within the property sheets for any directory contained in the application.

Configuration

Click this button to display the tabbed Application Configuration dialog, which you can use to set ISAPI caching, define application mappings, set application configuration options, and set application debugging options.

Run in separate memory space (isolated process)

Mark this checkbox, which is cleared by default, to run the application as a separate process. Choosing this option protects all other processes—including the WWW Service itself—from being affected if this application crashes and burns. The only downside to marking this checkbox is that it causes the application to consume more memory.

Permissions

Mark one of the following option buttons to specify whether or not applications can run in the directory or to limit the types of applications that can run.

None

Select this option button to prevent any programs or scripts from running in this directory.

Script

Select this option button, which is enabled by default, to allow applications mapped to a script engine to run even though Execute permission is not granted. Set this option button for directories that contain scripts, for example, CGI, IDC, or ASP scripts. Granting Script permission is safer than granting execute permission because it limits the types of programs that can run.

Execute (including script)

Select this option button to allow any application to run in the directory, including applications that are mapped to script engines and Windows NT executables.

A share located on another computer

Use the Home Directory page of the Web Site Properties dialog to change the location of or modify the properties for the home directory for the web site, if that home directory is located on a network share rather than on the computer where IIS is installed. All settings on this page (and the appearance of the page itself) are identical to those described in the preceding section, with the following exceptions:

Network Directory

Enter the location of the home directory on the network share, using UNC format, for example, `\\servername\sharename`.

Connect As

Click this button to display the Network Directory Security Credentials dialog, and enter the username and password you want to use to connect to this share.

A redirection to a URL

Use the Home Directory page of the Web Site Properties dialog to redirect requests for the source URL to a URL you specify. Set the following options:

Redirect to

Specify a valid URL to which requests will be redirected, as follows:

- To map requests to another web site, enter the fully qualified URL of that web site. For example, if this web site is *www.tgnet.com* and you want to redirect requests to *www.oreilly.com*, enter *http://www.oreilly.com* here.
- To map requests to a virtual directory, enter the virtual path here. For example, to redirect requests to the virtual directory *wwwtemp*, enter */wwwtemp* here.
- To map requests selectively, you may enter a URL here that uses redirection variables and wildcards, as described in the online IIS documentation.

The client will be sent to

Mark one of the checkboxes below, as follows:

The exact URL entered above

Mark this checkbox, which is cleared by default, to redirect a virtual directory to the target URL without adding any part of the original URL. For example, if you want to redirect requests to the virtual directory */wwwtemp* to the HTML page *index.html*, enter *index.html* in the Redirect to: box and mark this checkbox.

A directory below this one

Mark this checkbox, which is cleared by default, to redirect a parent directory to a child directory. For example, if you want to redirect the home directory (*/*) to a subdirectory named */wwwtemp*, enter */wwwtemp* in the Redirect to: box and mark this checkbox. If this checkbox is not marked, the WWW Service will always map the parent directory to itself.

A permanent redirection for this resource

Mark this checkbox, which is cleared by default, to permanently redirect one resource to another. Ordinarily, redirects are temporary. When this checkbox is marked, the WWW Service returns a 301 Permanent Redirect message to the requesting browser, which can use that message to permanently alter a stored URL like a bookmark or favorite.

Configuring Documents properties

Use the Documents page of the Web Site Properties dialog to configure default documents and document footers. You can configure Documents properties at the web site, directory, and virtual directory levels, as follows:

Enable Default Document

Mark this checkbox, which is marked by default, to cause the web site to return a default document to a web browser that does not request a specific file name. The default document may be the home page for the directory, or the index page described earlier that allows the user to navigate the directory structure. You can specify multiple default documents, and the web site will return the first listed document it locates to the requesting browser. Use the Add and Remove buttons to modify the list of documents shown in the pane, and the up and down arrow keys to set the priority for each, with the top-most document having the highest priority.

Enable Document Footer

Mark this checkbox, which is cleared by default, and enter the full path and file name of an HTML-formatted page fragment in the box if you want the web site to append that HTML fragment as a footer to every page it delivers. This fragment should contain only the HTML tags necessary to format and display the footer content. The most common use of this feature is to append relatively static information, for example, copyright notices, to the bottom of each page delivered by the web site.

Configuring Directory Security properties

Use the Directory Security page of the Web Site Properties dialog, shown in Figure 10-7, to configure security settings for the web site.

Set the following options:

Anonymous Access and Authentication Control section

To allow anonymous users to access public information on the web site while permitting only designated users to access restricted content, you can configure the web site to authenticate users. To do so, click Edit to display the Authentication Methods dialog, shown in Figure 10-8.

Configure the following options to control access based on existing Windows NT user accounts and existing NTFS permissions on files and directories:

Allow Anonymous Access

Mark this checkbox, which is marked by default, if you want to allow users to connect to the server anonymously with restricted permissions (the normal state of affairs for a web server). When a user connects anonymously, the web server logs the user on with a valid Windows NT user account, which by default is named IUSR_<computer-name>, in this case

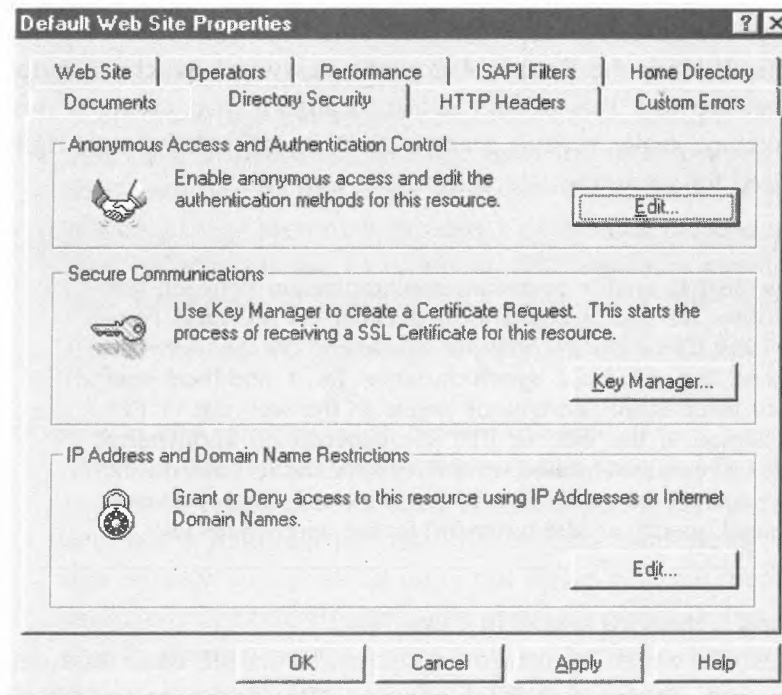


Figure 10-7. The Directory Security page

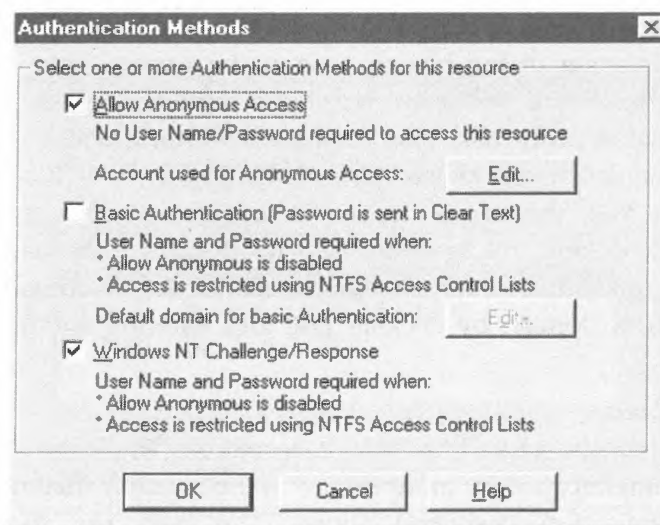


Figure 10-8. The Authentication Methods dialog

IUSR_BASTET. Windows NT creates this user account in User Manager for Domains and Internet Service Manager when IIS is installed, and assigns it the limited permissions needed by anonymous users. To change this anonymous username, click Edit to display the Anonymous User Account

dialog, and make the necessary changes. If you create a new anonymous user account, you must make sure that the UMD and ISM password settings are identical. Mark the Enable Automatic Password Synchronization checkbox to ensure that this occurs automatically. If you create a new anonymous account, make sure to grant it the "Log on locally" user right, which is required for anonymous access to the web site.

WARNING You can use ISM to enable password synchronization between ISM and a Windows NT user account located either on the local computer that runs IIS or on a computer elsewhere on the network. However, enabling password synchronization for a non-local user account may result in all anonymous access to the web site or FTP site being denied. If the web or FTP site depends on anonymous users accessing resources located on the network (rather than on the local IIS computer), you cannot use the password synchronization feature. Instead, specify a valid password for the anonymous user.

Basic Authentication (Password is sent in Clear Text)

Mark this checkbox, which is cleared by default, to enable Basic Authentication for the web site as a fallback method. The web site uses Basic Authentication only if anonymous access has been disabled, or with anonymous access enabled, if a user attempts to access content that is forbidden to anonymous users. When either of these conditions obtains, the user's web browser displays a dialog box to prompt the user to enter a valid Windows NT username and password, which is transmitted in unencrypted form, a potential security risk. ISM displays a warning dialog to that effect when you mark this checkbox. Users who log in with Basic Authentication must provide the logon domain in addition to the user name and password. By default, IIS uses the local IIS domain if the user does not enter a logon domain. You can change the default logon domain to other than the local IIS domain by clicking Edit and entering another domain name.

Windows NT Challenge/Response

Mark this checkbox, which is marked by default, to enable Windows NT Challenge/Response authentication, a more secure authentication method than the Basic Authentication described above. The web site uses Windows NT Challenge/Response Authentication only if anonymous access has been disabled, or with anonymous access enabled, if a user attempts to access content that is forbidden to anonymous users. When either of these conditions obtains, the user's web browser (which must be Microsoft Internet Explorer 2.0 or higher) displays a dialog box to prompt the user to enter a valid Windows NT username and password. During

this authentication process, the web server encrypts the exchanges required to authenticate the user.

Secure Communications section

You cannot use the secure communications features of the WWW Service until you have applied for, received, and installed a server certificate, and bound that certificate to the server key pair. Until you have taken these actions, the button in this section is labeled Key Manager. Clicking it displays Key Manager, which you use to create an SSL certificate request for this server. Once that certificate is installed and configured, the button in this section is relabeled Edit. Clicking it allows you to configure the SSL and PCT options on the server.

IP Address and Domain Name Restrictions section

You can use this section to deny all but specified IP addresses and/or domain names access to the web site. For example, if you have created a private web site that is intended for use only by your employees, you might use this feature to deny access to all users but those who are members of your own DNS domain. Alternatively, you can elect to grant all but specified IP addresses and/or domain names access to your web site. For example, if for some reason you decide that you don't want any user from the *aol.com* domain to access your web site, you can choose to deny that domain. To configure permit/deny settings, click Edit to display the IP Address and Domain Name Restrictions dialog, shown in Figure 10-9.

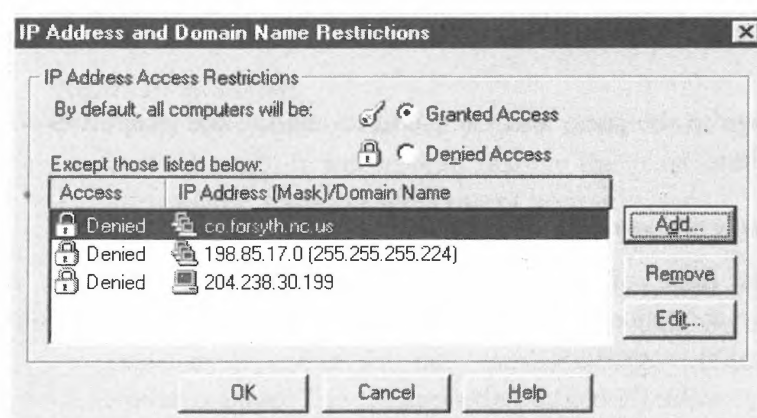


Figure 10-9. The IP Address and Domain Name Restrictions dialog

Begin by marking one of the option buttons at the top of the dialog to specify the default access. Mark the Granted Access option button if you want to grant access to all computers except those you enter in the list. Mark the Denied Access option button if you want to deny access to all computers except those you enter in the

list. Once you have specified the default access method, you may take the following actions to modify the list of computers that are granted or denied permission to access the site.

Add

Click this button to display the Deny Access On dialog (if you marked the Granted Access option button for default access) or Grant Access On dialog (if you marked the Denied Access option button for default access). Under Type, mark one of the following option buttons:

Single Computer

To display an IP address entry field in dotted decimal format. ISM enters a line item in the list that grants (or denies, as appropriate) access to this single computer.

Group of Computers

To display a Network ID entry box and a Subnet Mask entry box, both formatted as dotted decimal. Enter the network ID and subnet mask to grant or deny access to the specified subnet.

Domain Name

To display an entry box for domain name. Note that filtering by domain name is a very resource intensive option, because it requires a reverse DNS lookup for each operation.

Remove

Highlight the line item in the pane and click Remove to remove that grant or deny filter.

Edit

Highlight the line item in the pane and click Edit to change the properties for that grant or deny filter.

Configuring HTTP Headers properties

Use the HTTP Headers page of the Web Site Properties dialog, shown in Figure 10-10, to configure the values returned by the web site in the HTML header and to set content expiration properties.

Set the following options:

Enable Content Expiration section

Mark this checkbox, which is cleared by default, and set expiration options to control the display of time-sensitive content, for example, seasonal material or time-limited offers. The WWW Service embeds content-expiration data in content page HTTP headers. The client browser compares its current date with the expiration date supplied with the content to determine whether to display the

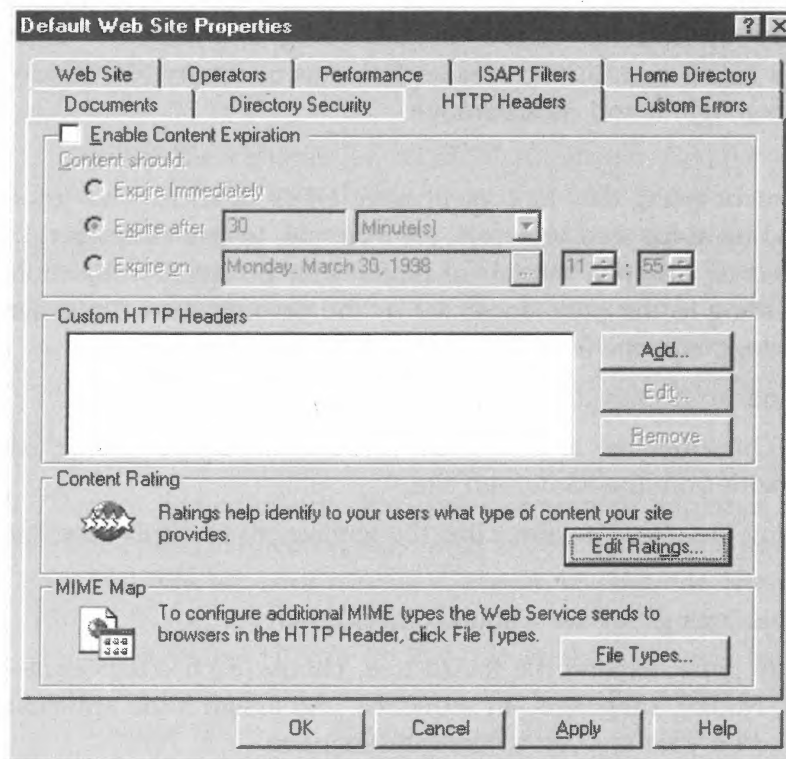


Figure 10-10. The HTTP Headers page

cached page or to request an updated page from the web server. If you enable content expiration, select one of the following option buttons:

Expire Immediately

Select this option button if you never want the browser to display a cached page. It will instead display the page only once, and then request an updated page on subsequent accesses.

Expire after

Select this option button, enter a number, and use the drop-down list to select minutes, hours, or days to specify that the browser may display this page from cache for the specified time period before requesting an updated page. The duration defaults to 30 minutes.

Expire on

Select this option button and enter a date and time to specify that the browser may display this page from cache until the specified date and time. The default value is 10 days since ISM was last started.

Custom HTTP Headers section

Use this section to enter custom headers that the web server will send to client browsers. To add a custom header, click Add to display the Add/Edit Custom Header dialog, and enter values for Custom Header Name and Custom

Header Value. To edit an existing custom header, highlight the custom header, click Edit to display the Add/Edit Custom Header dialog, and alter the values for Custom Header Name and Custom Header Value as necessary. To remove a custom header, highlight it and click Remove.

Content Rating section

IIS can embed content rating data in content page HTTP headers. This information can be read by some web browsers, for example, Internet Explorer 3.0 or higher, and used to suppress display of pages with potentially objectionable content, according to the preferences set by the browser user. To assign ratings to your content, take the following steps:

1. Click Edit Ratings to display the Content Ratings dialog.
2. Click Ratings Questionnaire to download the current version of the ratings questionnaire from the RSAC web site.
3. After completing the questionnaire, click the Ratings tab to display the Ratings page.
4. Mark the Enable Ratings for this resource checkbox.
5. In the Category pane, expand the RSACi tree, choose each component—Violence, Sex, Nudity, Language—in sequence, and assign it the appropriate rating based on your answers to the questionnaire.
6. In the Optional Information section, enter the email address of the person who rated the content and click Date to enter a date when the rating information expires.

MIME Map section

To change MIME mappings for this web site, click File Types to display the File Types dialog, and use this dialog to add, edit, or remove registered file types as described earlier in the section about configuring Master Properties. The mappings you modify here apply only to this web site. If you set MIME mappings in Master Properties, you can still modify the mappings on a site by site basis. However, when you reapply Master Properties, the individual per-site MIME mappings are overwritten by those contained in Master Properties.

Configuring Custom Errors properties

Use the Custom Errors page of the Web Site Properties dialog to configure the type of error message that the WWW Service returns to the client browser when an HTTP error occurs. For each HTTP 1.1 error, you can select among the following options:

Default

Display the default HTTP 1.1 error message, for example, “404—Object Not Found”. If you set an HTTP 1.1 error to use the default message, the contents of that error message are displayed in the Error Message pane. By default, IIS

displays default HTTP 1.1 error messages for 403;14 - Forbidden—Directory Listing Denied; 500—Internal Server Error; 501—Not Implemented; and 502—Bad Gateway.

File

Display the contents of an HTML-formatted file. For most HTTP 1.1 errors, Microsoft supplies a more informative friendly version to replace most default error messages. Each of these messages is contained in an HTML-formatted file that is named with the HTTP 1.1 error number. You can use these replacement error message files as is, modify them to suit you, or replace them with your own versions. If you set an HTTP 1.1 error to use a custom message from a file, the path and filename are displayed in the Error Message pane.

URL

Display the contents of the specified URL, which must be located on a local server. At first glance, this option appears to duplicate the functionality of the File option. However, it is intended for a different purpose. If you use static HTML files for error messages, always use the File option. Use the URL option only if you are using a custom ASP or ISAPI application to return dynamic error messages. If you do this, the application must set the HTTP header status appropriate for the error. Otherwise, the server will always return HTTP 1.1 status 200—OK. If you set an HTTP 1.1 error to use a custom message from a URL, the URL is displayed in the Error Message pane.

You can configure custom error messages at the web site, directory (physical or virtual), and file level. When you configure custom error messages, all lower entities inherit that list, which replaces the existing list rather than being merged with it.

To configure the error message for an HTTP 1.1 error, highlight the error in the Error Message pane, and click Edit Properties to display the Error Mapping Properties dialog, shown in Figure 10-11. Use the Message Type drop-down list to select Default, File, or URL. If you select Default, there are no further options to choose. If you select File, enter the path and filename of the custom error file in the File box, or click Browse to locate it. If you select URL, type the full URL in the URL box. After you complete your edits, click on OK to save the change and return to the Custom Errors page.

Creating Additional Web Sites

IIS can support multiple web sites on one computer. Each web site must be uniquely identified by a combination of IP address, host header name, and/or TCP port number, as follows:

IP Address

By far the cleanest method is to assign a unique static IP address to each web site and create a DNS entry for each. For example, we could assign the web

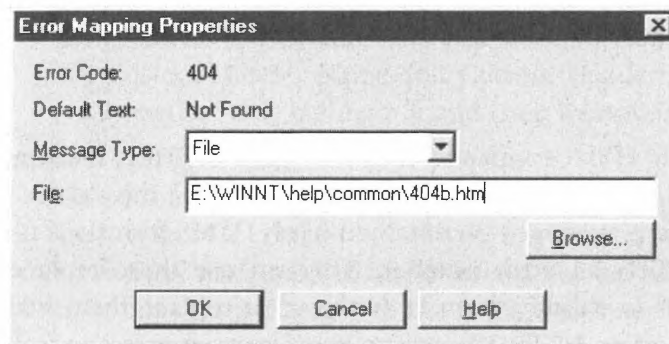


Figure 10-11. Configuring the error messages that will be returned by the server to clients when HTTP errors occur

site *www.ttgnet.com* the IP address 204.238.30.165 and the web site *support.ttgnet.com* the IP address 204.238.30.166, create CNAME records for each, and use the drop-down IP Address list on the Web Site page of the Web Site Properties dialog to associate each IP address with its corresponding web site. There is no ambiguity when a client browser attempts to access one of these sites, because the resolver stub in the browser uses the web site name to resolve a unique IP address for the web site.

Host header name

If you cannot assign a unique IP address to each web site—for example, if your ISP has given you only one static IP address—you can use the same IP address to support multiple web sites by assigning each web site a unique host header name. For example, *www.ttgnet.com* and *support.ttgnet.com* could both use the IP address 204.238.30.165. When a client browser requests either site, the request is directed to the same IP address, but IIS uses the host name requested by the client to determine which web site content to deliver. This method works with modern browsers, but fails with older browsers unless you take the steps described in the IIS documentation under “Supporting Host Header Names in Older Browsers”. To configure multiple web sites using host header names, use the Advanced button on the Web Site page of the Web Site Properties dialog to associate each web site with its corresponding host header name.

TCP Port number

As a last resort, you can define multiple unique web sites on an IIS server by assigning each web site the same IP address, but with a unique TCP Port number for each site. We say as a last resort, because every web browser on the planet assumes that a web site will respond to TCP Port 80, the Well-Known Address for HTTP. For a client browser to access a web site that uses a TCP Port number other than 80, the browser must explicitly enter the port number with the URL.

After you have decided how to identify the new site uniquely, take the following steps to create it:

1. Start ISM and highlight the IIS computer in the left pane.
2. Select Action → New → Web Site to invoke the New Web Site Wizard.
3. Enter a name for the new web site in the Web Site Description box and click Next. Note that the name you assign here is only the display name used by ISM. It need not be the same as the DNS name for the web site.
4. Use the Select the IP Address to use for this Web Site drop-down list to choose the IP address for the site, and enter the TCP Port number in the TCP Port this Web Site should use (Default: 80) box. If you have installed a server certificate and want to use SSL, enter the SSL port. Click Next.
5. Enter (or browse for) the home directory path for this web site. By default, the "Allow anonymous access to this web site" checkbox is marked. Clear it if you want to disable anonymous access and require anyone who wants to use the site to provide a valid username and password. Click Next.
6. Set the access permissions for the new web site. By default, only the "Allow Read Access" and "Allow Script Access" checkboxes are marked. The "Allow Execute Access (includes Script Access)", "Allow Write Access", and "Allow Directory Browsing" checkboxes are cleared. Once you have configured the access permissions, click Finish to continue.
7. ISM creates the web site and installs it in the tree for the computer. By default, the new web site is stopped. To start it, right click the new web site name in ISM to display the context sensitive menu and choose Start.
8. Use the Web Site Properties dialog for the new web site to make any configuration changes necessary.
9. Create a DNS CNAME entry for the new web site.

Creating an FTP Site

Like setting up a web site, setting up an FTP site with IIS is a two-step process. You first design your FTP directory structure, create the directory tree, and populate it with the files you want available for download. Once you have done so, you configure the properties for the FTP site that will make those files accessible to users. To create an FTP site based on the Default FTP Site that was installed when you installed IIS, take the following steps:

1. If you accepted the defaults when installing IIS, the Default FTP Site home directory is the `\inetpub\Ftproot` directory on the drive where you installed IIS. If the FTP site will have only a few files, you can copy them all to this

directory. If you will make many files available for download, create a subdirectory structure under the home directory and use it to organize the files.

2. Create a CNAME DNS entry to alias ftp to the computer name that runs IIS. For example, we installed IIS on the computer *bastet.ttgnet.com*. To allow DNS users to resolve the FTP site as *ftp.ttgnet.com*, we added a DNS entry to alias *ftp.ttgnet.com* to *bastet.ttgnet.com*. When a user enters *ftp.ttgnet.com* in his browser or FTP client, DNS resolves the request to the computer *bastet.ttgnet.com*.
3. Modify the Default FTP Site Properties dialog as necessary. Configuring FTP site properties is done with a tabbed dialog similar to that used to configure web site properties. It includes the following pages:

FTP Site

Configure identification, connection limits, and logging options for the FTP site.

Security Accounts

Configure anonymous connection options and specify which users and groups can perform routine administrative functions for the FTP site.

Messages

Configure the messages that FTP users will see when they connect to and exit the FTP site, and the message that the FTP server returns to clients who attempt to connect to it when the maximum number of concurrent connections has been exceeded.

Home Directory

Configure the location of or modify the properties for the home directory for the FTP site, and specify the type of directory listing—Unix or MS-DOS—that will be returned to FTP clients.

Directory Security

Configure TCP/IP access restrictions for the FTP site, to grant or deny access to particular IP addresses, subnets, or domain names.

Installing IIS4 using Typical installs a Default FTP Site. You can use the procedures described in the following sections to modify the properties for this site, as well as for other FTP sites you create. Changes you make to them affect only the individual FTP site you are changing. You can also use these same procedures to modify the Master Properties for the FTP Service, described earlier. Changes you make to the Master Properties for the FTP Service are used as default settings when you create a new FTP site, and may optionally be used to update (and overwrite) the properties for existing FTP sites.

You can designate one FTP site as the default FTP site for IIS 3.0 administration. Any software that creates virtual directories will use the designated default FTP site

as the target. To designate a default FTP site, right-click the computer name in MMC to display the context-sensitive menu and choose Properties to display the <computer-name> Properties dialog. In the Master Properties section, use the drop-down list to select FTP Service, and click Edit to display the FTP Service Master Properties for <computer-name> tabbed dialog. Click the IIS 3.0 Admin tab, and use the Default FTP Site drop-down list to select the default FTP site.

To change properties for an FTP site, right-click that web site in MMC to display the context-sensitive menu, and then choose Properties to display the tabbed <FTP-site-name> FTP Site Properties dialog.

Configuring FTP Site properties

Use the FTP Site page of the FTP Site Properties dialog to configure identification, connection limits, and logging options for the FTP site, and to view and manage connected users, as follows:

- FTP Site Identification section

Description

The name of the FTP site. This is what appears in Internet Service Manager tree view.

IP Address

Use the drop-down list to select an IP address to associate with the FTP site. Only IP addresses that have been assigned to this computer (using the Control Panel Network tool) appear in this list. If you accept the default setting for this field, All Unassigned, this web site responds to all IP addresses assigned to this computer that are not assigned to other sites.

TCP Port

Specifies the TCP port upon which the FTP Service responds to queries, by default port 21. You can specify any other TCP port number here, but clients must explicitly use that port number to access the FTP server. TCP Port number is required. If you change the TCP Port, you must restart the server before the change takes effect.

- Connections section

Unlimited

Mark this option button to allow unlimited simultaneous connections to the FTP site.

Limited To

Mark this option button, which is marked by default, and enter a value for connections to limit the number of simultaneous connections to the FTP site. By default, the concurrent connection limit is set to 100,000.

Connection Timeout

Specify, in seconds, how long the FTP server waits before disconnecting an inactive user. The default value is set to 900 seconds.

- Enable Logging section

Enable Logging

Mark this checkbox, which is marked by default, to cause IIS to log FTP user activities.

Active log format

If you enable logging, use the drop-down list to select one of the following log file formats. Once you have selected a format, click Properties to display a property sheet specific to that format, where you can set various logging options, including log time period, log file location, maximum log file size, items to be logged, and so on.

Microsoft IIS Log File Format

An ASCII log file format with predefined headings.

ODBC Logging

A fixed format logged to an ODBC-aware database, for example, Access or SQL Server. You must create the database yourself before data can be written to it. Using this format allows you to use the more powerful data analysis and reporting tools available with the database application.

W3C Extended Log File Format

The default log file format. W3C is a configurable ASCII format. By default, Time, Client IP Address, Method, URI Stem, and HTTP Status are logged. You can select among numerous other data types to be logged.

You can also use this page to view and manage active FTP sessions. To do so, click Current Sessions to display the FTP User Sessions dialog, shown in Figure 10-12. This dialog displays the total number of users currently connected to the FTP server and, for each connected user, the identity of the user (typically, that user's email address), the IP address from which the user is connected, and the elapsed duration of the connection.

This dialog presents a snapshot of the current sessions as of the time you display it rather than updating sessions dynamically. Use this dialog to perform the following activities:

- To update the current sessions list, click Refresh.
- To disconnect one user session, highlight that session and click Disconnect. ISM displays a warning message to notify you that you are about to terminate the session. Click Yes to terminate the session. When you terminate a session, the connected user does not receive any preliminary warning.

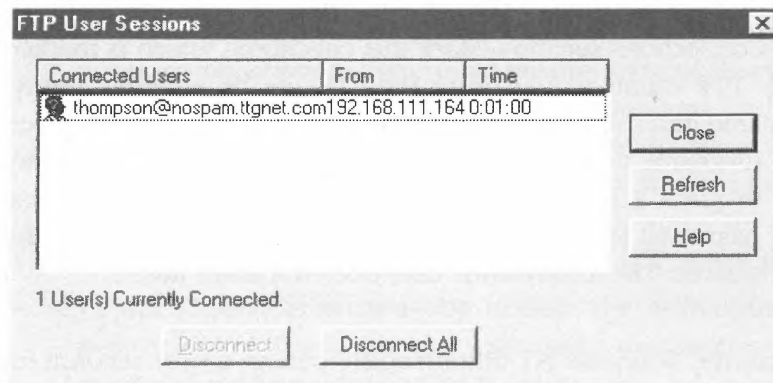


Figure 10-12. The FTP User Sessions dialog.

- To disconnect all user sessions, click Disconnect All. ISM displays a warning message to notify you that you are about to terminate all user sessions. Click Yes to terminate the sessions immediately.

Configuring Security Accounts properties

Use the Security Accounts page of the FTP Site Properties dialog, shown in Figure 10-13, to configure anonymous access options and to specify which users and groups can perform routine administrative functions for the FTP site.

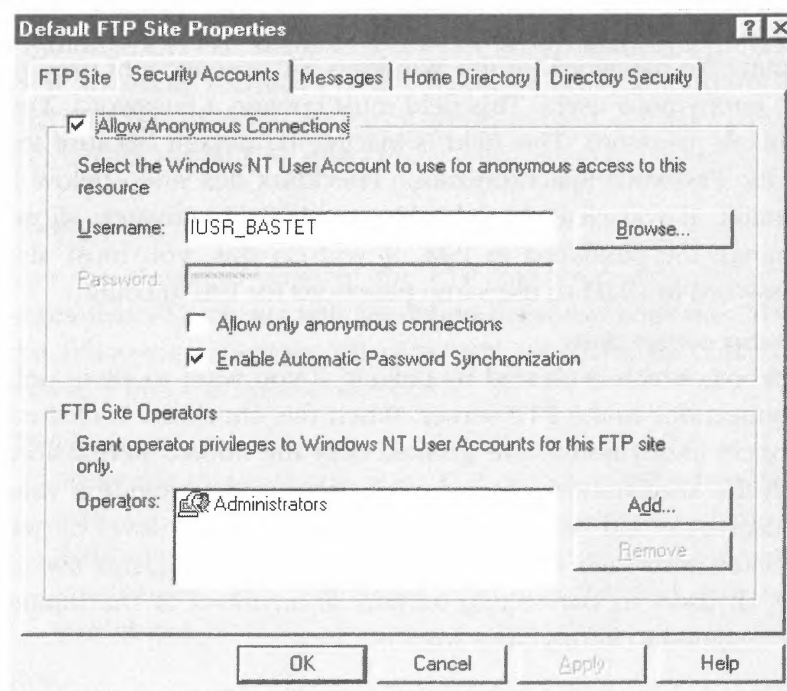


Figure 10-13. The Security Accounts page of the FTP Site Properties dialog

Configure the following settings:

- **Allow Anonymous Connections** section—Mark this checkbox, which is marked by default, to allow FTP clients to log on to the FTP site by entering anonymous as their username and their email address as the password. The FTP Service then uses the username and password described below as the Windows NT logon account to grant access to resources on the FTP server. Note that this username and password is only used internally by Windows NT to grant access to shared resources. The anonymous user does not enter them.

Username

When you install IIS, Windows NT automatically creates a user account for anonymous logons in User Manager for Domains and in Internet Service Manager, and assigns the same random password to each of them. By default, this account is given the name IUSR_<computer-name>, for example, IUSR_BASTET. When an anonymous user connects to the FTP server, the FTP Service uses this account to access shared Windows NT resources and to determine the permissions available to the anonymous user. To substitute an existing Windows NT user account as the anonymous logon account, click **Browse** to display the **Select Windows NT User Account** dialog and select the account you want to use for anonymous logons. This account must have the “Log on locally” user right, which normal user accounts do not have by default.

Password

This field contains the password for the Windows NT user account used to grant access to anonymous users. This field must contain a password. You cannot use a blank password. This field is inactive by default because the **Enable Automatic Password Synchronization** checkbox described below is enabled by default. If you clear that checkbox, this field activates, allowing you to change the password in ISM. If you do this, you must also change the password in UMD to the same password for this account.

Allow only anonymous connections

Mark this checkbox, which is cleared by default, if you want to allow only anonymous connections to the FTP server. When this checkbox is cleared, users who connect anonymously are granted only the limited permissions associated with the anonymous account, while users who provide a valid Windows NT username and password are granted the higher level of permissions associated with their own user accounts. By marking this checkbox, you limit all users to connecting as user anonymous at the limited privilege level assigned to anonymous logons.

Enable Automatic Password Synchronization

If you configure a different Windows NT user account to be used for anonymous logons, you must ensure that the password for this account is identical in both User Manager for Domains and Internet Service Manager. Mark this checkbox to cause ISM to automatically update the ISM password for the anonymous user account when that password is changed in UMD. This checkbox is marked by default if the account used for anonymous logons exists in ISM but not in UMD when that account is created.

- **FTP Site Operators section**—By default, the Administrators group is assigned operator status. However, you can assign any user or group as an operator. Assign and remove operators as follows:

Add an operator

Click on Add to display the Add Users and Groups dialog. Use the List Names From drop-down list to specify the domain from which the account is to be added. The Names pane lists the available users and groups. Double-click a user or group name to add it to the Add Names pane, and then click on OK. ISM adds the selected user or group to the Operators pane.

Remove an operator

Highlight the user or group name in the Operators pane and click Remove.

Granting operator status to a user or group grants privileges only for this FTP site. Note that only members of the Windows NT Administrator group can manage virtual FTP sites. Adding a user or group to the Operators pane does not enable them to manage virtual FTP sites.

Configuring Messages properties

Use the Messages page of the FTP Site Properties dialog to configure the messages that FTP clients will see when they visit your site. You can create or modify the following messages, all of which are blank by default, simply by typing the message into the appropriate box:

Welcome

Enter the message you want FTP clients to see when they first connect to your FTP site. It's a good idea to include the name of the site with the greeting. Nowadays, many sites use this message to display copyright information, legal disclaimers, and a warning that unauthorized access or use of the site is prohibited.

Exit

Enter the message you want FTP clients to see when they log off the server. Traditionally, you thank them for visiting the site and invite them to return soon—kind of like the Beverly Hillbillies.

Maximum Connections

If you restrict concurrent connections, enter the message you want FTP clients to see when they attempt to log on to the server when all available connections are already in use.

Configuring Home Directory properties

Use the Home Directory page of the FTP Site Properties dialog, shown in Figure 10-14, to change the location of or modify the properties for the home directory for the FTP site. Installing IIS creates the FTP root directory that you specify, ordinarily `\inetpub\ftproot`. You can use this dialog to change that location. This is a dynamic dialog, whose contents vary according to the option button you select in the top section, as follows:

A directory located on this computer

Select this option, which is the default, to use an FTP root directory on the local computer where you installed IIS. Use this page to specify the location, access permissions, and directory listing style for the local directory. Uses standard drive/directory syntax, for example, `C:\web\ftpfiles`.

A share located on another computer

Select this option to use an FTP root directory located on a network share, using UNC syntax in the form `\\servername\sharename`, for example, `\\bastet\ftpfiles`. When you enter the sharename, click **Connect As** to provide the username and password that will be used to access that share. The other settings are identical to those available when the FTP root directory is on the local computer.

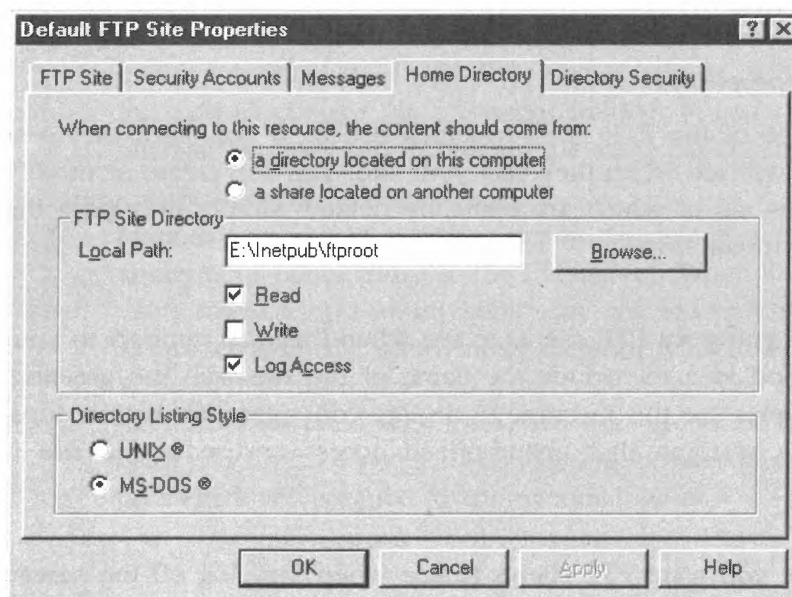


Figure 10-14. The Home Directory page of the FTP Site Properties dialog

Set the following options:

FTP Site Directory section

Local Path / Network Share

Type the drive and directory for the local path where the home directory resides on the local computer, or browse for the location. If you've chosen to locate the FTP root directory on a network share, enter the network share name here in UNC form, and click Connect As to enter the username and password for the account that will be used to access the share.

Read

Mark this checkbox, which is marked by default, to assign Read permission if you want FTP clients to be able to read or download the files contained in the home directory. This checkbox must be marked for FTP to be functional.

Write

Mark this checkbox, which is cleared by default, to assign Write permission if you want FTP clients to be able to upload files to the FTP site. Set this permission only for directories that are intended to receive uploaded files.

Log access

Mark this checkbox, which is marked by default, to cause the FTP Service to write a log file entry for each visit to this directory. For this setting to be effective, logging must be enabled for the FTP site in the FTP Site properties page, which it is by default.

Directory Listing Style section

Specify the directory listing style—Unix or MS-DOS—that the FTP Service will use when returning directory listings to FTP clients. Most modern FTP clients can accept either style, but some clients choke on MS-DOS style listings, so select Unix for maximum compatibility.

Configuring Directory Security properties

Use the Directory Security page of the FTP Site Properties dialog, shown in Figure 10-15, to grant or deny all but specified IP addresses and/or domain names access to the FTP site. For example, if you have created a private FTP site that is intended for use only by your employees, you might use this feature to deny access to all users but those who are members of your own DNS domain. Alternatively, you can elect to grant all but specified IP addresses and/or domain names access to your FTP site. For example, if a particular computer is downloading an excessive number of files from your FTP site, you can deny FTP access to that computer by IP address.

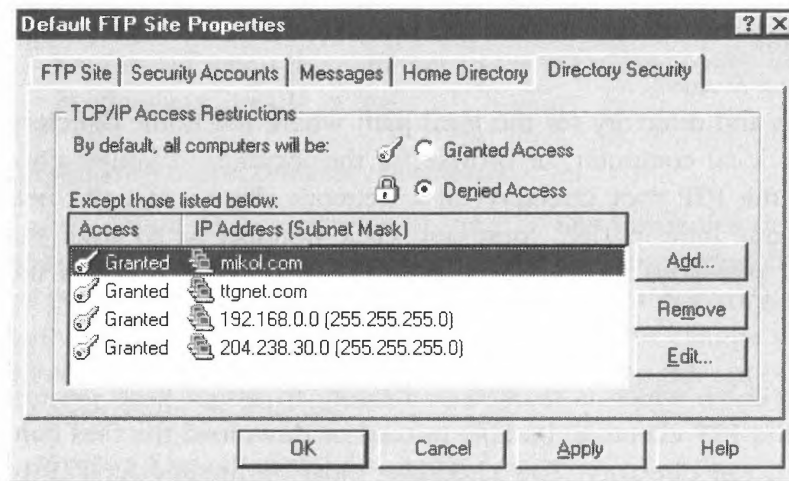


Figure 10-15. The Directory Security page of the FTP Site Properties dialog

Begin by marking one of the option buttons at the top of the dialog to specify the default access. Mark the Granted Access option button if you want to grant access to all computers except those you enter in the list. For a public FTP site, this is the proper choice. Mark the Denied Access option button if you want to deny access to all computers except those you enter in the list. For a private FTP site, this is the usual choice. Once you have specified the default access method, you may take the following actions to modify the list of computers that are granted or denied permission to access the site.

Add

Click this button to display the Deny Access On dialog (if you marked the Granted Access option button for default access) or Grant Access On dialog (if you marked the Denied Access option button for default access). Under Type, mark one of the following option buttons:

Single Computer

To display an IP address entry field in dotted decimal format. ISM enters a line item in the list that grants (or denies, as appropriate) access to this single computer.

Group of Computers

To display a Network ID entry box and a Subnet Mask entry box, both formatted as dotted decimal. Enter the network ID and subnet mask to grant or deny access to the specified subnet.

Domain Name

To display an entry box for domain name. Note that restricting access by domain name is a very resource intensive option, because it requires a reverse DNS lookup for each connection.

Remove

Highlight the line item in the pane and click Remove to remove that grant or deny filter.

Edit

Highlight the line item in the pane and click Edit to change the properties for that grant or deny filter.

Creating Additional FTP Sites

IIS can support multiple FTP sites on one computer. Each FTP site must be uniquely identified by either IP address or TCP port number, as follows:

IP Address

If possible, assign a unique static IP address to each FTP site and create a DNS entry for each. For example, we could assign the FTP site *ftp.ttgnet.com* the IP address 172.16.10.167 and the FTP site *files.ttgnet.com* the IP address 172.16.10.168, create CNAME records for each, and use the drop-down IP Address list on the FTP Site page of the FTP Site Properties dialog to associate each IP address with its corresponding FTP site. There is no ambiguity when an FTP client attempts to access one of these sites, because the resolver stub in the FTP client uses the FTP site name to resolve a unique IP address for the FTP site.

TCP Port number

If you cannot assign a unique IP address to the new FTP site—for example, if your ISP has given you only one IP address—you can define multiple unique FTP sites on an IIS server by assigning each FTP site the same IP address, but with a unique TCP Port number for each site. Use this method only if you must, because FTP clients assume that an FTP server will respond to TCP Port 21, the Well-Known Address for FTP. For an FTP client to access an FTP site using a nonstandard port number, that client must explicitly specify the port number to establish the connection.

After you have decided how to identify the new site uniquely, take the following steps to create it:

1. Start ISM and highlight the IIS computer in the left pane.
2. Choose Action → New → FTP Site to invoke the New FTP Site Wizard.
3. Enter a name for the new FTP site in the FTP Site Description box and click Next. Note that the name you assign here is only the display name used by ISM. It need not be the same as the DNS name for the FTP site.
4. Use the Select the IP Address to use for this FTP Site drop-down list to choose the IP address for the site, and enter the TCP Port number in the TCP Port this FTP Site should use (Default: 21) box. Click Next to continue.

5. Enter (or browse for) the home directory path for this FTP site. Click Next.
6. Set the access permissions for the new FTP site. By default, the Allow Read Access checkbox is marked and the Allow Write Access checkbox is cleared. Accept or modify the default access permissions and click Finish to continue.
7. ISM creates the FTP site and installs it in the tree for the computer. By default, the new FTP site is stopped. To start it, right click the new FTP site name in ISM to display the context sensitive menu and choose Start.
8. Use the FTP Site Properties dialog for the new FTP site to make any configuration changes necessary.
9. Create a DNS CNAME entry for the new FTP site.

Creating an SMTP Site

Installing IIS4 automatically installs the SMTP Site for the Microsoft SMTP Service. You cannot create additional SMTP sites, and you cannot delete the existing SMTP site. There is no SMTP Service selection in Master Properties, because the Default SMTP Site is the one and only SMTP site for the computer. You configure the SMTP Site using the SMTP Site Properties tabbed dialog, which includes the following pages:

SMTP Site

Configure identification, connection options, and logging options for the SMTP site.

Operators

Specify which users and groups can perform routine administrative functions for the SMTP site.

Messages

Limit maximum message and session sizes, set the maximum number of outbound messages per connection and the maximum number of recipients per message, and specify what actions the SMTP Service takes when a message cannot be delivered.

Delivery

Configure message queue options, domain options, smart host settings, and outbound security.

Directory Security

Configure settings for anonymous access and authentication, secure communications, IP address and domain name restrictions, and SMTP relay restrictions.

To change properties for the SMTP site, right-click the site entry in MMC to display the context-sensitive menu, and then choose Properties to display the tabbed

13

Information Resources

In this chapter:

- *The World Wide Web*
- *Anonymous FTP*
- *Retrieving RFCs*
- *Mailing Lists*
- *Newsgroups*
- *The White Pages*
- *Summary*

Now that our network is configured, debugged, and secure, how will we use it? The classic applications Telnet, FTP, and mail, are still popular. But increasingly the network is used not merely as a delivery link between two hosts, but as a path to information resources. Information servers, file repositories, databases, and information directories are available throughout the Internet.

An important application for these information resources is to keep you up-to-date about the latest developments in Windows NT and in TCP/IP network technologies. Computer technology changes very rapidly. The things that you read about in this book will surely change over time.* Online information can help you keep your knowledge current.

This chapter explores various ways to avail yourself of this storehouse of information. We look at how information is retrieved from network servers, and some tools that make it easier to locate that information.

The World Wide Web

The primary method used to retrieve network information is the World Wide Web. The Web is an interlinked network of hypertext servers based on the *Hypertext Transfer Protocol* (HTTP) that runs on top of TCP/IP. The Web is accessed via a *browser*, which is a program that provides a consistent graphical interface to the user. All of the popular browsers, including Microsoft Internet Explorer, are modeled after the original browser developed at the National Center for Supercomputer Applications (NCSA), and therefore share a common look and feel.

* We maintain a web site at www.ttnet.com/nttcp.html that contains online updates for this book and other useful information.

Windows NT systems ship with a built-in browser. The Microsoft Internet Explorer is bundled with the operating system. Other browsers are available on the Internet. The Netscape browser is available at <http://www.netscape.com>. It can be downloaded and quickly installed. Netscape is a popular browser, but Internet Explorer is probably the most popular browser for Windows NT.

You can, of course, also set up your Windows NT Server as a Web server. In this chapter we only look at browsing other services. To see how to set up your own service, refer to Chapter 10, *Internet Information Server (IIS)*.

Obtaining information from hypertext Web pages is a common use for a browser. Use yours to keep up with the most current network information. Figure 13-1 shows a network administrator checking online security information.

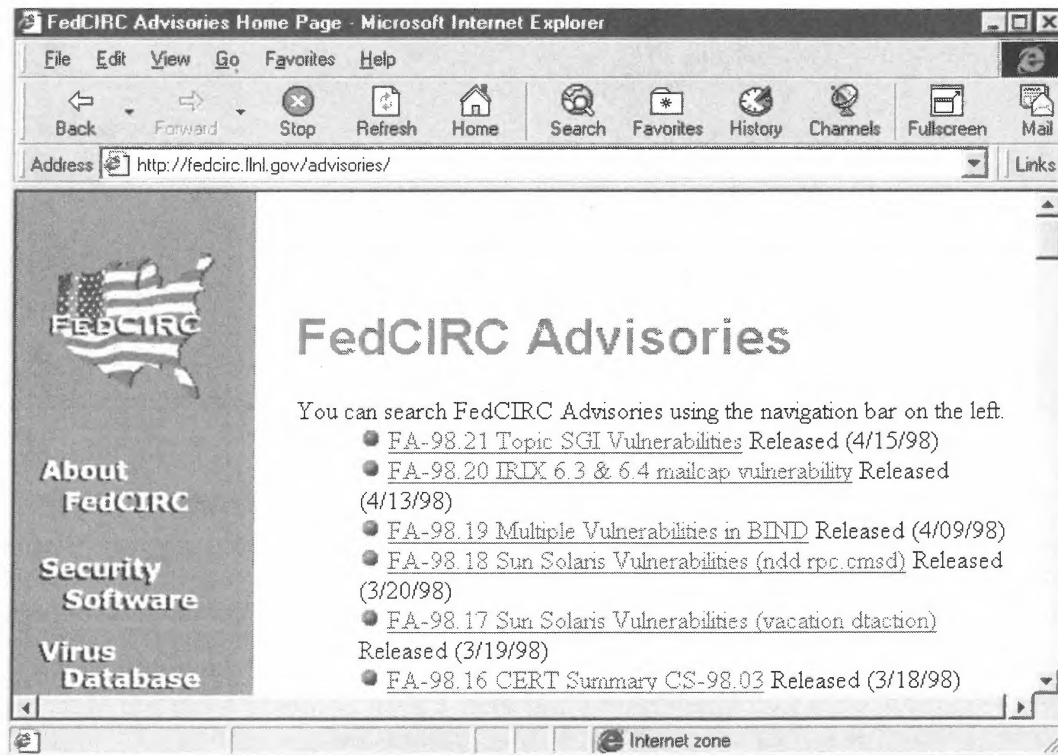


Figure 13-1. Obtaining information with the Web

The Address field near the top of the sample screen is the location of the Web page we are reading. On some other browsers this field is labeled URL, Location, or Netsite, but in all cases it performs the same function: it holds the path to the information resource. In the example the location is <http://fedcirc.llnl.gov/advisories/>. The Address is a *universal resource locator* (URL). It is a standard way of defining a network resource and it has a specific structure:

service://server/path/file

In the sample URL, *http* is the service; *fedcirc.llnl.gov* is the server; and *advisories* is the path to the resource contained on that server. No file name is provided, so the default file, usually *index.html*, is used. This tells the browser to locate a host with the domain name *fedcirc.llnl.gov*, and to ask it for the hypertext information located in the default file in the *advisories* path.

Hypertext is not the only type of information that can be retrieved by a browser. The browser is intended to provide a consistent interface to various types of network resources. HTTP is only one of the services that can be specified in a URL.

A web browser can be used to view local hypertext files. Increasingly this is how documentation is delivered. Figure 13-2 shows an NT administrator reading the mailsrv documentation.



Figure 13-2. Reading documentation with a browser

The URL in Figure 13-2 is *file:///c:/ntreskit/mailsrv/mailsrv.htm*. The service is *file*, which means that the resource is to be read via the standard file system. No server name is provided so the Internet Explorer looks for the resource on the local host. The path is *c:/ntreskit/mailsrv*, and the file is *mailsrv.htm*.

The browser is also often used to download files, a role that is similar to FTP. Figure 13-3 shows an NT administrator using a browser to download new Windows NT modem drivers.

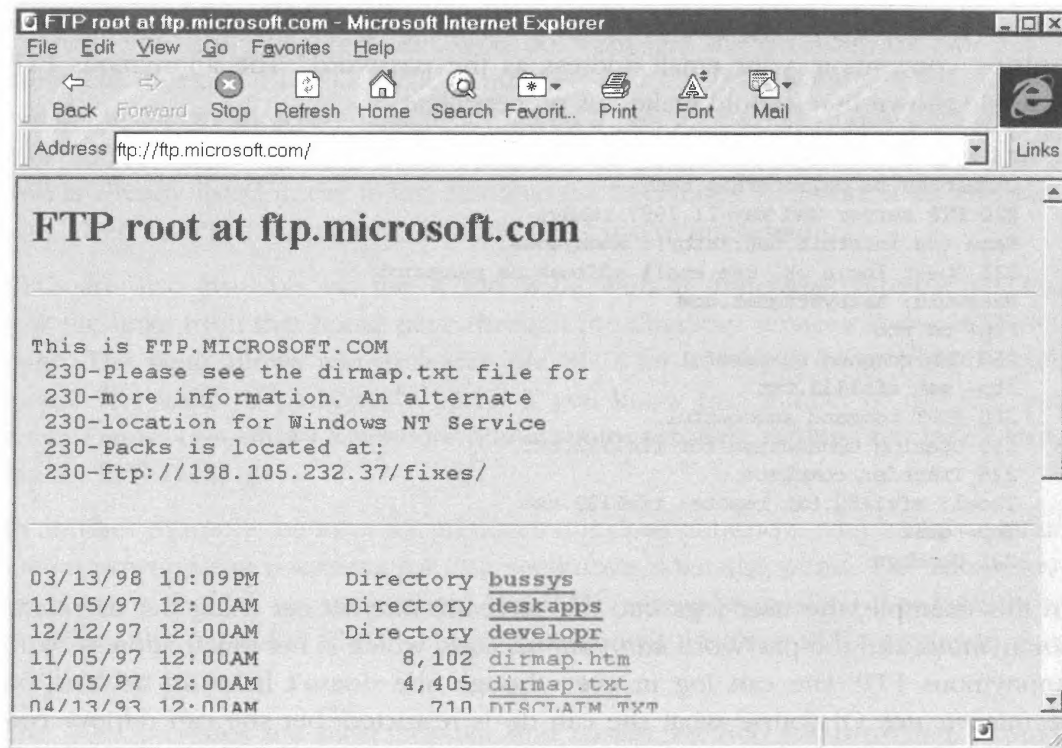


Figure 13-3. Using the Web for file transfer

The URL in Figure 13-3 shows HTTP being used to retrieve a file. FTP can also be the service used to access a resource through the browser. For example, *ftp://ftp.microsoft.com* connects to the anonymous FTP server at Microsoft. Files can be downloaded via HTTP or FTP.

Reading important announcements and documentation and downloading files are probably the most common uses a network administrator has for a Web browser. There are, however, many other things that can be done with a browser and the huge number of resources available on the network. A detailed discussion of browsers and the Web is beyond the scope of this book. See *The Whole Internet User's Guide and Catalog*, by Ed Krol, for a full treatment of these subjects.

The browser provides a consistent interface to a variety of network services. But it is not the only way, or necessarily the best way, to access all of these service. In particular, it may not be the fastest or most efficient way to download a file. An alternative is to invoke *ftp* directly.

Windows NT TCP/IP Network Administration

Hunt & Thompson



Windows NT TCP/IP Network Administration



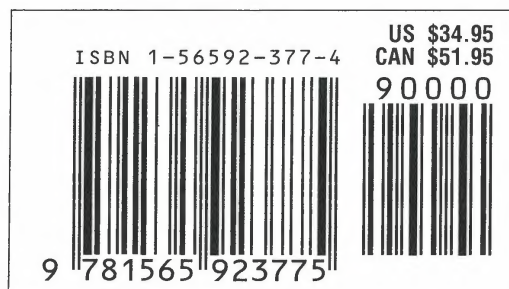
Windows NT TCP/IP Network Administration is a complete guide to setting up and running a TCP/IP network on Windows NT. Windows NT and TCP/IP have long had a close association, and this is the first book to focus exclusively on NT networking with TCP/IP. It starts with the fundamentals—what the protocols do and how they work, how addresses and routing move data through the network, and how to set up a network connection. Beyond that, all the important networking services provided as part of Windows NT—including IIS, RRAS, DNS, WINS, and DHCP—are presented in detail. This book is the NT administrator's indispensable guide.

Contents include:

- Overview
- Delivering the data
- Network services
- Getting started
- Installing TCP/IP
- Using Dynamic Host Configuration Protocol
- Using Windows Internet Name Service
- Using Domain Name System
- Microsoft RRAS
- Internet Information Service
- Troubleshooting TCP/IP
- Network security
- Information resources
- Appendixes on the PPP scripting languages, DNS resource records, Microsoft DHCP option support, and routing protocols

Craig Hunt is an expert on TCP/IP and the author of the bestseller *TCP/IP Network Administration*.

Robert Bruce Thompson is an expert on Windows NT and the author of several books on NT including the recently released *Windows NT Server 4.0 for NetWare Administrators*.



Visit O'Reilly on the Web at www.oreilly.com



RepKover™



Printed on Recycled Paper