



NAS 6000



Administration Guide
MaxAttach NAS 6000

MaxAttach NAS 6000 Installation and Configuration Guide

Document Revision Information

Document Title:	MaxAttach NAS 6000 Administration Guide
Part Number:	000001628
Corporation:	Maxtor Corporation
Product Name:	MaxAttach NAS 6000
Operating System:	Microsoft Windows-Powered Max Operating System Version 2.0
O/S Name Revision:	Max O/S 2.0
Manual Release Date:	11/07/01
Manual Revision:	Revision 2.0.03A
Change History:	Second Release - 2.0.04A - 11/07/01; First release - 2.0.03 - 10/16/01

Copyright and Trademarks

©2001 Maxtor Corporation. All Rights Reserved. Maxtor is a registered trademark of Maxtor Corporation. MaxAttach™ and MaxNeighborhood™ are trademarks of Maxtor Corporation. Other product names, company names, and logos are trademarks or registered trademarks of their respective owners.

Specifications Subject to Change

Specifications are subject to change without notice. Maxtor reserves the right to revise this publication and to make changes in the content hereof without the obligation of Maxtor to notify any person of such revision or changes.

Register Your System for On-site Support

Register now to activate on-site service for your Maxtor MaxAttach NAS 6000. We are pleased to provide standard Next Business Day on site service for your MaxAttach NAS 6000 and wish to ensure that your service is activated. If you have not already received a service activation contract from Maxtor, please contact 1-800-4MAXTOR or visit our web site at www.MaxAttach.com. Should you have any questions about activating your MaxAttach NAS 6000, please do not hesitate to contact us. Thank You

Worldwide Customer Support

Technical support is available worldwide.

United States	1-800-4MAXTOR	www.maxattach.com
United Kingdom, France, Italy, Spain, Portugal, and Denmark	+353 1 204 11 11 (Ireland)	EuroNSG@Maxtor.com
Germany	+49 (0) 89 96241919	EuroNSG@Maxtor.com
Asia Pacific	+852-2585-4500	ApacNSG@Maxtor.com

Max Attach NAS 6000 Administration Guide

Table of Contents

Chapter #1 - Installation - Rack Mounting Your NAS 6000	1
Chapter #2 - Overview - MaxAttach NAS 6000 Hardware	18
Chapter #3 - Overview - Microsoft Windows O/S Version 2.0	41
Chapter #4 - Overview - NAS 6000 Disk Array	116
Chapter #5 - O/S 2.0 - Network Configuration	131
Chapter #6 - O/S 2.0 - Disk and Volume Properties	168
Chapter #7 - Persistent Storage Manager	175
Chapter #8 - O/S 2.0 - Folders and Shares	184
Chapter #9 - O/S 2.0 - Users and Groups	222
Chapter #10 - O/S 2.0 - Maintenance	232
Chapter #11 - Appendix - Disk Array RAID Concepts	254
Chapter #12 - Appendix - SNMP	270
Chapter #13 - Appendix - Disk Drive Error Codes	277
Chapter #14 - Appendix - Disk Array Error Codes	280

Detailed Table of Contents

Who Should Use This Guide	xviii
How to Use This Guide.....	xviii
MaxAttach NAS 6000 Documentation.....	xviii
Quick Start Card	xix
Getting Started Documents	xix
Installation and Configuration Guide.....	xix
Release Notes	xix
Typographical Conventions	xix
Observing Notes, Cautions, and Warnings	xx
Notes	xx
Cautions	xx
Warnings	xx
Installation - Rack Mounting Your NAS 6000	1
Chapter Outline	1
User-Supplied Materials and Services	1
Install the Equipment Rack	2
Install the AC Power Strips	2
Mount the MaxAttach NAS 6000 Equipment Enclosures	2
Re-Seat All Hard Disk Drive Carrier Assemblies	3
Review the Connector Locations	3
Install the External SCSI Cables	4
Cabinet-Mount System or Single Base Unit Rack Mount System	5
SCSI Connections Between Base Unit and First Expansion Unit	5
SCSI Connections Between the First and Second Expansion Units	6
Install EMU Cables	7
EMU Cable on Base Unit Installation	7
DECISION POINT - Are there Expansion Units to Install?	8
EMU Cable Between Base Unit and First Expansion Unit	8
DECISION POINT - One or Two Expansion Units	8
EMU Cable Between First and Second Expansion Unit	8
Install Network and AC Power Cables	9
Network Connections.....	9
AC Power Connections.....	11
International AC Power Strip Solutions for Rack Mount Systems	12
Localized Internal AC Power Cords	12

Localized AC Power Strips/Blocks	13
Australia	13
Europe	14
Japan	15
United Kingdom	15
United States	16
Overview - MaxAttach NAS 6000 Hardware	18
Chapter Outline	18
System Features	18
Overview	19
Cross-Platform File Sharing	20
Enclosure Configuration Options	20
Rack Mount Systems	21
Cabinet Mounted System	21
Major Components of the Maxtor MaxAttach NAS 6000	22
Base Unit Front Panel	23
Base Unit Front Panel Status LEDs	24
Overview	24
Front Panel LEDS	25
Hard Disk Drive Module Status LEDs	26
Power Supply Status LEDs	26
LCD Alert Panel	27
Logo and Alert Message Display Area	28
Network Information Display Area	29
Status Icon Display Area	29
Base Unit Back Panel	31
Expansion Unit	31
Expansion Unit Front Panel	31
Expansion Unit Back Panel	32
Description of System Components	32
Power Supply Modules	33
Disk Drive Carriers	33
CPU I/O Panel	34
CPU Ethernet Port	35
Network Interface Cards (NICs)	35
Hot Swappable Fans and Blower	36
SCSI Interface Connectors to Optional Expansion Enclosures	39
Environmental Monitoring Unit (EMU) Connectors	39
Overview - Microsoft Windows O/S Version 2.0	41
Chapter Outline	41
O/S Overview	42
Navigation Overview	42
Welcome Page	43
Take a Tour	43
Initial System Settings	44
Set Server Appliance Name	44

Set Administrator Password	45
Set Default Page	45
System Status Summary	46
Status Page	46
System Summary Page	46
System Health Page	47
Installed Software Elements	48
Windows System Files Page	48
Export SysInfo Page	49
Network Configuration	49
Network Page	50
Identification Page	50
Global Settings Page	53
Interfaces Page	57
Administrator Account Page	61
Administration Web Site Properties Page	62
SNMP Service Configuration Page	63
Telnet Page	63
NIC Configuration Page	64
Base Unit Network Port	65
Standard NIC Configuration	65
Gigabit Ethernet NIC with Copper Connections	67
Gigabit Ethernet NIC with Fiber Optic Connections	67
Disks and Volumes	70
Disks Page	70
Disks and Volumes	71
Disk Quotas Page	71
Persistent Storage Manage Page	74
Disk Defragmenter Page	80
Users and Groups	81
Users Page	81
Local Users Page	81
Local Groups Page	83
Local Groups Members Page	84
Folders and Shares	85
Shares Page	85
Volumes Page	85
Folders Page	86
Shared Folders Page	87
Shared Properties - General Tab	88
Sharing Protocols Page	93
AppleTalk Service Properties Page	93
FTP Service Properties Page	94
HTTP - Hypertext Transfer Protocol Service Properties Page	96
NetWare Protocol Service Properties Page	97
NFS Protocol Properties Page	97
Maintenance Page	99

Software Update Page	100
Date and Time	101
Shutdown	101
Logs	101
Backup Page	103
Terminal Services	103
Alert Email	105
Language Page	106
System Recovery Option Page	107
Session Timeout Options Page	107
Re-Image System Drive Page	109
Services for UNIX	110
Overview	110
NFS Client Groups	110
NFS Locks	111
User & Group Mappings	111
Services for Netware	114
Overview	114
NetWare Users	114
Help Pages	115
Overview - NAS 6000 Disk Array	116
Chapter Outline	116
Standard Disk Array Configuration	116
Disk Drive Array Organization	118
Logical Drive Organization	119
SCSI Channel Structure	120
Notes on SCSI Channels	121
SCSI Bus and Target LUN IS Assignments	121
RAID Array Organization	122
Base Unit Operating System Arrays	124
Drive C:\	124
Drive D:\	124
Base Unit User Data Arrays	125
Drive E:\	125
Drive F:\	125
First Expansion Unit User Data Arrays	126
Drive G:\ and Drive H:\	126
Second Expansion Unit User Data Arrays	126
Drive I:\ and Drive J:\	127
Re-Configuring Your MaxAttach NAS 6000 Drive Arrays	128
Best Practices	128
O/S 2.0 - Network Configuration	131
Chapter Outline	131
Network Configuration Overview	131
Network Identification	132
Server Appliance Name	134

Domain	134
Workgroup	135
Network Global Settings	136
DNS Name Resolution	137
Name Resolution Systems	138
DNS Configuration	138
TCP/IP Hosts	140
NetBIOS LMHOSTS File	141
Guidelines for LMHOSTS Files	143
IPX Settings	144
Network Adapter Interface	145
Configuring a Network Adapter	145
Renaming a Connection	146
AppleTalk Local Area Network Connection	146
Configuring an AppleTalk Network Connection	146
IP Address Configuration	147
Changing IP General Tab Settings	147
Changing IP Settings on the Advanced Tab	148
Changing Gateway Address Settings	149
DNS Configuration	149
Obtaining IP Address from DHCP Server	150
Manually Setting DNS Server to Use	150
WINS Configuration	151
Changing WINS Settings	152
Administrator Account and Password	152
Changing Administrator Account Password	153
Changing Administrator Account Name	154
Administration Web Site	154
Changing Administration Web Site Properties	155
Telnet	155
Configuring System for Telnet Administration	155
Network Adapter Interfaces	156
Configuring Network Adapters	156
Renaming a Connection	157
Apple Talk Local Area Network Connection	157
IP Address Configuration	158
DNS Configuration	160
WINS Configuration	161
Change Administrator Password	162
Administration Web Site	164
Telnet	165
Network Interface Cards	166
Standard Configuration	166
Base Unit Network Port	166
Simple Network Management Protocol - SNMP	166
O/S 2.0 - Disk and Volume Properties	168
Chapter Outline	168

Disks and Volumes	168
Disk Quota Management	168
Enabling Quota Management	169
Quota Entries	170
Adding Quota Entries	171
Removing Quota Entries	171
Modifying Quota Properties	172
Persistent Storage Manager and Images	174
Persistent Storage Manager	175
Chapter Outline	175
Persistent Storage Manager Introduction	175
Persistent Storage Manager and Images	176
Using Persistent Storage Manager	176
Persistent Image Scheduling	176
Disaster Recovery	176
Administration	176
Setting Up Persistent Storage Manager	177
Persistent Storage Manager Configuration	177
Configuration Fields	177
Managing Persistent Storage Manager Schedules	178
Working with Persistent Images	178
Creating a New Persistent Image	178
Deleting a Persistent Images	179
Undoing Persistent Image Writes	179
Editing Persistent Image Properties	179
Context of Persistent Image Groups	180
Group Page Field Definitions	180
Managing Persistent Image Schedules	180
Adding Persistent Image Schedule Items	181
Deleting a Persistent Image Schedule	181
Editing Persistent Image Schedule Properties	182
Disaster Recovery	182
Restoring a Volume Set from a Persistent Image	183
O/S 2.0 - Folders and Shares	184
Chapter Outline	184
Overview of Supported Protocols	185
Supported Protocols	185
Microsoft Windows File Sharing Overview	186
Manual Caching for Documents	186
Automatic Caching for Documents	186
Automatic Caching for Programs	186
Network File System (NFS) Overview	187
File Transfer Protocol (FTP) Overview	188
Web Hypertext Transfer Protocol (HTTP) Overview	188
NetWare Sharing Protocol Overview	189
AppleTalk Protocol Overview	189

Managing Folders	190
Sharing Folders	191
Navigating Through Folders	191
Adding a Folder	192
Removing a Folder	193
Opening a Folder	193
Modifying Folder Properties	194
Sharing a Folder	195
Managing Shares	196
Adding a Share	196
Removing a Share	197
Modifying Share Properties	197
Setting Windows CIFS Share Properties	198
Setting NFS Share Properties	199
Setting FTP Share Properties	200
Setting Web HTTP Share Properties	201
Setting NetWare Share Properties	202
Setting AppleTalk Share Properties	203
Managing Sharing Protocols	205
Enabling Sharing Protocols	205
Disabling Sharing Protocols	206
Configuring Sharing Protocol Properties	206
NFS Sharing Protocol	207
Setting NFS Sharing Protocol	207
Adding NFS Client Groups	207
Editing NFS Client Groups	208
Removing NFS Client Groups	209
Setting NFS Locks	209
NFS Protocol with User and Group Mappings	210
Setting NFS User and Group Mappings	210
Enabling Simple NFS Maps	212
Configuring Explicit User NFS Maps	213
Configuring Explicit Group Maps	215
FTP Sharing Protocol	216
Setting FTP Sharing Protocol	216
Enabling FTP Logging	217
Enabling FTP Anonymous Access	217
Disabling FTP Anonymous Access	218
Adding Custom FTP Messages	218
Web HTTP Sharing Protocol	219
Setting Web HTTP Sharing Protocol	219
NetWare Sharing Protocol	220
Setting NetWare Sharing Protocol	220
AppleTalk Sharing Protocol	221
Setting AppleTalk Sharing Protocol	221
O/S 2.0 - Users and Groups	222
Chapter Outline	222

Users and Groups	222
Manage Local Users	223
Adding a User Account	223
Enabling the Guest Account	224
Removing a User Account	225
Setting a User Password	226
Modifying User Properties	226
Manage Local Groups	228
Adding a Group Account	228
Removing a Group Account	229
Modifying Group Properties	230
O/S 2.0 - Maintenance	232
Chapter Outline	232
Software Update	233
Setting Date and Time	233
Shutting Down the System	233
Add or Remove Programs	234
Automatic System Backup Schedule	236
Changing the Automatic Backup Schedule	236
Disabling the Automatic Backup Schedule	236
Manual Back Up	237
Re-Image System Drive	238
Set Session Timeout	238
Setting Alert E-Mail	239
Backing up and Restoring the O/S	240
Terminal Services Client	241
Using the Clipboard During Terminal Server Sessions	243
Local Printing During Terminal Server Sessions	243
Automatic Printer Redirection	243
Manual Printer Redirection	244
To Close the Client	244
Logs	245
Managing Application Logs	245
Managing FTP Logs	246
Managing NFS Logs	246
System Log	247
Security Log	247
Managing Web HTTP Shares Logs	248
Managing Web Administration Logs	248
Clear Log Files	249
Download Log Files	250
Modify Log Properties	251
View Log Entry Details	252
Global Array Manager Overview	252
Appendix - Disk Array RAID Concepts	254
Chapter Outline	254

Introduction	255
RAID - Redundant Array of Independent Disks	255
RAID Introduction and Overview	255
Key RAID Technical Methods	256
Hardware RAID and Software RAID	256
Striping	256
Mirroring	256
Parity Checking	257
RAID and JBOD Types	257
RAID 0 Striping	258
Description	258
Fault Tolerance Cost	258
Performance	258
Application Focus	258
Array Size	258
RAID 1 Mirroring	259
Description	259
Fault Tolerance Cost	259
Performance	259
Application Focus	259
Array Size	259
RAID 0 +1 Mirrored Sets of Striped Drives	260
Description	260
Fault Tolerance Cost	260
Performance	260
Application Focus	260
Array Size	260
RAID 5 Multiple Disk Striping with Distributed Parity	261
Description	261
Fault Tolerance Cost	261
Performance	262
Array Size	262
JBOD Just a Bunch of Disks Single Disk Control	263
Description	263
Fault Tolerance Cost	263
Performance	263
Array Size	263
RAID Benefits Comparison	263
RAID Functional Comparison	264
RAID Fault Tolerance Characteristics	265
RAID and Obtaining Maximum Performance	265
Maxtor MaxAttach NAS 6000 RAID Operations and the GAM	266
Normal Array Status	266
Critical Array Status	266
Hot Swap Drives	266
Hot Spare Drives	267
Comparison of Terms	268

Volume Set	269
Logical (System) Drives	269
System Drives	269
Appendix - SNMP	270
Chapter Outline	270
Overview	270
MaxAttach SNMP Alert Overview	270
SNMP Management System	271
SNMP Agent	271
MaxAttach and Windows 2000 as SNMP Agents	271
Respond Only To Queries	271
SNMP Community	271
Management Information Base	272
Configuring SNMP Service	272
MaxAttach SNMP Specifications	272
MIB File Locations and Types	273
Windows 2000 Server SNMP MIBs	273
MIB Specifications	274
MaxAttach NAS 6000 SNMP MIB	274
MaxAttach NAS 6000 Series MIB Variables	274
MaxAttach NAS 6000 Series MIB Tree	275
MaxAttach SNMP Traps	276
Appendix - Disk Drive Error Codes	277
Mylex Disk Drive Failure Error Codes	277
Appendix - Disk Array Error Codes	280
Error Codes Overview	280
Mylex Severity Levels	280
O/S Error Processing	280
Listing of SupportedEvents.Inf	281
Instructions to Turn Amber Disk Status LEDs Off	281
Instructions to Turn Amber Disk Status LEDs On	281
Viewing and Changing Error Codes	282
Error Codes - EVENTDEF.TXT	283
Mylex Error Codes Table	283

List of Procedures

Installation - Rack Mounting Your NAS 6000	1
Overview - MaxAttach NAS 6000 Hardware	18
Overview - Microsoft Windows O/S Version 2.0	41
Overview - NAS 6000 Disk Array	116
To see total system space and total space used	116
To see total system space for each volume or logical drive	117
To re-configure the disk RAID arrays	129
O/S 2.0 - Network Configuration	131
To set the name and domain membership of the server appliance	132
To set the default domain used for logon	135
To set or change the workgroup membership of the server appliance	136
To automatically set or change DNS suffixes	136
To manually add specific DNS suffixes	137
To manually remove specific DNS suffixes	137
To set the server appliance to automatically obtain DNS server information from a DHCP server	139
To manually set the DNS servers to be used by the server appliance	139
To edit the Hosts file	141
To edit the LMHOSTS file	144
To configure the IPX address	144
To configure a network adapter	145
To rename an interface connection	146
To configure a network interface for AppleTalk	146
To set or change the IP settings on the General tab	147
To set or change the IP settings on the Advanced tab	148
To set or change the gateway address settings	149
To set the server appliance to automatically obtain DNS server information from a DHCP server	150
To manually set the DNS servers to be used by the server appliance	150
To change the WINS settings	152
To change the administrator account password	153
To change the administrator account name	154
To change the administration web site properties	155
To configure the MaxAttach NAS 6000 for Telnet administration	155
To configure a network adapter	156
To rename an interface connection	157
To configure a network interface for AppleTalk	157

To set or change the IP settings on the General tab	158
To set or change the IP settings on the Advanced tab	158
To set or change the gateway address settings	159
To set the server appliance to automatically obtain DNS server information from a DHCP server	160
To manually set the DNS servers to be used by the server appliance	160
To change the WINS settings of the server appliance	162
To change the administrator account password	163
To change the administrator account name	164
To change the administration web site properties	165
To configure your NAS 6000 appliance for Telnet administration	165
O/S 2.0 - Disk and Volume Properties	168
To enable or disable quota management on a volume	169
To set or change quota entries on the server appliance	170
To add a new quota entry	171
To allow unlimited disk use	171
To limit disk space	171
To remove a quota entry	171
To modify the properties of a quota entry	172
To allow unlimited disk use	172
To limit disk space	172
To modify the properties of multiple quota entries	173
To allow unlimited disk use	173
To limit disk space	173
Persistent Storage Manager	175
To create a new persistent image	178
To delete a persistent image	179
To undo persistent image writes	179
To edit persistent image properties	180
To work with schedule items	181
To add a persistent image to the schedule	181
To delete a persistent image schedule	181
To edit persistent image schedule properties	182
Using disaster recovery	182
To restore volumes from a persistent image	183
O/S 2.0 - Folders and Shares	184
To share folders	191
To manage folders	191
To navigate among folders	192
To create a new folder	192
To delete folders	193
To open a folder	193
To change the name of a folder	194
To compress a folder	194
To share a folder	195
To add a share	196

To remove a share and all its protocols	197
To remove specific protocols	197
To modify share properties	197
To set the user limit	198
To set user or group permissions	198
To add a new NFS client or client group to a share	199
To add an existing NFS client or client group	199
To remove an NFS client	200
To allow clients permission to an FTP share	200
To log client visits to an FTP share	201
To allow clients permission to a Web share	201
To set NetWare sharing properties	202
Setting AppleTalk Sharing Properties	203
To enable a sharing protocol	205
To disable sharing protocols	206
To configure network protocol properties	206
To configure the NFS protocol	207
To add an NFS client group	207
To add members to an NFS client group	208
To remove members to an NFS client group	208
To remove an NFS client group	209
To manage NFS locks	210
To map NFS users and groups	211
To configure for using an NFS server	211
To configure for using password and group files	211
To enable simple NFS maps	212
To create explicit user NFS maps	213
To set one of the NFS mappings as primary for a given user	214
To delete explicit user maps	214
To create explicit group maps	215
To set one of the mappings as the primary maps for a given group	216
To delete explicit group maps	216
To enable FTP logging	217
To enable FTP Anonymous	217
To disable FTP anonymous	218
To add custom messages	218
To configure Web (HTTP) sharing properties	220
O/S 2.0 - Users and Groups	222
To add a user account	224
To enable the guest account	225
To remove user accounts	225
To set the user password	226
To access user properties	226
To add a group account	228
To remove a user account	229
To set or modify a group name or description	230

To set or modify group membership	230
To add a new member:	230
To remove a member	231
O/S 2.0 - Maintenance	232
To update the software	233
To set the date, time, and time zone	233
To shut down or restart the system	234
To schedule a shutdown or restart	234
To remove a program	235
To add a program or driver	235
To change the automatic backup schedule	236
To disable the automatic backup schedule	236
To immediately back up the system	237
To set the session timeout interval	239
To set the alert e-mail feature	239
To back up or restore the OS	240
To connect to Terminal Services	241
To check the Terminal Services Client version	242
To use shortcut keys	242
To disconnect without ending a session	244
To log off and end a session	245
To manage application logs	246
To manage FTP logs	246
To manage NFS logs	247
To manage system logs	247
To manage security logs	248
To manage Web (HTTP) shares logs	248
To manage Web administration logs	249
To clear application, NFS, security, or system logs	249
To clear FTP, Web administration, or Web (HTTP) shares logs	249
To download application, security or system logs	250
To download NFS logs	250
To download FTP, Web administration, or Web (HTTP) shares logs	251
To modify the properties of a log file	251
To view the details of a log file	252
To start the Global Array Manager:	253
Appendix - Disk Array RAID Concepts	254
Appendix - SNMP	270
To configure the SNMP service	272
Appendix - Disk Drive Error Codes	277
Appendix - Disk Array Error Codes	280
To change an error code description	282

Preface

Who Should Use This Guide

This Administration Guide is designed as a comprehensive technical reference for the MaxAttach NAS 6000 system including hardware and software. It assumes that you are highly familiar with networking and system administration basics, that you have read through the Installation and configuration Guide, and that you have your MaxAttach NAS 6000 running on your network.

The primary purpose of this guide is to support you in performing long term administration, configuration, and maintenance on your MaxAttach

How to Use This Guide

Use this guide to provide reference material for installation and administration specific issues.

The first chapter covers rack mount installation details.

The next three chapters provide an in-depth overview description of the MaxAttach NAS 6000 hardware, operating system, and disk arrays.

The balance of the regular chapters each focus on specific O/S functions such as Networking or User and Groups.

This guide concludes with appendices that cover disk array basics, SNMP, and additional reference information for the RAID controller.

MaxAttach NAS 6000 Documentation

Other documentation available on your CD-ROM disk includes the documents described below.

Quick Start Card

This document is especially targeted towards single MaxAttach NAS 6000 Base Unit cabinet mounted or rack-mountable systems where quick plug and play is the goal.

Getting Started Documents

The *Getting Started* series of documents are longer than the *Quick Start Card*, but strive to provide you with the minimum necessary information to unpack, assembly, install, launch, and disk array configure a specific MaxAttach NAS 6000 system configuration.

Each document is targeted at different system and provides just the information required to get it on your network and ready for use or advanced configuration. If needed, the document includes quick step-by-step instructions on how to configure the disk arrays into the factory default configuration. Each document includes all the information needed to get a specific configuration installed and running. The *Getting Started* series documents are:

- *Getting Started for Cabinet Systems*
- *Getting Started for Base Only Rack Mount Systems*
- *Getting Started for Base Plus Systems*
- *Getting Started for 48" Cabinet Rack Systems*
- *Getting Started for 84" Cabinet Rack Systems*
- *Getting Started for Disk Array Configuration*

Installation and Configuration Guide

The *Installation and Configuration Guide* is targeted at getting your NAS 6000 rack installed, cabled, identified on the network, and available on your network with a minimum of configuration steps. It concludes with disk array management suggestions and instructions on how to configure your disk arrays into the factory suggested RAID 5 arrays.

Release Notes

For the latest in developments on your MaxAttach NAS 6000, be sure to review the *Release Notes* document (in paper) that was included with your shipment.

Typographical Conventions

The following typographical conventions are used in this guide to help you locate and identify information:

- *Italic text* is used for emphasis and book titles.
- **Bold text like this** identifies menu names, menu options, items you can click on the

screen, and keyboard keys.

- **Courier font** identifies file names, folder names, text that either appears on the screen or that you are required to type in, or listings of programs or output reports.

Observing Notes, Cautions, and Warnings

The following text types call out special attention to important parts of this manual. They always appear before the actual text.

Notes

Notes provide extra information, tips, and hints regarding the topic.



NOTE

Notes provide extra information, tips, and hints regarding the topic.

Cautions

Cautions identify important information about actions that could result in damage to data or loss of data or could cause the system to behave in unexpected ways.



CAUTION

Cautions identify important information about actions that could result in damage to data or loss of data or could cause the system to behave in unexpected ways.

Warnings

Warnings identify critical information about actions that could result in unexpected equipment failure, loss of critical operating system files, or potential bodily injury.



WARNING

Warnings identify critical information about actions that could result in unexpected equipment failure, loss of critical operating system files, or potential bodily injury.

Chapter #1 - Installation - Rack Mounting Your NAS 6000



NOTE

If you have a cabinet-mounted version of the MaxAttach NAS 6000, skip this section and continue with the next chapter.

Chapter Outline

This chapter provides an in depth description of installation requirements for MaxAttach NAS 6000 rack-mountable systems. It also describes how to get your MaxAttach NAS 6000 mechanically ready by performing the following tasks:

- Install the user-supplied equipment rack.
- Install the user-supplied AC power strips.
- Install all MaxAttach equipment enclosure shelves into the rack.
- Install the MaxAttach SCSI connector cables for the hard disk drives.
- Install the MaxAttach Serial Port connector cables for the Environmental Monitoring Unit (EMU).
- Install the Ethernet Network Interface Card (NIC) cables between the MaxAttach NICs and your network.
- Prepare the MaxAttach for power up.

1: User-Supplied Materials and Services

The following user-supplied materials are required:

- A standard 19" equipment rack.
 - The minimum rack vertical size depends on the configuration of your MaxAttach.

- A Single Base Unit Enclosure requires four rack spaces (4U) with a size of 7”H x 19”W x 22”D - 17.7cmH x 48.2cmW x 55.8cmD.
- A Base Unit Enclosure and one Expansion Enclosure requires 8U with a size of 14”H x 19”W x 22”D - 35.5cmH x 48.2cmW x 55.8cmD.
- A Base Unit Enclosure with two Expansion Enclosures requires 12U with a size of 21”H x 19”W x 22”D - 53.3cmH x 48.2cmW x 55.8cmD.
- Two standard AC power strips.
 - At least three power outlets per strip are required.
 - More sockets per strip are recommended.
 - Minimum rating for US installations is 120 VAC at 15 Amps.
- At least two network cables of sufficient length to reach from the MaxAttach to your network.
 - Two cables are required if you only want to use the card cage mounted Ethernet Gigabit NICs.
 - An additional CAT-5 cable is required if you also want to use the CPU Motherboard Ethernet port.
 - At least one network connection is required.

2: Install the Equipment Rack

Follow the manufacturer’s installation recommendations for rack installation. Make sure the unit is securely fastened to permanent fixtures such as the floor or overhead support.

3: Install the AC Power Strips

Install the AC power strips on either side of the rack. They must be close enough to the rack for the Maxtor-supplied power cords to reach from the enclosure power supply.

4: Mount the MaxAttach NAS 6000 Equipment Enclosures

Mount the Base Unit and any equipped Expansion Units into your rack.

1. Mount the base unit enclosure shelf in the rack at the bottom of the stack and tighten all hardware.

2. If equipped, add the first Expansion Unit enclosure above the Base Unit and tighten all hardware.
 - There should be no gap between the two enclosures.
3. If equipped, add the second Expansion Unit enclosure above the first expansion enclosure and tighten all hardware.
 - There should be no gap between the two enclosures.

5: Re-Seat All Hard Disk Drive Carrier Assemblies

Shipping vibration may have disconnected individual hard drives from their back plane connectors. One drive at a time, pull the drive out of its Drive Bay, record its size and serial number information, and replace it in its as-shipped Drive Bay location.



CAUTION

REPLACE DRIVE IN ORIGINAL DRIVE BAY SLOT AND SHELF: Be sure to replace the drive in its original as-shipped Drive Bay. If you mix the drive and Drive Bays locations up, you will probably have to reconfigure the disk RAID arrays.

1. For each drive, push down on the Ejector Tab, and then lift up on the Ejector Lever.
 - The drive releases from its Drive Bay connector.
2. Pull the drive out of its Drive Bay.
 - This is a good time to record the drive type and serial number.
3. Replace the drive in its Drive Bay until it begins to engage the connector.
4. Make sure the Ejector Lever is free of the Ejector Tab and place your thumbs on either side of the drive LEDs and press gently into the bay.
5. Lower the Ejector Lever to latch the drive into place and then lock the Ejector Lever on the Ejector Tab.

6: Review the Connector Locations

You will make connections on and between all installed enclosures. The connections are for the:

- Small Computer System Interface (SCSI) bus
- Environmental Monitoring Unit (EMU) serial port daisy chain
- NIC cables
- AC power.

Note that the base unit is on the bottom, the first expansion unit in the middle, and the second expansion unit on the top.

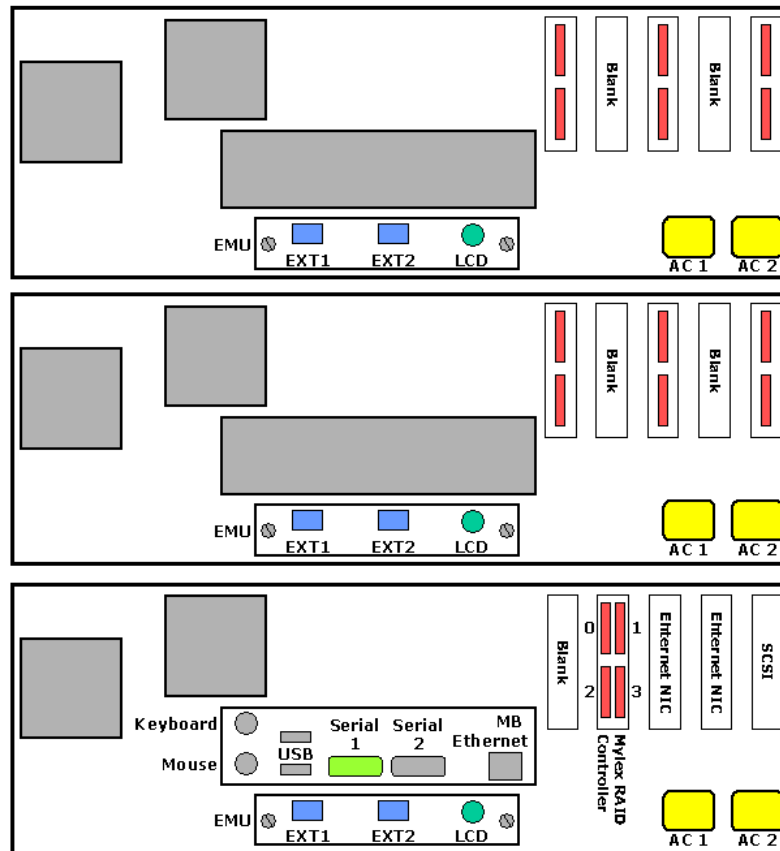


Figure #2 NAS 6000 Rack Mount System Back Panel Connectors

7: Install the External SCSI Cables

In this section, you will install SCSI drive cables between the Base Unit and your Expansion Units.

Cabinet-Mount System or Single Base Unit Rack Mount System

1. Process Branch Point:
 - If your system has a Base Unit and one or two Expansion Units, perform the next step in this process immediately below in the section titled **SCSI Connections Between Base Unit and First Expansion Unit** on page 5.
 - If you have a cabinet-mounted stem or a single Base Unit rack-mount system, no SCSI cabling is required. Skip ahead below to the section titled **Install EMU Cables** on page 7.

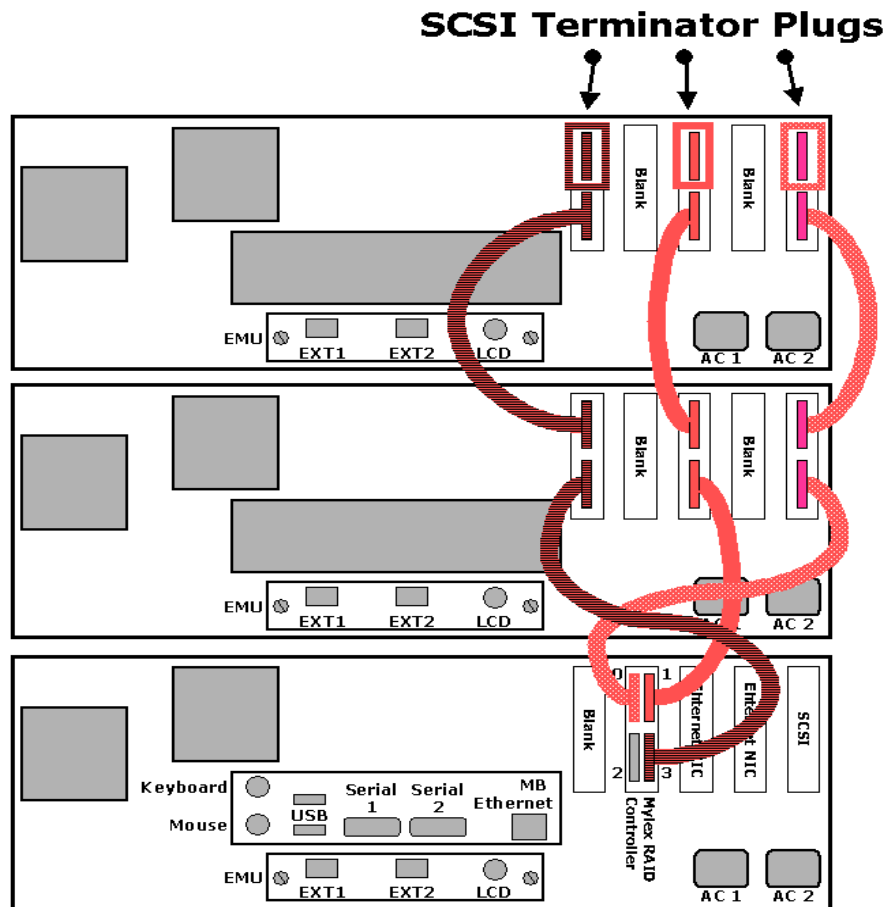


Figure #3 NAS 6000 SCSI Cable Connections

SCSI Connections Between Base Unit and First Expansion Unit

2. Connect a SCSI cable from the Mylex upper left Port 0 connector to the right side SCSI Connector Board.
3. Connect a second SCSI cable from the Mylex upper right Port 1 to the center SCSI

Connector Board.

4. Connect a third SCSI cable from the Mylex lower right Port 3 to the left side SCSI Connector Board.
5. Process Branch Point:
 - If your system only has a single Expansion Unit, your next step below is **Step #6**.
 - If your system has an additional Expansion Unit to install, skip below to **Step #8**.
6. Add SCSI Terminator Plugs to the upper connector on each SCSI Connector Board.
7. Your SCSI Cabling is complete. Skip ahead below to section **#8: - Install EMU Cables** on page 7.

SCSI Connections Between the First and Second Expansion Units

8. Connect the two left side SCSI Connector Cards with a first SCSI Cable.
 - Use the lower SCSI connector for all cable runs.
9. Connect the two center SCSI Connector Cards with a second SCSI Cable.
10. Connect the two right side SCSI Connector Cards with a third SCSI Cable.
11. Add SCSI Terminator Plugs to the upper connector on each SCSI Connector Board.



NOTE

If you ordered two Expansion Units, you may end up with an extra set of unused SCSI Connector Cards.

8: Install EMU Cables

In this section, you will connect the Base Unit CPU to the Environmental Monitor Unit (EMU) mounted in each enclosure unit.

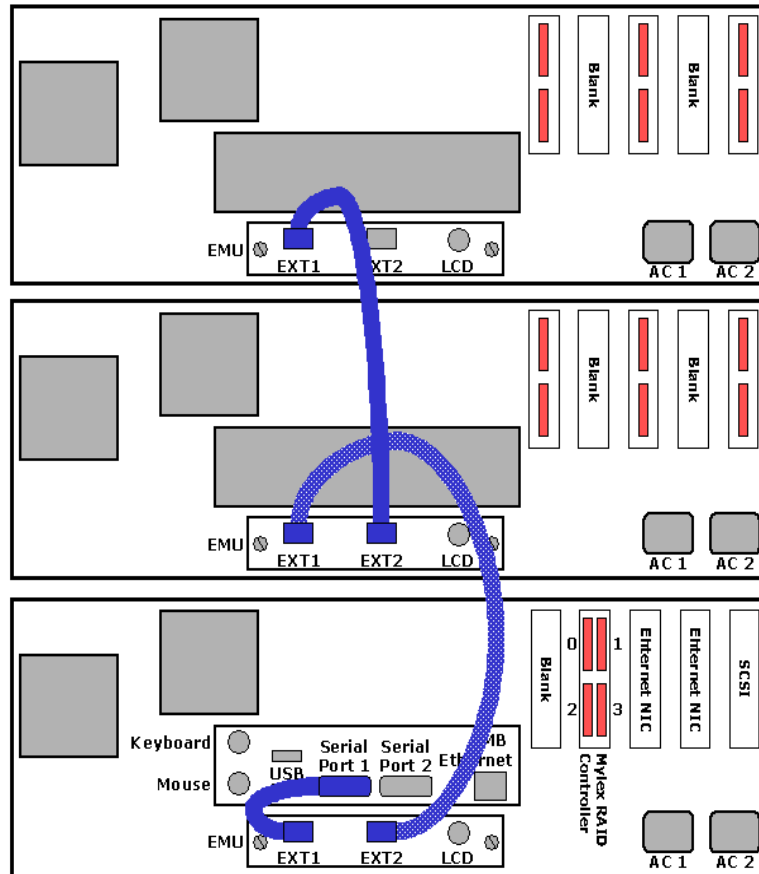


Figure #4 NAS 6000 EMU Cable Connections

EMU Cable on Base Unit Installation

1. Install the Base Unit EMU Cable.
 - Short Male/Male (M/M) serial cable
 - Start at EMU left side EXT1 port
 - Connect to CPU I/O Panel Serial Port 1.
 - Connect Base Unit to First Expansion Unit

9: DECISION POINT - Are there Expansion Units to Install?

- If your system has only a single Base Unit, skip ahead to **Step #13 - Install Network and AC Power Cables** on page 9 below.
- If you system has a Base Unit and one or two Expansion Units, to continue with the step immediately below.

10: EMU Cable Between Base Unit and First Expansion Unit

1. Install the Base Unit to First Expansion Unit EMU Cable
 - Longer M/F serial cable.
 - Start at the Base Unit EMU EXT2 port.
 - Connect to EMU EXT1 port on the first Expansion Unit.

11: DECISION POINT - One or Two Expansion Units

- If your system has only a single Base Unit, skip ahead to **Step #13 - Install Network and AC Power Cables** on page 9 below.
- If you system has a Base Unit and two Expansion Units, to continue with the step immediately below.

12: EMU Cable Between First and Second Expansion Unit

2. Install first Expansion Unit to second Expansion Unit EMU cable.
 - Longer M/F serial cable.
 - Start at first Expansion Unit EMU EXT2 port.
 - Connect to EMU EXT1 port on the second Expansion Unit.
3. Your EMU cabling is complete.



NOTE

There is no terminator on the last EMU EXT2 port.

13: Install Network and AC Power Cables

In this section, you will connect your Network Interface Cards (NICs) to your network hub with user-supplied NIC cables. You will also connect the AC power cords to the equipment shelves and connect them to user-supplied AC power strips.

Network Connections

Connect the appropriate NIC cables as follows:

1. Between each NIC and network hub or ports.
2. At least one network connection is required.
3. You can also add a network connection from the CPU I/O panel network port to

your network for administrative functions.

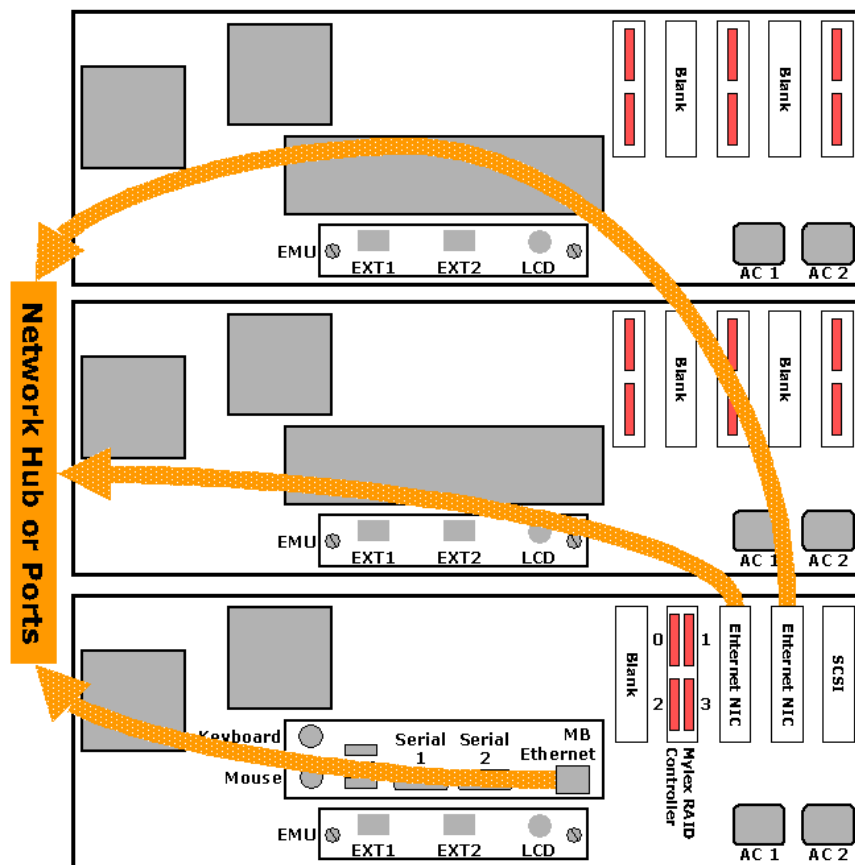


Figure #5 NAS 6000 Network Cable Connections

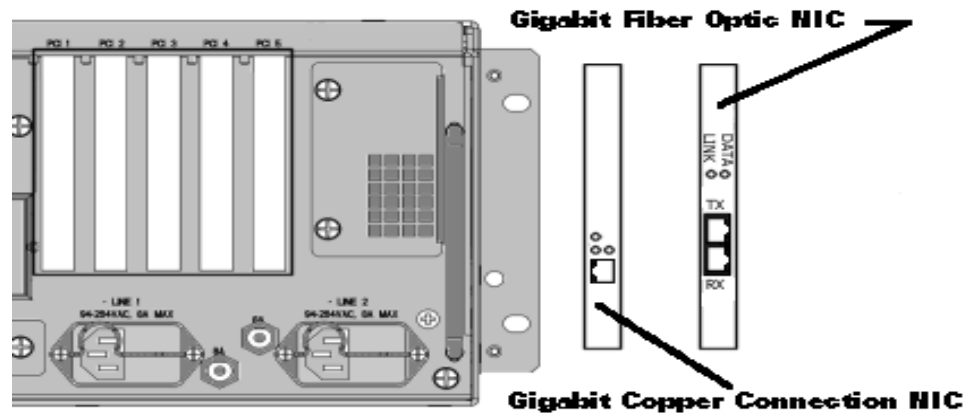


Figure #6 NAS 6000 Network Interface Card Connector Options

AC Power Connections

1. Connect each AC power strip cord to the local AC power source.
 - Recommend that each AC power strip be on a separate circuit.
2. Connect the NAS 6000 Expansion Unit enclosure to the user-supplied AC power strips.
3. Install two AC power cords in each enclosure shelf.
4. Route the left side cords to the left side AC power strip.
5. Route the right side cords to the right side AC power strip.
6. Make sure all the power supply back panel ON/OFF rocker switches are in the OFF or "O" position.
 - There are two back panel switches on each enclosure shelf.

7. Your MaxAttach NAS 6000 is ready to be powered up.

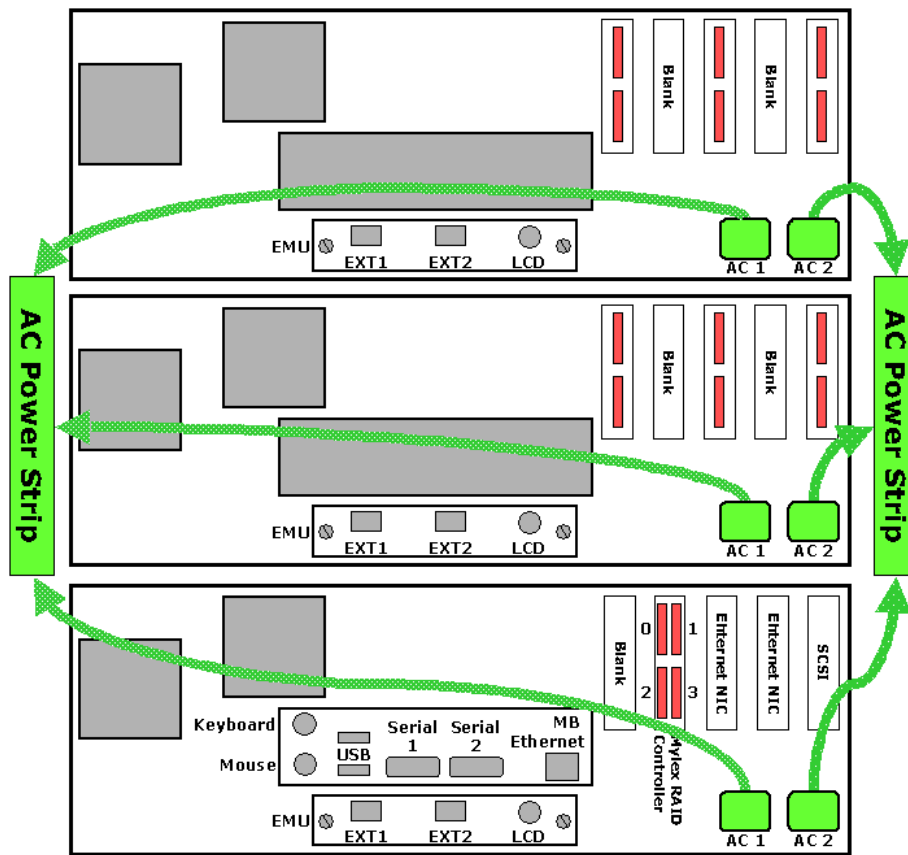


Figure #7 NAS 6000 AC Power Connections

14: International AC Power Strip Solutions for Rack Mount Systems

For MaxAttach NAS 6000 installations in locations outside of North America, localized AC power strips are required.

Localized Internal AC Power Cords

For international locations, the MaxAttach NAS 6000 ships with the correct AC power cord for connection between each Base and Expansion Unit equipment shelf and the user-supplied AC power strips.

Localized AC Power Strips/Blocks

Maxtor has identified four power strip solutions for the following countries and world areas:

- Australia
- Europe
- Japan
- United Kingdom
- United States

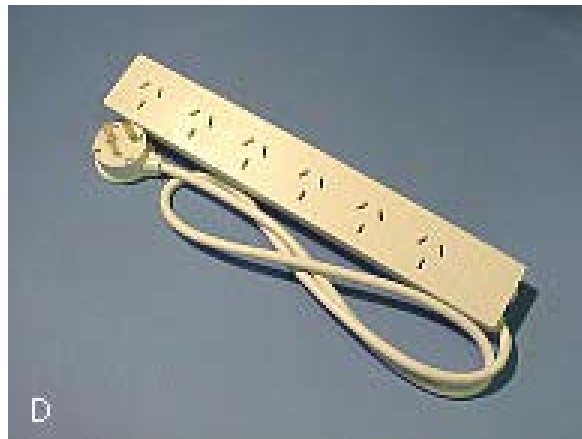
The specifications of these strips plus a US approved power strip is detailed below.

Australia

Vendor:

- Panel Components Corporation
- Address: PO Box 115, Oskaloosa, IA 52577, USA
- Email: info@panelcomponents.com
- Web Site: <http://www.panelcomponents.com>

Photo:



AC Power Strip Specifications:

- Vendor's Part Number: 85010050
- Socket Type: AS3112
- Number of Sockets: 6
- Cord Length: 1.04 meters
- Cable Plug: AS3112
- Case: Plastic, includes circuit breaker

- Color: White
- Rating: 250VAC / 10A

Agency Approvals:

- Australia DFT 15632

Europe***Vendor:***

- Panel Components Corporation
- Address: PO Box 115, Oskaloosa, IA 52577, USA
- Email: info@panelcomponents.com
- Web Site: <http://www.panelcomponents.com>

Photo:***AC Power Strip Specifications:***

- Vendor's Part Number: 85003040
- Socket Type: CEE 7
- Number of Sockets: 4
- Cord Length: 2.5 meters
- Cable Plug: CEE 7/7
- Case: Metal, includes rocker switch

- Color: Orange
- Rating: 250VAC / 16A

Agency Approvals:

- Germany, VDE, 15970

Japan***Vendor:***

- Wirecom Corporation
- 3PL, No. 290, Sec 4., Yen Ping North Road, Taipei, Taiwan
- Telephone: 886-2-2597-6617
- FAX: 886-2-2597-6625
- Email: Not available
- Web Site: Not available

AC Power Strip Specifications:

- Vendor's Part Number: SLW6, SP6, or CK6
- Socket Type:
- Number of Sockets: 6
- Cord Length: 0.61 meters to 7.6 meters
- Cable Plug: Mounded-on grounding type attachment plug.
- Case: Plastic
- Color: White
- Rating: 125VAC / 15A

Agency Approvals:

- UL

United Kingdom***Vendor:***

- Panel Components Corporation
- Address: PO Box 115, Oskaloosa, IA 52577, USA
- Email: info@panelcomponents.com
- Web Site: <http://www.panelcomponents.com>

Photo:**AC Power Strip Specifications:**

- Vendor's Part Number: 85010322
- Socket Type: BS1363
- Number of Sockets: 4
- Cord Length: 2.5 meters
- Cable Plug: BA1363
- Case: Plastic, includes switch and fuse
- Color: White
- Rating: 250VAC / 13A

Agency Approvals:

- Not available from Panel Components

United States**Vendor:**

- Panel Components Corporation
- Address: PO Box 115, Oskaloosa, IA 52577, USA
- Email: info@panelcomponents.com
- Web Site: <http://www.panelcomponents.com>

AC Power Strip Specifications:

- Vendor's Part Number:
- Socket Type:
- Number of Sockets:
- Cord Length:
- Cable Plug:
- Case:
- Color:
- Rating:

Agency Approvals:

- UL

Chapter #2 - Overview - MaxAttach NAS 6000 Hardware

Chapter Outline

This chapter covers the following topics:

- System features
- System data storage solutions
- Hardware features
- Advanced data protection features
- System disk drive configuration
- Enclosure configuration options
- Major components
- Base Unit Enclosure description
 - Front panel description
 - Back panel description
- Expansion Unit Enclosure description
 - Front panel description
 - Back panel description
- Description of system components
 - Power supplies
 - Disk drive carriers
 - CPU I/O panel
 - Network interface cards
 - Fans and blowers
 - SCSI interface connectors and cabling
 - Environmental monitoring unit connectors and cabling

System Features

- User data capacities are stated as available disk drive array capacities when factory configured to RAID 5 arrays across six physical disks.

- RAID 5 provides cross disk striping with distributed parity for optimal balance of read/write speed coupled with maximum fault tolerance and recovers in the event of a disk drive failure.
- Usable user data capacities along with relative fault tolerance and read/write speed will vary if other RAID configuration are used.
- Enterprise NAS software powered by Windows operating system
- Cross-platform file sharing
- Hardware RAID 0, 1, 0+1, 5, and JBOD (just a bunch of disks)
- Capability to provide snapshot using Persistent Storage Manager
- Hot swappable and redundant hardware:
 - Fans
 - Blowers
 - Power supplies
 - Hard disk drive carrier assemblies.
- Up to three NIC connections:
 - 10/100-BaseT Ethernet from CPU
 - Gigabit Ethernet with Copper Connections
 - Gigabit Ethernet with Fiber Connections
- Three mounting options:
 - Standard rack-mount units for user-provided 19" rack
 - Self-contained roll around 28" cabinet for under-desk installations
 - Chatsworth cabinet racks in 48" and 84" heights for mounting multiple systems in one location.

Overview

MaxAttach NAS 6000 is an easy to configure, enterprise-class network-attached storage (NAS) server. This file server provides unparalleled value in data management solutions. Based on a Microsoft Windows-Powered operating system, the MaxAttach NAS 6000

provides a comprehensive suite of storage management tools or can be managed with existing enterprise management tools. From directory support to security, to backup, MaxAttach integrates seamlessly into any network environment.



Figure #3 MaxAttach Network Attached Storage 6000 Cabinet System

MaxAttach NAS 6000 is a scalable, reliable, and cost-effective storage solution for heterogeneous file sharing, archiving and disk-based backups. Based on a Windows Powered operating system, the MaxAttach NAS 6000 provides a comprehensive suite of storage management tools and enables easy integration into enterprise network storage architecture.

Cross-Platform File Sharing

MaxAttach NAS 6000 enables cross-platform file sharing among clients and servers: Windows, UNIX/Linux, NetWare and Apple Macintosh environments. The support extends fully into the security and directory infrastructure of these platforms, including cross-platform file locking.

Enclosure Configuration Options

The MaxAttach NAS 6000 provides the user with highly configurable storage solutions by varying the enclosure type, its basic capacity, and its available disk space for user data.

The MaxAttach NAS 6000 is available in two basic enclosure types of rack-mount ready in a standard 19" rack or assembled in a roll around self-contained cabinet. The rack mount version takes 4 rack space units (4U) per disk drive enclosure (4U, 8U or 12U).

The available user storage space depends on the number of expansion enclosures that are used with the system and the drive array selected by the user.

Rack Mount Systems

The Max Attach NAS 6000 can be mounted in a user-supplied EIA standard 19" rack for installation in equipment rooms and wiring closets. Each equipment enclosure only requires 4U. The base unit is mounted on the bottom, and up to two expansion enclosures may be mounted above it.

Cabinet Mounted System

MaxAttachNAS 6000 systems may also be ordered mounted into a roll-around, lockable cabinet for installation in office environments

- The basic cabinet system has a small footprint and measures 28.5" H x 21.75" W x 26" D - 72.4cmH x 55.2cmW x 66cm D.
- The cabinet-mounted system can be user-lowered an extra 0.5 inches - 13mm to accommodate under cabinet storage locations.

Major Components of the Maxtor MaxAttach NAS 6000

The Base Unit and the Expansion Unit enclosures are the two major assemblies in the MaxAttach NAS 6000. Within these two assemblies are the sub-assemblies described below.

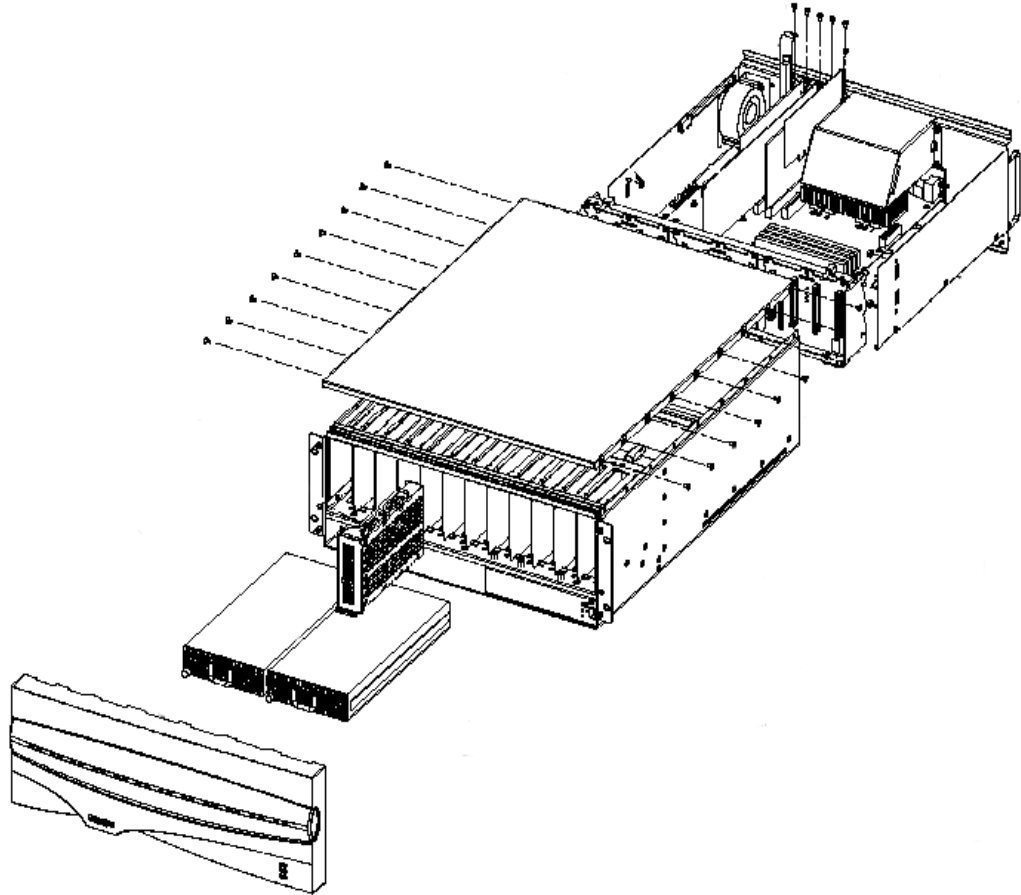


Figure #4 Exploded View of a Base Unit

Base Unit Front Panel

The Base Unit is required for every MaxAttach NAS 6000 and contains the system CPU, two power supplies, the fans, the necessary SCSI and Environmental Controllers, and 12 Disk Drive Carrier Assemblies. The Base Unit front panel provides local system control, LED indicators for key system parameters, and an LCD panel for a summary of status alerts.

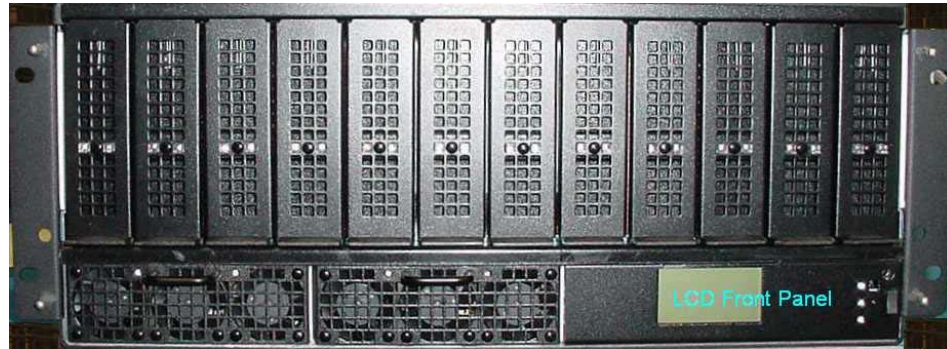


Figure #5 NAS 6000 Base Unit Front Panel Photo

The base unit front panel contains LED indicators for drive, power supply, and system status and a power switch.

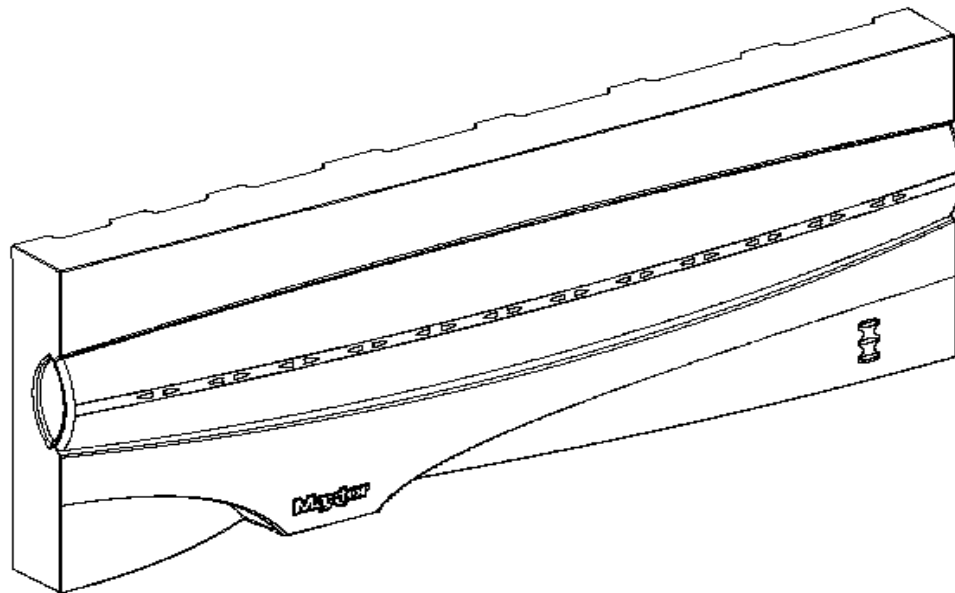


Figure #6 NAS 6000 Base Unit Front Panel Diagram

Base Unit Front Panel Status LEDs

The figure below shows the location of the LEDs on the Base Unit front panel.

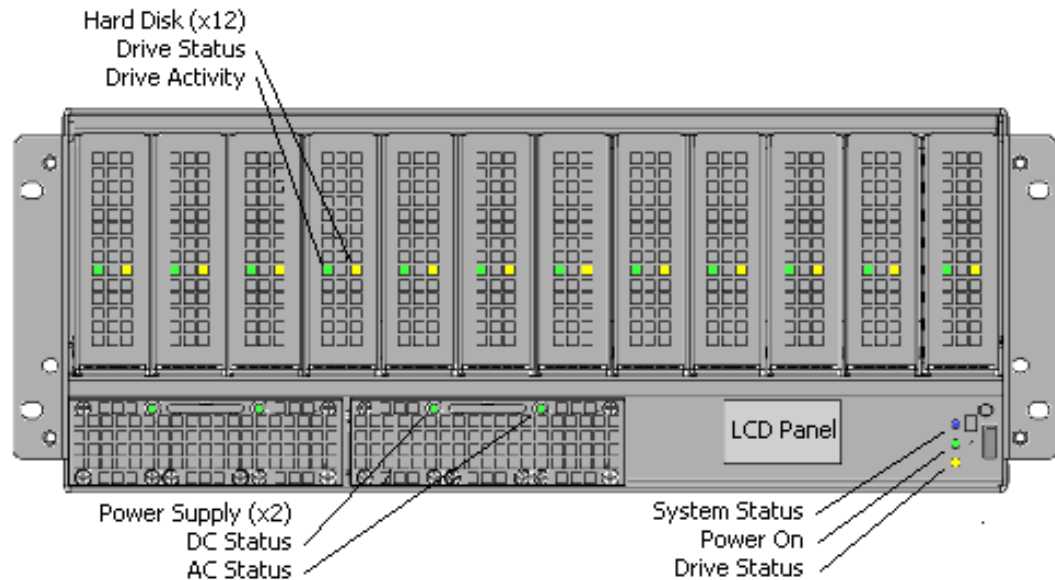


Figure #7 Base Unit Status LEDs

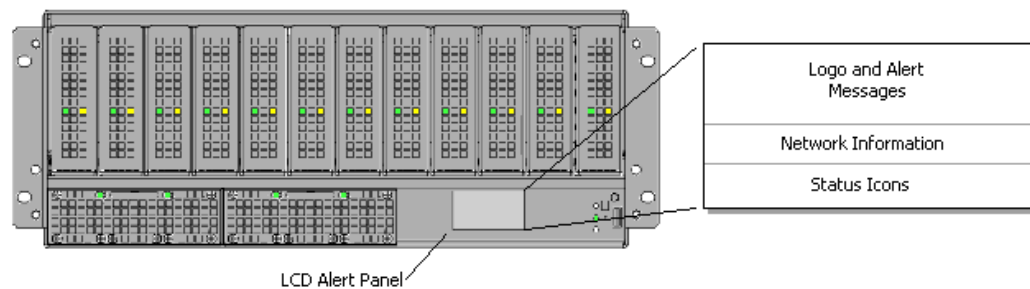


Figure #8 Base Unit LCD Panel

Overview

The MaxAttach NAS 6000 provides a wide range of alerts to inform the system administrator about system status. There are five categories of alerts:

- **LED Alerts:** Front panel LEDs indicate status of disk drives, power supplies, and other system components.

- **LCD Alerts:** Messages are displayed on a small liquid crystal display (LCD) on the MaxAttach front panel.
- **Web UI Alerts:** Error messages and condition alerts that you access from the device's LED Status Indicators

LED (light emitting diode) status indicators are available on the front panels of the base unit and each installed expansion unit and provide general information about:

- Activity and condition of the hard disk drive modules (on all enclosures)
- Status of the unit's power supplies (on all enclosures)
- Over-all system status (only on the Base Unit enclosure).

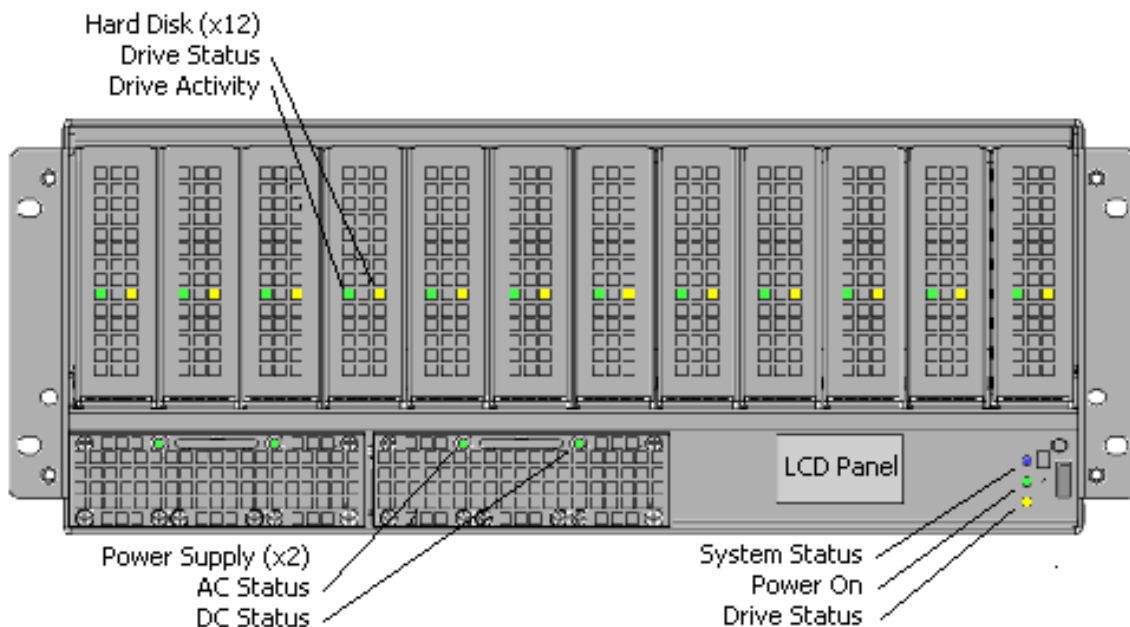


Figure #9 NAS 6000 LED Locations and Functions

Front Panel LEDs

There are three LED indicators in the lower right-hand corner of the main front panel that indicate general system status. These are the System Status Alarm indicator, the Power On indicators, and the Drive Status indicator.

- **BLUE System Status Alarm Indicator - Normally OFF**
 - This is a blue lamp which reports overall system status. The lamp remains off unless there is an alarm from a source below.
 - Blower or fan alarm - the blower or a fan is indicating an underspeed condition.

- Power supply voltage alarm – a power supply indicates that one or more voltages are out of limits.
- Temperature alarm – temperature inside the enclosure has exceeded programmed limits.
- HDD alarm – one or more HDDs are failing. The failed drive will have its Drive Status (yellow) indicator on
- GREEN Unit Power-On Indicator – Normally ON
 - This is a green lamp indicating that power is on.
 - The lamp will flash (indicating not ready) until the system has completed its boot-up sequence and is ready for operation.
- YELLOW Drive Status Indicator – Normally OFF
 - This is a yellow lamp indicates there is a HDD problem.
 - If there is a HDD problem this lamp will be lit.
 - If any HDD module status lamp is on, this lamp will also be on.

**NOTE**

Expansion units indicate their own status and activity. However, you must start the base unit to enable the expansion unit status indicators. The base unit's soft power switch controls the start-up of the expansion units.

Hard Disk Drive Module Status LEDs

Each Hard Disk Drive (HDD) Module has two LED indicators on its front panel:

- A green **Drive Activity** indicator.
 - This indicator flashes in response to drive accesses
- A yellow **Drive Status** indicator.
 - This indicator is off during normal operation.
 - It lights if there is an HDD module failure.
 - When the unit's back panel AC power switch is on and the front-panel soft power switch is off, all drive status indicators are on.
 - As the unit powers up, the indicators go off as each drive becomes ready.

Power Supply Status LEDs

The MaxAttach 6000 is equipped with dual power supplies. Should one supply fail, the other takes over. Each power supply has a green AC-OK indicator and a green DC-OK indicator.

- AC-OK Indicators
 - These indicators remain lit as long as AC power is supplied to the power supplies.
 - If a lamp is off, it indicates that the AC power has been interrupted to the power supply. This could indicate the supply's power cord is detached, the power supply is turned off, the supply's circuit breaker has opened, or that there is an open in the internal AC wiring harness.
- DC-OK Indicators
 - These indicators remain lit as long as the supply's DC voltages are normal.
 - If a lamp is off, it indicates either the AC power is off (check the supply's AC-OK indicator) or one or more of the DC voltages is out of its normal range.

**NOTE**

If a single DC-OK indicator is off, the system may still function properly using the other power supply. However, you should take corrective action as soon as possible.

LCD Alert Panel

The front-panel LCD (liquid crystal display) alert panel is a small 2.25"W x 1.25"H - 57mmW x 37mmH display with a resolution of 128 pixels W x 64 pixels H.

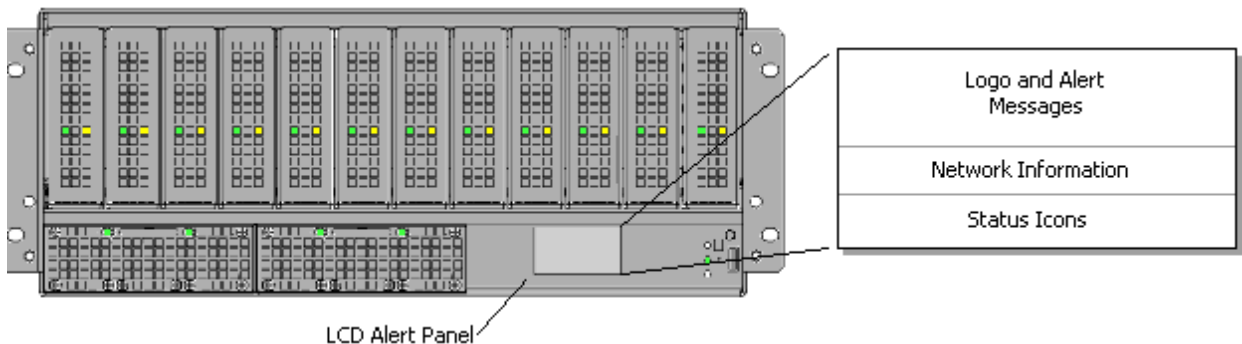


Figure #10 NAS 6000 LCD Front Panel Location and Display Areas

**NOTE**

When the MaxAttach unit is housed in a system cabinet, each unit's alert messages can be sent to the LCD panel on the cabinet. Up to three MaxAttach servers can be supported by the cabinet LCD alert panel.

The LCD alert panel displays summary status messages about the state of the MaxAttach. The display is divided into three separate status display areas:

- Logo and Alert Message Area – Top display area
 - 128 W x 36H pixel area – 2.25”W x 0.7”H – 57mmW x 18mmH.
 - Displays a Microsoft Windows-Powered logo during normal operation.
 - It displays an alert name and title when the system generates an alert.
- Network Information Area – Middle display area
 - 128W x 12H pixel area – 2.25”W x 0.26”H – 57mmW x 7mmH
 - Alternately displays the unit's host name and IP address.
- Status Icon Display Area – Bottom display area
 - 128W x 16H pixel area – 2.25”W x 0.3”H – 57mmW x 8mmH
 - Normally displays three standard icons indicating the status of the system, disk, and network.
 - During alert conditions, the system may display multiple error condition icons.

Logo and Alert Message Display Area

The Logo and Alert Message display area is on the top of the LCD display. Under normal operation, the logo and message display area shows a Microsoft Windows-Powered logo.

During alert conditions, the LCD panel shows an alert name and title and a message counter that consists of the message number, a slash, and the total number of pending messages (e.g. 1/20 for message number one of twenty total messages). If multiple messages have been generated, the panel displays the most recent message until it is cleared at the Web user interface.

The LCD panel reports alerts from the following systems:

Environmental Monitoring Unit (EMU)

The LCD panel displays specific information about a subsystem problem:

- Disk failure
- Power supply failure
- Fan failure
- Disk backplane voltage error
- Abnormal temperature

TCP/IP and NetBT

The LCD panel displays a network-related system problem:

- Network interface card (NIC) failure

- Duplicate IP address
- Duplicate computer name (NetBT)

GAMevlog

The LCD panel displays HDD-related problems and directs users to the Web user interface to obtain more detailed information.

Mylex RAID Controller

Mylex RAID controller-generated event are also displayed. If appropriate, the LCD panel will also display an alert icon (described below). For example, during a Fan Failure alert, the icon display area will show a Fan Error icon.



Figure #11 NAS 6000 Fan Failure Icon

Network Information Display Area

The Network Information display area is the middle display area on the LCD panel. Every five seconds, the display alternates between the MaxAttach NAS 6000's IP address and its server name. Only the first 20 to 25 letters of the server name will be displayed; longer names will be truncated.













Status Icon Display Area

The Status Icon Display area is the bottom display area on the LCD panel. There are 12 icons that display either transitional status such as the start-up process, normal status such as system availability, or alert status such as disk or network problems. Multiple icons can be displayed at the same time. During normal operation, the icon display shows a system starting icon, a disk normal icon, and a network normal icon.



Figure #12 NAS 6000 LCD Panel Normal Operation System Icons

The available system icons are:

Table #1 - LCD Icons and Definitions			
Icon	Icon Definition	Icon	Icon Definition
	System starting (OS Starting)		System normal and ready (OS Ready)
	System halted (OS Halted)		System shutting down (Shutdown)
	Disk normal and in good condition (Disk OK)		Disk error
	Waiting		Local area network normal and in good condition (LAN OK)
	Local area network error (LAN Error)		Fan error, problem, or fan inoperative
	Over temperature detected		Voltage out of acceptable tolerance range

Base Unit Back Panel

The back panel of the base unit provides I/O connection for inter-enclosure SCSI and EMU cabling, connections for the NICs and Ethernet Port, and system hard power switches. In addition, access to the hot swappable fans and blower is provided. Other than on the NICs, there are no status indicators.



Figure #13 Base Unit Back Panel

Expansion Unit

Up to two Expansion Units may be added above a single MaxAttach NAS 6000 Base Unit. Each Expansion Unit provides 12 disk drives mounted in their Hard Disk Driver carrier Assemblies. In normal default RAID configuration, each unit is divided into two six-disk RAID 5 arrays. RAID 5 is striping across multiple drives with distributed parity for an optimum balance between fault tolerance and recovery, maximum disk drive space, and I/O read/write speeds.

Expansion Unit Front Panel

The Expansion Enclosure front panel is similar to the Base Unit front panel with the following exceptions:

- No System Status LED
- No Power On LED
- No Drive Status LED
- No front panel power rocker switch.

The Power Supply LEDs and the Hard Disk Drive Carrier Assembly LEDs are the same.

Expansion Unit Back Panel

The Expansion Enclosure Back Panel is similar to the Base Unit with the following exceptions:

- No CPU I/O Panel
- Three SCSI Connector Cards mounted in the card cage instead of a single RAID Controller Card.
- No NICs
- The Power Supply Switches, Fans, and Blowers are the same.

Description of System Components

Major MaxAttach NAS 6000 Base Unit components:

- Power Supply Modules - hot swappable - two per Base Unit enclosure
- Hard Disk Drive Carrier Assemblies- hot swappable - 12 per Base Unit enclosure
- Standard network Ethernet port mounted on the CPU I/O Panel - one per Base Unit enclosure
- High performance Gigabit Ethernet Network Interface Card (NIC) with copper connections - one per Base Unit enclosure
- High performance Gigabit Ethernet NIC with fiber optic connections - one per Base Unit enclosure
- Cooling Fans - hot swappable - two per Base Unit enclosure
- Cooling Blower - hot swappable - one per Base Unit enclosure
- SCSI RAID Controller Card -- connection to and management of disk arrays in the Base Unit and any attached Expansion Units - one per Base Unit enclosure
- Environmental Monitoring Unit (EMU) Card -- monitoring system environmental conditions such as temperature and power consumption - one per Base Unit enclosure

Power Supply Modules

There are two hot swappable power supplies per Base Unit cabinet enclosure. Each power supply is capable of running the system independently and can be hot swapped with another assembly at any time. Each power supply has three fans on its front panel to help with system cooling.



Figure #14 Hot Swappable Power Supply Three-Quarters View

Disk Drive Carriers

The system disk drives are enclosed in individual disk drive carriers 12 per enclosure. Individual failed drives can be hot swapped while the system is running. In the default RAID-5 configuration, a RAID-5 array will continue to function with slightly degraded service in the event of a drive failure.

However, prompt action should be initiated to replace the failed drive. When a drive fails in a fault tolerant RAID array, the array is put into a “critical” state where the failure of a second drive in the array will lead to non-recoverable data loss. After the user replaces the failed drive, the system administrator must initiate the RAID volume rebuild in the background, a process which can take several hours.

Optionally, an administrator can modify the default RAID configuration and leave one or two drives available as hot spare drives. These are drives that are powered up, but unused in any array. In the event of a drive failure, the failed drive drops offline and is replaced automatically by the hot standby drive. The RAID rebuild process starts automatically and immediately.

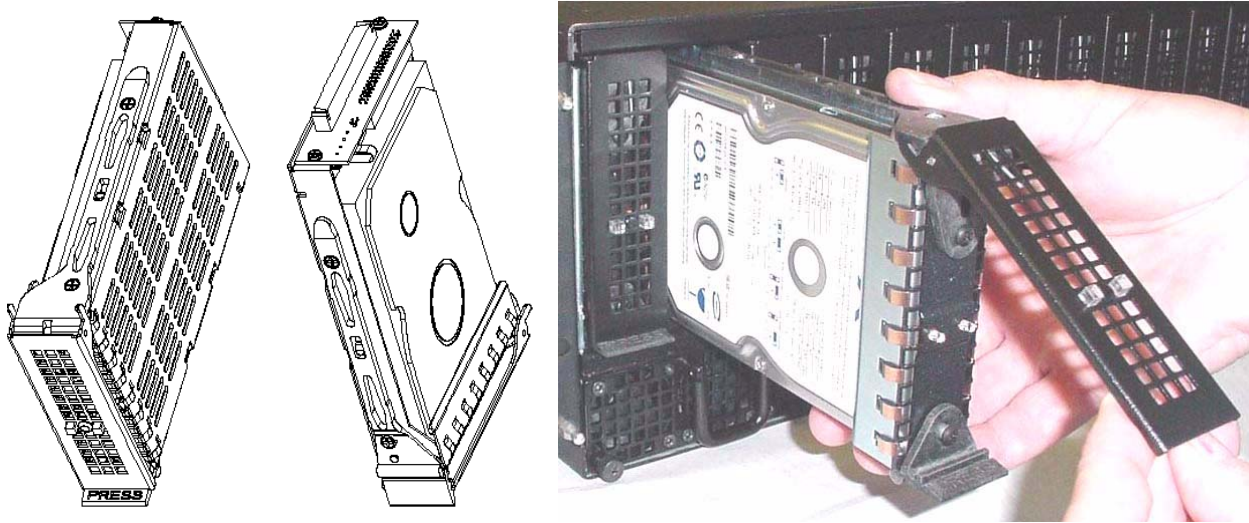


Figure #15 Hot Swappable Hard Disk Drive Carrier Diagram and Photo

CPU I/O Panel

The CPU I/O Panel is located on the Base Unit's Back Panel and it is the primary diagnostic and administration interface into the MaxAttach NAS 6000.

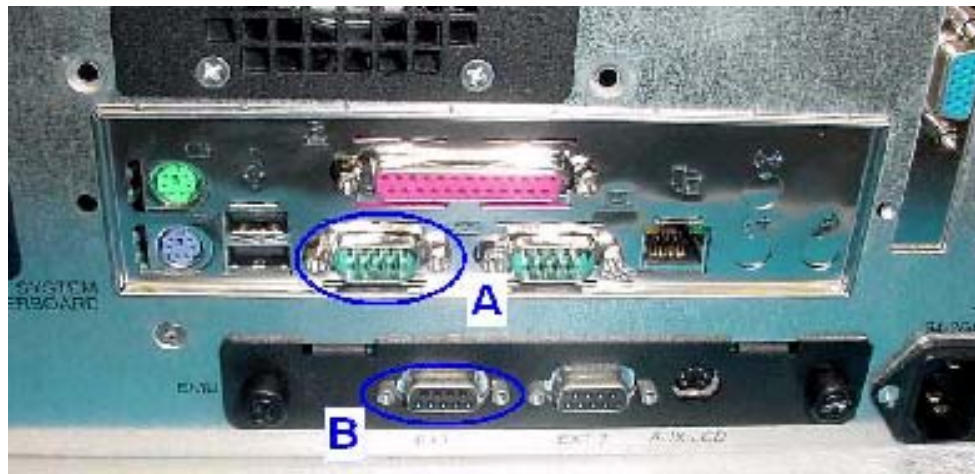


Figure #16 CPU I/O Panel Above the EMU Connector Panel

It provides connections for:

- Mouse (used only for diagnostics)
- Keyboard – used only for diagnostics
- USB ports – two – not used
- Parallel I/O port – not used
- Serial port 1 – used by the Environmental Monitoring Unit (EMU)
- Serial port 2 – not used
- Ethernet port from the CPU motherboard

CPU Ethernet Port

Every system is equipped with a standard IEEE 802.3/IEEE 802.3U-LAN-compliant 10BaseT/100BaseTX Ethernet port on the CPU motherboard of the MaxAttach NAS 6000 Base Unit chassis. Located on the CPU I/O Panel, the LAN connector for this port is a standard RJ-45 type, compatible with standard CAT 3, 4, and 5 UTP cabling for 10BaseT operation (10 Mb/s) and Cat-5 UTP cabling for 100BaseTX operation (100 Mb/s).

The CPU Ethernet Port is only replaceable by replacing the CPU motherboard.

Network Interface Cards (NICs)

The Maxtor MaxAttach NAS 6000 is equipped with two high performance NICs in addition to the Ethernet port on the CPU I/O Panel. The default configured NICs are:

- A gigabit Ethernet NIC with copper wire connections
- A gigabit speed Ethernet NIC with fiber optic connections

Clients attached to a particular network type (10BaseT/100BaseTX, Gigabit copper, Gigabit fiber-optic) access the MaxAttach NAS 6000 at the IP address assigned to each LAN adapter.

The software drivers for Windows 2000 have been pre-installed at the factory and there is no user configuration required other than entering local network parameters such as IP address.

All set up operations for the installed network interfaces are automatic. Once the cables are attached, there are no user controls or adjustments. The devices automatically detect the network speed and configure themselves for optimum throughput.

All of the card cage NICs are field replaceable units, although system down time is required to access the system internal components.

Determining Your System's NIC Configuration

There is a five-slot card cage in the MaxAttach NAS 6000 Base Unit. The card cage holds a video card, a RAID Controller Card, and a SCSI connector. The two remaining slots hold the NICs. To determine which NICs are installed in your system, locate the card cage at the back of the MaxAttach NAS 6000 and identify the three standard system cards by their connectors (these may occupy any slot):

- The Video Card has a 15-pin DSUB connector.
- The RAID Disk Controller Card has 4 high-density 68-pin SCSI connectors.
- The SCSI Connector Card has a single 68-pin connector.
- In the remaining two card cage slots, look at the connectors and compare them to the examples shown in the following diagram.

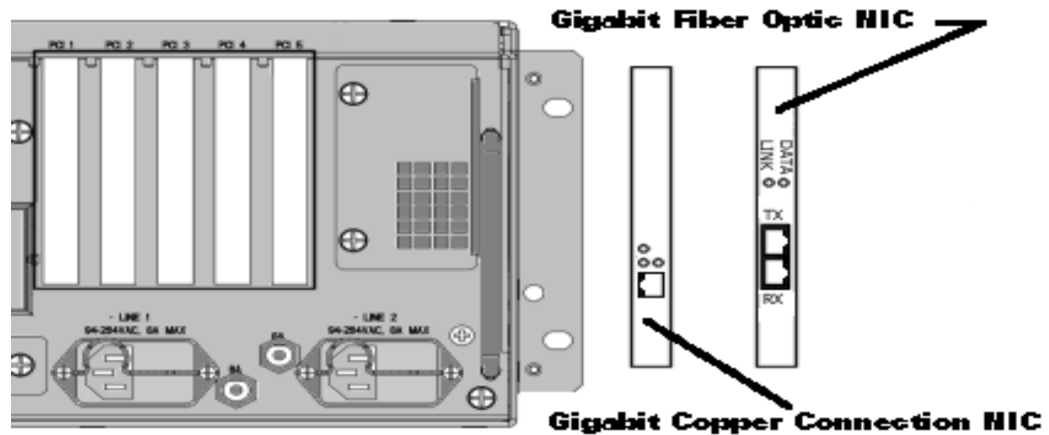


Figure #17 Network Interface Cards I/O Ports Diagram

The manufacturer and configuration of the NICs may differ from your system's conjuration.

Hot Swappable Fans and Blower

To provide maximum system life, each chassis enclosure comes with two Back Panel fans and a single Blower. In the event of a failure, each unit is hot swappable with no loss of system up time.

In addition, the Base Unit enclosure comes with a fan on each CPU microprocessor. These units are cold swappable, requiring approximately 30 minutes to access and change out.

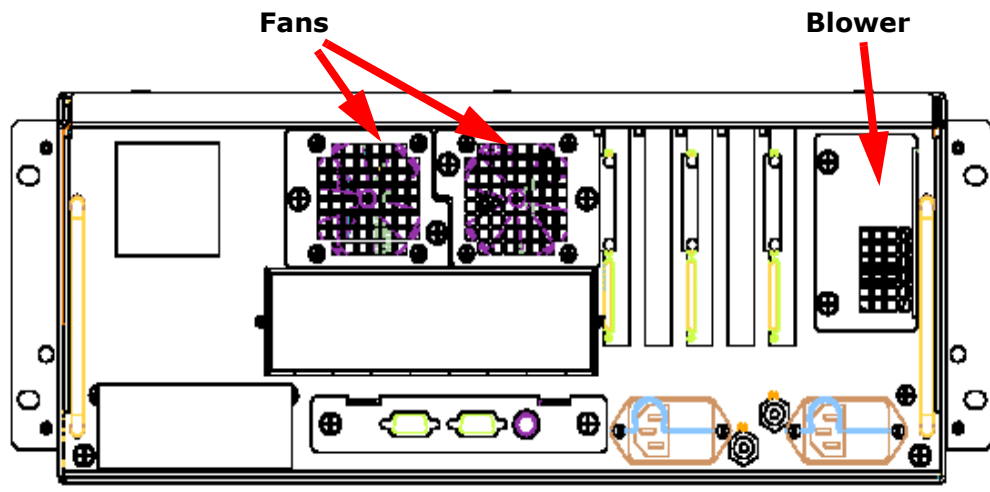


Figure #18 Back Panel Fan Locations

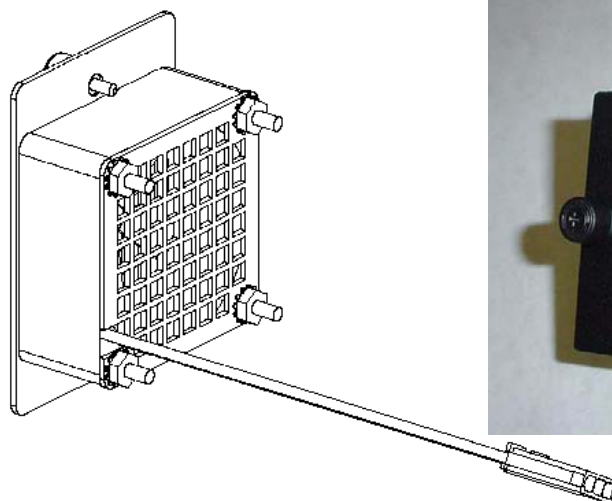


Figure #19 Fan Assembly

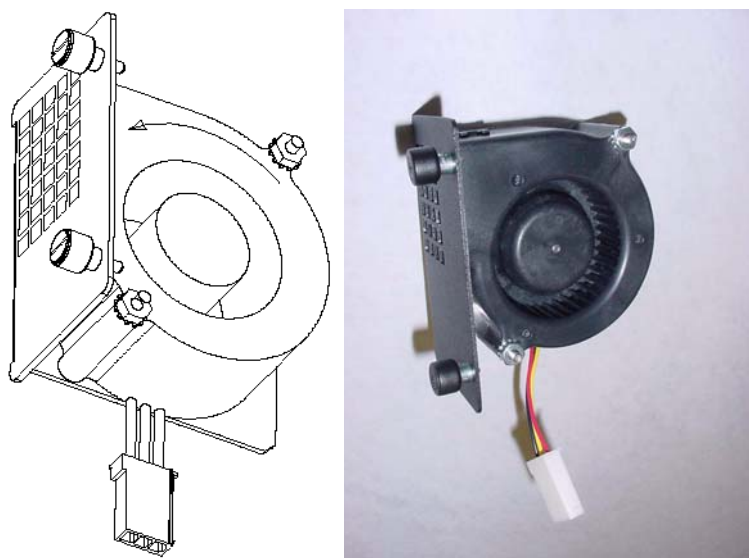


Figure #20 Blower Assembly Diagram Three Quarter View

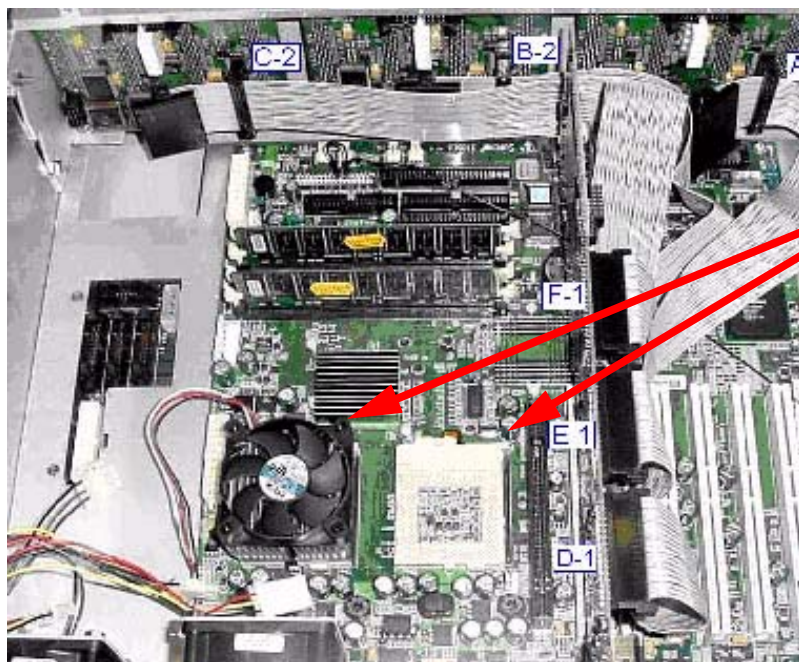


Figure #21 CPU Fan Location With Covers Off

SCSI Interface Connectors to Optional Expansion Enclosures

If your system has an optional expansion enclosure/s, the SCSI Interface Connectors from the Mylex SCSI RAID controller card mounted in the PC card cage are used to interconnect the base unit to the next expansion enclosure. There are four SCSI Ports on the card, only Ports 0, 1, and 3 are used.

The Mylex RAID Controller Card is a field replaceable unit.

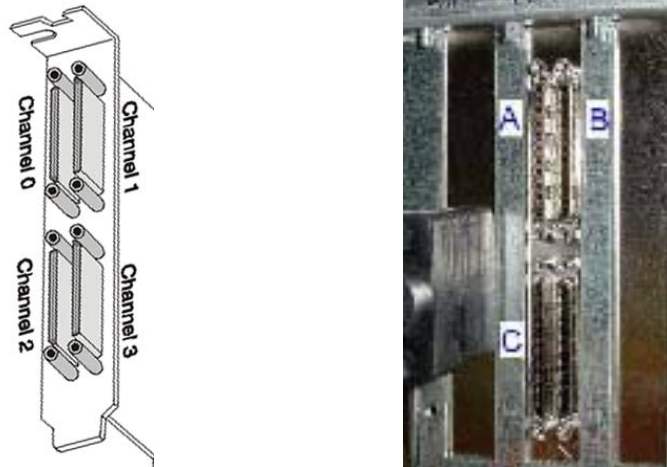


Figure #22 RAID Controller SCSI Connections Diagram and Photo - Channel 2 Not Used

Environmental Monitoring Unit (EMU) Connectors

The EMU is responsible for gathering the environmental status of the connected Base and Expansion Units and then routing the information to the CPU O/S for action. Typical monitoring conditions include temperature, fan rotation, and voltages that are both in and out of specification. These environmental signals in turn generate alerts which are distributed to some combination of LCD panel, LED indicators, email to administrators, web user interface, and SNMP actions.

The EMU is a field replaceable unit.

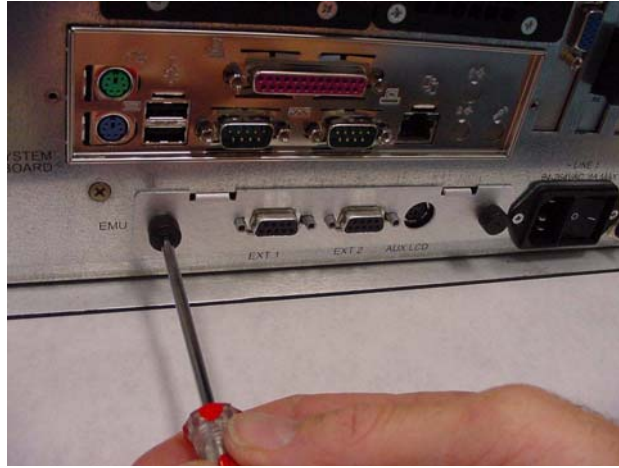


Figure #23 Base Unit Rear View Diagram with EMU

Chapter #3 - Overview - Microsoft Windows O/S Version 2.0

Chapter Outline

- Overview of operating system (O/S)
- Navigation overview
- Home and welcome screens
- Initial system setting screens
- System status screens
- Network configuration screens
- Disks and volumes screens
- Users and groups screens
- Folders and shares screens
- Maintenance screens
- Services for UNIX screens
- Services for NetWare screens



NOTE

For detailed information and instructions about using the Microsoft Windows-Powered Max Operating System Version 2.0, consult the O/S chapters following on each topic such as Network, Folders and Shares, and Maintenance.

O/S Overview



This chapter provides you with a quick overview of the Microsoft Windows-Powered Max Operating System Version 2.0, its screens, and their major functions.

Navigation Overview

The navigation user interface provides both a top of screen two level navigation bar as well as clickable hot links on every page. The figure below shows the primary navigation settings for each top level option.

Navigation Bar > Welcome Tab	
Welcome Status Network Disks Users Shares Maintenance Help ?	
Take a Tour Set Server Appliance Name Set Administrator Password Set Default Page	
Navigation Bar > Status Tab	
Welcome Status Network Disks Users Shares Maintenance Help ?	
System Summary System Health Installed Software Elements Windows System Files Export SysInfo	
Navigation Bar > Network Tab	
Welcome Status Network Disks Users Shares Maintenance Help ?	
Identification Global Settings Interfaces Administrator Administration Web Site SNMP Service Configuration Telnet NIC Configuration DHCP Configuration	
Navigation Bar > Disks Tab	
Welcome Status Network Disks Users Shares Maintenance Help ?	
Disks and Volumes Disk Quota Persistent Storage Manager Disk Defragmenter RAID Configuration	
Navigation Bar > Users Tab	
Welcome Status Network Disks Users Shares Maintenance Help ?	
Local Users Local Groups	
Navigation Bar > Shares Tab	
Welcome Status Network Disks Users Shares Maintenance Help ?	
Folders Shares Sharing Protocols	
Navigation Bar > Maintenance Tab	
Welcome Status Network Disks Users Shares Maintenance Help ?	
Software Update Date/Time Shutdown Logs Backup Terminal Services Alert E-Mail Language Add/Remove Programs Session Time Out	
Computer Management System Recovery Option Re-Image System Drive	

Figure #4 O/S Navigation Bar Tab Settings

Welcome Page

The Welcome page is displayed when you connect to the MaxAttach NAS 6000NAS from a client computer on the network. The navigation bars described above allow you full access to all O/S functions.

The links on the page provide specific access to”

- Take a tour of major O/S features
- Set Administrator Password
- Set Server Appliance Name
- Set Default Page

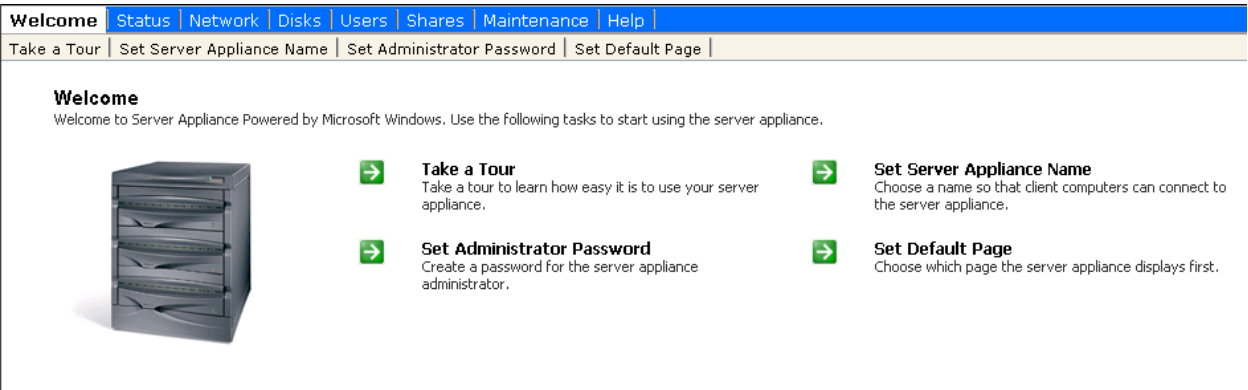


Figure #5 Welcome Page Screen

Take a Tour

Take a Tour shows you how easy it is to use the MaxAttach NAS 6000 and provides an overview of the O/S features and functions.

[Previous](#) [Top](#) [Next](#)

Tour

Using your Windows Powered server appliance couldn't be easier. Whether your appliance is dedicated to providing Network Attached Storage (NAS), dedicated to hosting Web sites, or is designed to provide custom services, you can administer it quickly and easily from a remote computer using the Web user interface (UI). Read the following topics for specific information on how to use your server appliance:

[Getting Started](#)

[Navigation Mode of the Web UI](#)

[Configuring Network Attached Storage](#)

[Configuring a Web Server Appliance](#)

[Disk Management](#)

[Maintenance](#)

[Network Setup](#)

[Share Management](#)

[User Account Management](#)

[Web Server](#)

[Web Site Configuration](#)

Figure #6 Take a Tour Screen

Initial System Settings

Set Server Appliance Name

The Set Server Appliance Name page allows you to:

- Set the name of the server appliance
- Set the DNS suffix
- Become a member of a NT 4 or Active Directory domain or remain a member of a workgroup.
- Set the AppleTalk name.
- Set the NetWare server name.

Server Appliance Identity

Server appliance name:

DNS suffix:

Member of: ☐ Workgroup:

☒ Domain:

Type the information for the user who has permission to join the domain. Include the domain name when you enter the User name (for example: DOMAIN\USER)

User:

Password:

AppleTalk name:

NetWare name:

Figure #7 Set Server Appliance Name Screen

Set Administrator Password

The Set Administrator Password page allows you to change the password of the MaxAttach NAS 6000 administrator account.



Administrator Account

User name: ADMINISTRATOR

Current password:

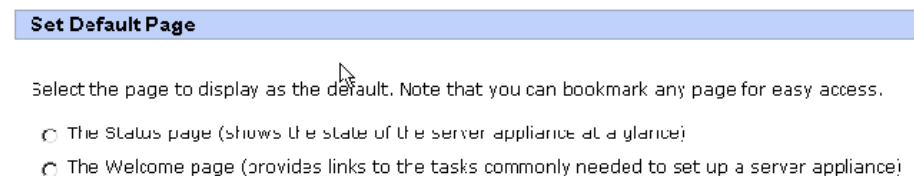
New password:

Confirm new password:

Figure #8 Set Administrator Password Screen

Set Default Page

The Set Default Page allows you to set what page the MaxAttach NAS 6000 displays first. You can display either the Status or Welcome page.



Set Default Page

Select the page to display as the default. Note that you can bookmark any page for easy access.

☐ The Status page (shows the state of the server appliance at a glance)

☐ The Welcome page (provides links to the tasks commonly needed to set up a server appliance)

Figure #9 Set Default Page Screen

System Status Summary

Status Page

From the Status page, you have access to real-time operational and management data for the administration of the MaxAttach NAS 6000. The Status selection options on the secondary menu bar provide access to specialized subsets of system status information:

- System summary
- System health
- Installed software elements
- Windows system files
- Export system information

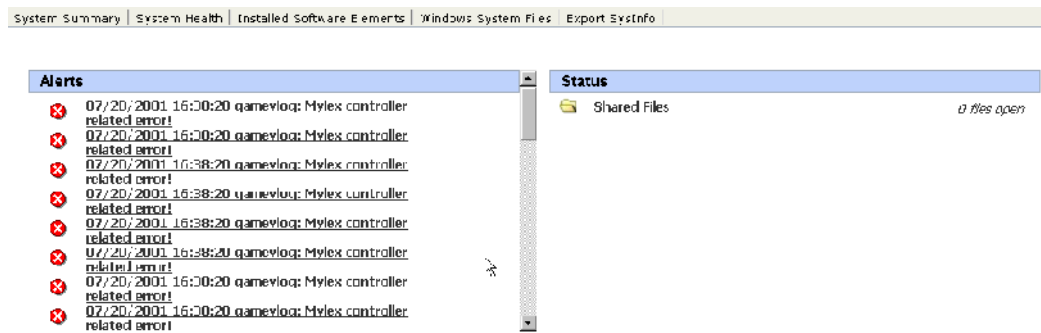


Figure #10 System Status Page Screen

System Summary Page

The Summary Status page provides a quick overview of system configuration information and includes:

- Computer name
- Processor type, manufacturer, and model
- BIOS version and date
- System TCP/IP address
- Total physical memory
- Operating system and version
- Data and time for local system, install date, and last boot up date

- Number of physical disks, total space, and available free space.

System Summary

Computer name:	MA218D1D
Processor:	GenuineIntel x86 Family 6 Model 8 Stepping 6
Processor manufacturer:	Supermicro
Model:	370SSR/370SSE
BIOS version:	AMIBIOS (C)2000 American Megatrends Inc., Version 07.00.00
BIOS date:	06/12/01
TCP/IP address:	192.168.10.34
Total physical memory:	382 MB
Operating system:	Microsoft Windows 2000 Server
Version:	5.0.2195 Service Pack 2 build 2195
Local datetime:	2001/07/17 17:55:35 GMT -7
OS install datetime:	2000/12/31 23:07:25 GMT -8
OS last bootup datetime:	2001/07/17 08:12:02 GMT -7
Number of physical disks:	1
Total hard drive space:	275 GB
Total free hard drive space:	268 GB

Figure #11 System Summary Page Screen

System Health Page

The System Health page provides performance and health metrics for system hardware and major subassemblies including:

- Motherboard
- Processor
- Memory
- Drives
- BIOS
- Network configuration and network adapter cards.

System Health

----- Motherboard -----

Manufacturer:	Supermicro
Model:	370SSR/370SSE
Motherboard temperature:	41 C

System Slots

Description	Bus width	Status
PCI1	32 Bits	OK
PCI2	32 Bits	OK
PCI3	32 Bits	OK
AGP4X	32 Bits	Unknown

Figure #12 System Health Screen

Installed Software Elements

The Installed Software Elements page lists all installed software modules with typically over 100 listed packages or elements. The listing provides information fields of:

- Name of the software package or element
- Version number
- State of the software:
 - For normal operation, the software state is listed as Local, meaning the software is installed on the local machine.
 - Other possible software states include Absent, Error, Bad Configuration, Not Used, or Source Absent.
- Directory location of the software package or element.

Installed Software Elements			
Name	Version	State	Location
SvNfssprop	5.3000.1313.1	Local	C:\WINNT\System32\ntfsprop.dll
AdminUICommonMofFiles	5.3000.1313.1	Local	C:\WINNT\System32\wham\namespre.mof
AdminUIComm	5.3000.1313.1	Local	C:\sf\ADMIN\about.htm
AdminUIMapServer	5.3000.1313.1	Local	C:\sf\ADMIN\main.htm
AdminUIMapServerMofFiles	5.3000.1313.1	Local	C:\WINNT\System32\wbem\mapsvr.mof
AdminUI NFS	5.3000.1313.1	Local	C:\sf\ADMIN\client.htm
AdminUI NFSClient	5.3000.1313.1	Local	C:\sf\ADMIN\disec.js
AdminUI NFS Gateway	5.3000.1313.1	Local	C:\sf\ADMIN\gateway.htm
AdminUI NFS ServerMofFiles	5.3000.1313.1	Local	C:\WINNT\System32\wbem\svraudit.mof
AdminUI NFS Str	5.3000.1313.1	Local	C:\sf\ADMIN\rsrsecut.js
AdminUISfuMsc	5.3000.1313.1	Local	C:\sf\COMMON\sfumgmt.msc

Figure #13 Installed Software Elements Screen

Windows System Files Page

The Windows System Files page lists all the Windows DLL (dynamic linked library) files and all of the Windows SYS (system) files. Within each type of system file, the files are listed alphabetically by file name. Typically several hundred files are listed. The listing provides information fields of:

- File name and DLL or SYS file extension.
- File version
- Size in bytes
- Created date
- Last modified date
- Last access date

- Directory location.

Windows System Files					
Filename	Version	Size	Created date	Last modified date	Last access da
asaaanon.dll	5.00.2163.1	32015	5/5/2011 5:00:00 AM	5/6/2011 5:00:00 AM	7/17/2011 5:57:1
actres.dll	5.50.4522.1200	59904	6/28/2011 9:51:39 AM	5/6/2011 5:00:00 AM	7/17/2011 5:52:5
adedit.dll	5.00.2134.1	131856	5/5/2011 5:00:00 AM	5/6/2011 5:00:00 AM	7/17/2011 5:57:1
adui.dll	5.00.2191.2488	78095	5/5/2011 5:00:00 AM	5/6/2011 5:00:00 AM	7/17/2011 5:57:1
asetuic.dll	5.00.2167.1	4368	5/5/2011 5:00:00 AM	5/6/2011 5:00:00 AM	7/17/2011 5:57:1
asmh.dll	5.00.2167.1	11535	5/5/2011 5:00:00 AM	5/6/2011 5:00:00 AM	7/17/2011 5:57:1
asnap.dll	5.00.2167.1	268048	5/5/2011 5:00:00 AM	5/6/2011 5:00:00 AM	7/17/2011 5:57:1
atvies.dll	5.00.2191.2778	178950	5/5/2011 5:00:00 AM	5/6/2011 5:00:00 AM	7/17/2011 5:52:3
atbprxy.dll	5.50.4522.1300	79120	11/20/2011 4:50:44 PM	10/20/2010 4:50:44 PM	7/17/2011 5:57:1

Figure #14 Windows System Files Screen

Export SysInfo Page

The Export SysInfo page, allows the administrator to export either the system's current status or its original as-shipped status data via e-mail to the Administrator's mailbox.

Export System Information

What type of system information would you like to export to administrator's mailbox?

☒ Current
☐ Original

Export System Information

What type of system information would you like to export to administrator's mailbox?

☒ Current
☐ Original

④ Current system information has been sent out. Please check administrator's mailbox.

Figure #15 Export SysInfo Screen

Network Configuration



NOTE

For detailed procedures within O/S Network Configuration, see **Chapter #5 - O/S 2.0 - Network Configuration** on page 131.

Network Page

The Network page allows you configure the following network-related properties of the MaxAttach NAS 6000:

- Identification
- Global Settings
- Interfaces
- Administrator
- Administration Web Site
- SNMP Service Configuration
- Telnet
- NIC Configuration

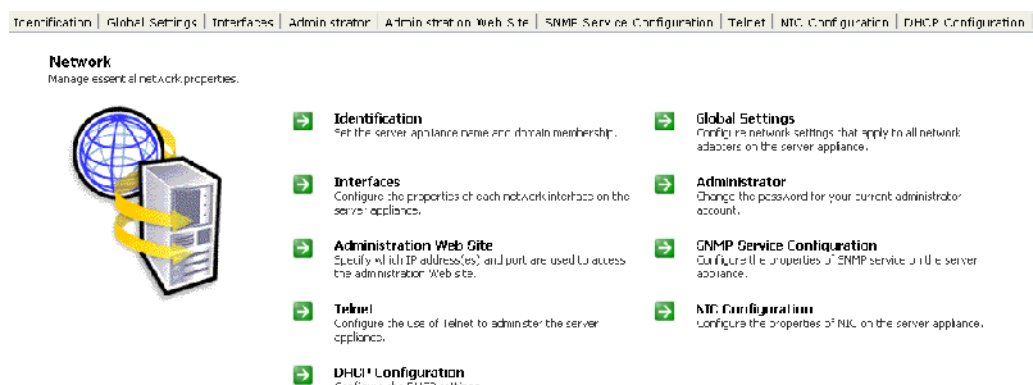


Figure #16 Network Page Screen

Identification Page

The Identification page allows you to:

- Set the name of the server appliance
- Set the DNS suffix
- Become a member of a NT 4 or Active Directory domain or remain a member of a workgroup
- Set the AppleTalk name

- Set the Netware name.

Server Appliance Identity

Server appliance name:

DNS suffix:

Member of:

☐ Workgroup:

☒ Domain:

Type the information for the user who has permission to join the domain. Include the domain name when you enter the User name (for example: DOMAIN\USER)

User:

Password:

AppleTalk name:

NetWare name:

Figure #17 Server Appliance Identify Identification Page Screen

Server Appliance Name

The server appliance name is the name of the server appliance on a network. The server appliance name must be unique and must meet certain requirements. The new server appliance name cannot be the same as another computer or the name of a Microsoft Windows domain.

It is recommended that you use names that are 15 characters or fewer. The server appliance name can be a maximum of 63 characters but should only contain the numbers 0-9, the uppercase letters A-Z, the lowercase letters a-z, or hyphens. You may use other characters, but doing so may prevent other users from finding your computer on the network. If your network is using the Microsoft DNS server, you can use any characters except periods.

If other networking protocols are installed without TCP/IP, the server appliance name is limited to 15 characters.

If you specify a server appliance name longer than 15 characters and you want longer names to be recognized by the Microsoft Active Directory domain, the domain administrator must enable registration of DNS names that are 16 characters or longer.

DNS Suffix

Domain-name system (DNS) suffixes have the following two primary purposes:

1. When appended to the server appliance host name, DNS suffixes constitute the fully qualified server appliance name.

2. To resolve IP addresses. If your server appliance is a member of Windows NT 4 domain, a Microsoft Active Directory, or a workgroup, the DNS suffix is dependent upon the domain environment.

Including hyphens and periods, a DNS suffix may contain up to 155 characters.

The MaxAttach NAS 6000 supports automatic DNS entry into an ADS domain. If you are using a Windows NT 4.0 DNS server, you will need to manually enter the MaxAttach NAS 6000 into the DNS database.

Domain

Your server appliance can be in a workgroup, active directory environment, or Windows NT 4 domain. In Microsoft Windows NT 4 and Microsoft Active Directory environments, a domain is a collection of computers defined by the administrator of a network that share a common directory database.

Utilized for Windows user and group information, Windows domains have a unique name and provide access to the centralized user accounts and group accounts maintained by the domain administrator. Each domain has its own security policies and security relationships with other domains, and each domain represents a single security boundary of a Windows computer network. Active Directory is made up of one or more domains, each of which can span more than one physical location.

For DNS, a domain is any tree or subtree within the DNS name space. Although the names for DNS domains often correspond to Active Directory domains, DNS domains should not be confused with Microsoft Windows and Active Directory networking domains.

By default a domain user must enter domain\user name when logging into a Web server appliance or a MaxAttach NAS 6000 with a browser.

Workgroup

A workgroup is a simple grouping of computers, intended only to help users find such things as printers and shared folders within that group. Your server appliance can be in a workgroup, active directory environment, or Windows NT 4 domain. Workgroups in Microsoft Windows 2000 do not offer the centralized user accounts and authentication offered by domains.

A workgroup name must not duplicate the computer name. A workgroup name can have as many as 15 characters, but cannot contain any of the following characters: ; : " < > + = \ | ? , .

AppleTalk Name

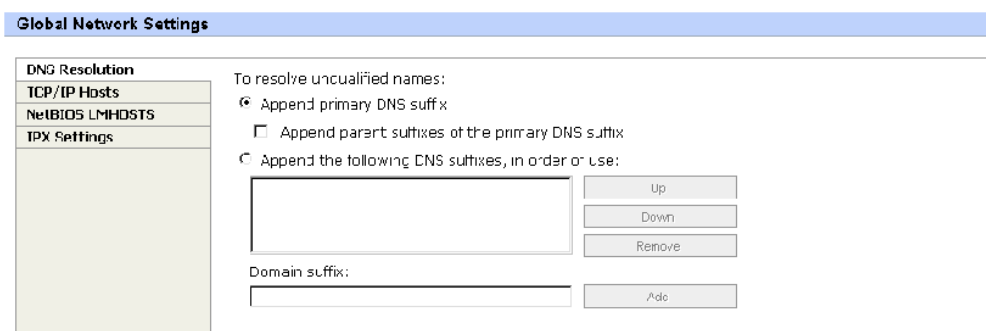
By default, the AppleTalk name will be the same as the standard server name. If you change the server name, the AppleTalk name will automatically change.

NetWare Name

The NetWare name must be different from the server appliance name. By default, the NetWare name will be the server appliance name with _FPNW appended to it.

Global Settings Page

The Global Settings page allows you to change the overall network settings for your server appliance by configuring the IPX settings as well as specifying the DNS suffixes and the LMHOSTS and HOSTS file to use. These files can be used to resolve the names of any computer or device.



The screenshot shows the 'Global Network Settings' window with the 'DNS Resolution' tab selected. On the left is a sidebar with links: 'DNS Resolution', 'TCP/IP Hosts', 'NetBIOS LMHOSTS', and 'IPX Settings'. The main area is titled 'To resolve unqualified names:' and contains two radio button options. The first option, 'Append primary DNS suffix', is selected. Below it is an unchecked checkbox for 'Append parent suffixes of the primary DNS suffix'. The second option, 'Append the following DNS suffixes, in order or use:', is also selected. This option includes a list box (currently empty) with 'Up', 'Down', and 'Remove' buttons to its right. Below the list box is a 'Domain suffix:' label followed by a text input field and an 'Add' button.

Figure #18 Global Network Settings - DNS Resolution Tab

DNS Name Resolution Tab

So that people can reach your Web site on an intranet or the Internet, you must have a unique IP address that identifies your computer on the network. This address consists of a long string of numbers separated by dots, for example, 172.16.255.255. Because a numeric address is difficult for people to remember, text names, or friendly names, are used to provide visitors with an easy-to-remember address, such as www.microsoft.com. Name resolution involves supplying the correct numerical address from the friendly name that was typed into a client browser.

Name Resolution Systems

Windows networking components rely on the NetBIOS naming convention. In contrast, TCP/IP components rely on a naming convention known as the Domain Name System (DNS). Under Windows, the DNS host name of your server appliance defaults to the same name as the NetBIOS computer name. The mapping of computer names to IP addresses can be accomplished using one of the following two methods:

- **Static**
 - The system administrator creates either a text file for DNS names, called a HOSTS file, or an LMHOSTS file for NetBIOS names, and enters each computer's name and IP address.
 - The file is then distributed on the network.
 - When a request for a connection to another computer is made, the file is used to resolve the name to the correct IP address.
 - This system works well for simple networks that change infrequently.
- **Dynamic**
 - When a client computer connects to a network with a DHCP server, the DHCP server assigns an address and sends the IP address assignment to a Windows Internet Name Service (WINS) server.
 - The WINS server registers the computer's name, and when a request is made for a NetBIOS computer name, the WINS server resolves the name to the correct IP address.
 - This automatic recognition and mapping of computer names and addresses eases the administrative burden of large or frequently changing networks.

DNS names are typically resolved using static information. The DNS server contains a portion of the static database listing host names and addresses. If the requested name is not in the DNS server's portion of the database, it sends a query to other DNS servers to get the requested information. The DNS server that runs on Windows can be configured to query a WINS server for name resolution of the lower levels of the DNS hierarchical naming structure. Because WINS assigns computer names dynamically, this effectively changes DNS from a static system to a dynamic system.

TCP/IP Hosts Tab

Windows networking components rely on the NetBIOS naming convention. In contrast, TCP/IP components rely on a naming convention known as the Domain Name System (DNS). Under Windows, the DNS host name defaults to the same name as the NetBIOS computer name. The mapping of computer names to IP addresses can be accomplished using one of the following two methods:

- **Static**

- The system administrator creates either a text file for DNS names, called a HOSTS file, or an LMHOSTS file for NetBIOS names, and enters each computer's name and IP address. The file is then distributed on the network. When a request for a connection to another computer is made, the file is used to resolve the name with the correct IP address. This system works well for simple networks that change infrequently.
- Dynamic
 - When a client computer logs on, a DHCP server assigns an address and sends the IP address assignment to a Windows Internet Name Service (WINS) server. The WINS server registers the computer's name, and when a request is made for a NetBIOS computer name, the WINS server resolves the name to the correct IP address. This automatic recognition and mapping of computer names and addresses eases the administrative burden of large or frequently changing networks.

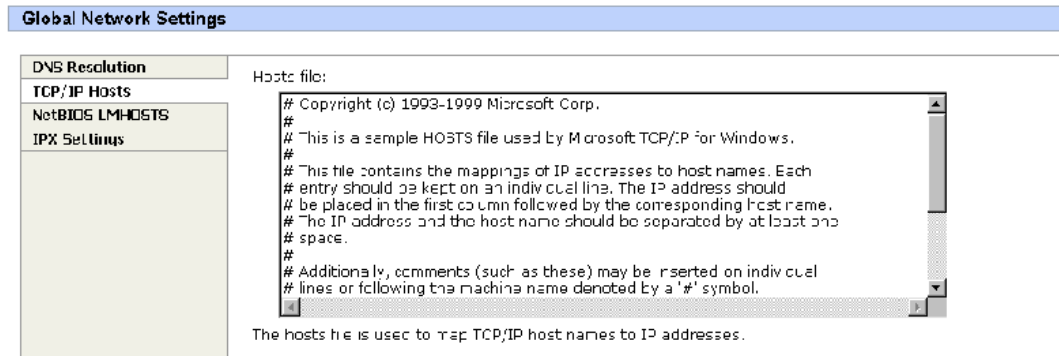


Figure #19 Global Network Settings - TCP/IP Hosts Tab

If you are setting up multiple Web or FTP sites on a single server, each with its own IP address, you might encounter problems with automatic DNS registration. To ensure correct IP binding and DNS registration, disable Windows 2000 Server automatic DNS registration and manually configure DNS registration for the Web sites. For more information about disabling automatic DNS registration and manually configuring DNS registration, see the Windows 2000 Server documentation.

If you want to assign multiple names to one server appliance, you must use a static name assignment for the server appliance. On one computer you can map multiple names to one IP address or you can use multiple names, each one mapped to its own IP address.

NetBIOS LMHOSTS Tab

The use of an LMHOSTS file is optional. If an LMHOSTS file is not used, however, you cannot use friendly text names. Instead, you must use IP addresses. This can be a disadvantage because Web sites on the Internet usually use the DNS. If you register a domain name for your Web site, users can contact your Web site by typing its domain name in a browser.

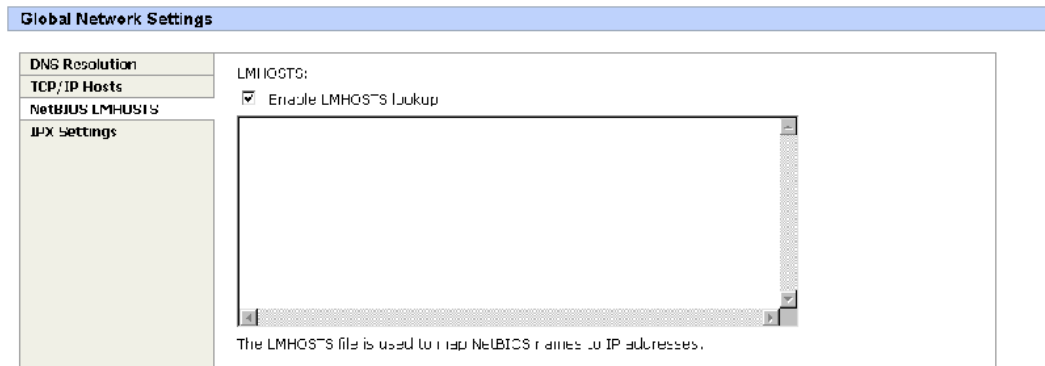


Figure #20 Global Network Settings Screen - NetBIOS LMHOSTS Tab

The LMHOSTS file is read when WINS or broadcast name resolution fails and resolved entries are stored in a system cache for later access. When the computer uses the replication service and does not use WINS, LMHOSTS file entries are required on import and export servers for any computers on different subnetworks participating in the replication.

IPX Settings Tab

Internetwork Packet Exchange (IPX) is the native NetWare protocol used on many earlier Novell networks.

To be accessible from clients running NetWare, your server appliance must provide an IPX address.

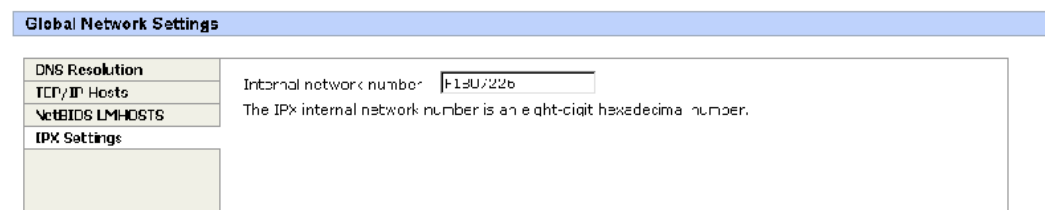


Figure #21 Global Network Settings Screen - IPX Settings Tab

Interfaces Page

The Interfaces page allows you to configure the local network settings on the MaxAttach NAS 6000 device. From this page, you can:

- Change the name of the connection.
- Set or change the Internet Protocol (IP) and gateway addresses, subnet masks, and metrics.
- Set or change how the server appliance resolves DNS names.
- Set or change the configuration of the Windows Internet Naming Service (WINS) clients.
- Configure AppleTalk.

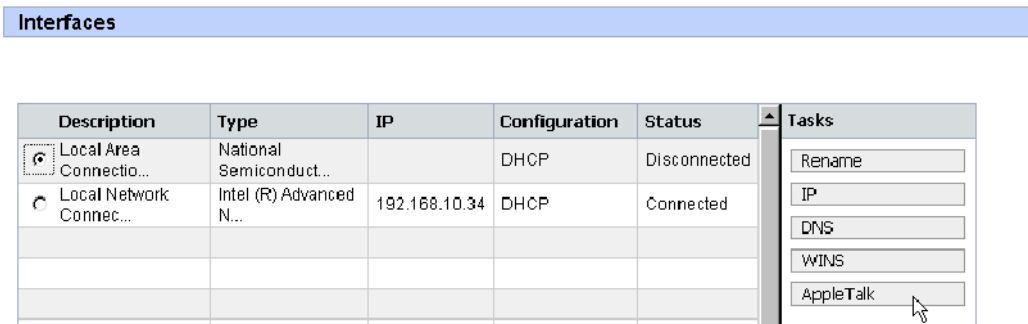


Figure #22 Interfaces Page Screen

Interfaces Page - Rename Link

The Rename page allows you to change the name of the connection.

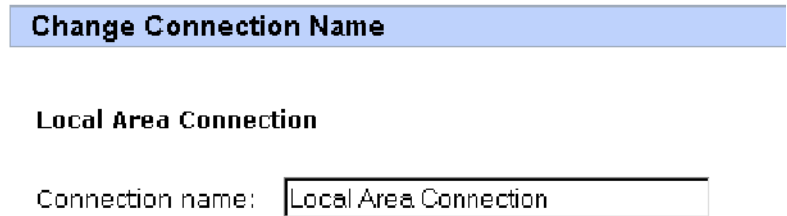


Figure #23 Rename Page Screen

Interfaces Page - IP Link

Each computer on the network must have a unique IP address to send and receive data. You can use the IP Address Configuration page to have your server appliance automatically obtain the IP address configuration from the Dynamic Host Configuration Protocol (DHCP) server. Alternately, you can configure the IP address(es) manually.

The figure shows two overlapping screenshots of the 'IP Address Configuration' window. The top screenshot displays the 'General' tab, which has two radio buttons: 'Obtain configuration from DHCP server' (selected) and 'Use the following IP settings:'. Below these are input fields for 'IP address', 'Subnet Mask', and 'Default gateway'. The bottom screenshot displays the 'Advanced' tab, which features a list of 'IP addresses' with 'Add' and 'Remove' buttons. It also has a 'Gateway addresses' section with similar buttons, and a 'Metric' field. A note at the bottom explains that the metric indicates the cost of using a route, typically the number of hops to the destination.

Figure #24 IP Address Configuration Screen - General and Advanced Tabs

In addition, you can use the IP Address Configuration page to specify one or more gateway addresses. A gateway address is the address of a local IP router residing on the same network as the server appliance that is used to forward traffic to destinations beyond the local network. The value in each field must be a number from 0-255.



NOTE

CHANGING IP ADDRESSES: Changing the IP address may cause the client to lose its connection with the server appliance. To reconnect, the user must either use the new IP address or wait until the DNS server is updated.

Interfaces Page - DNS Link

The domain-name system (DNS) is a static, hierarchical name service for TCP/IP hosts. The network administrator configures the DNS with a list of host names and IP addresses. This allows users on the network to query the DNS to specify remote systems by host names rather than IP addresses.

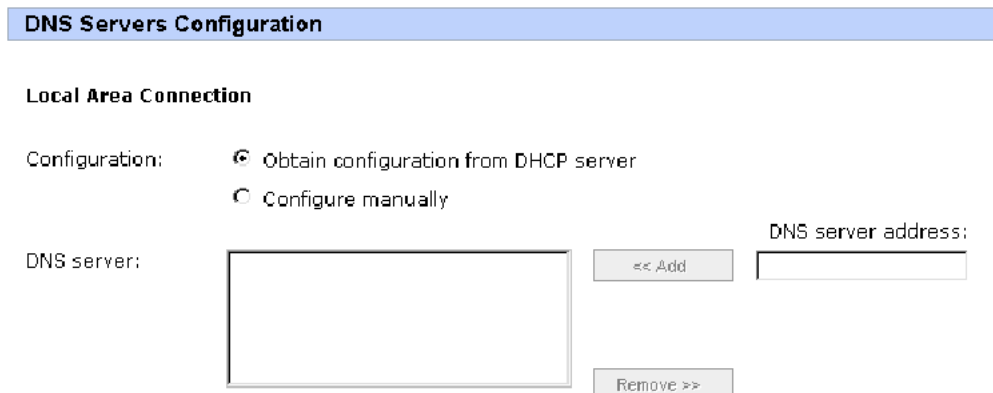


Figure #25 DNS Servers Configuration Screen



NOTE

DNS PAGE PURPOSE: The purpose of this property page is to allow you to enter the addresses of **EXTERNAL** DNS servers. The MaxAttach NAS 6000 does not contain a DNS server.

Interfaces Page - WINS Link

WINS clients attempt to register their names with a WINS server when they start or join the network. Thereafter, WINS clients query the WINS server as needed to resolve remote names.

WINS-enabled clients are computers that can be configured to make direct use of a WINS server. Most WINS clients typically have more than one NetBIOS name that they must register for use with the network. These names are used to publish various types of network service, such as the Messenger or Workstation Service, that each computer can use in various ways to communicate with other computers on the network. WINS-enabled clients communicate with the WINS server to:

- Register client names in the WINS database.
- Renew client names with the WINS database.
- Release client names from the WINS database.
- Resolve names by obtaining mappings from the WINS database for user names,

NetBIOS names, DNS names, and IP addresses.

WINS Servers Configuration

Local Area Connection

Configuration: ☒ Obtain configuration from DHCP server

☐ Configure manually

WINS servers:



<< Add

WINS server address:

Remove >>

Figure #26 WINS Servers Configuration Screen

Clients that are not WINS-enabled can use WINS proxies to participate in these processes in a limited way. If you are using a DHCP server to allocate WINS server IP addresses, you do not need to add WINS server addresses.

Keep in mind that the Web UI only allows you to manipulate two WINS addresses, and even then only if you statically assign the IP address for the adapter. If you have DHCP enabled, you can remove one or two existing addresses and add different addresses, but you will not be able to remove all WINS servers from a DHCP-enabled adapter. If you remove two WINS addresses and do not add at least one, DHCP will automatically assign WINS addresses.



NOTE

WINS PAGE PURPOSE: The purpose of this property page is to allow you to enter the addresses of EXTERNAL WINS servers. The MaxAttach NAS 6000 does not contain a WINS server.

Interfaces Page - AppleTalk Link

Use the AppleTalk Configuration page to specify which network adapter can receive inbound AppleTalk connections and in which AppleTalk zone the MaxAttach will appear. Only one AppleTalk adapter per system can be configured to receive inbound traffic.

Figure #27 AppleTalk Configuration Page

Administrator Account Page

The MaxAttach NAS 6000 server appliance comes with a set of default accounts. Only the administrator account has administrative privileges.

Figure #28 Administrator Account Screen



NOTE

DOMAIN ACCOUNTS AND ADMINISTRATORS: If an administrator adds a domain account to the local administrators group, the domain user may access and administer the server appliance. However, the administrator cannot use the Change Administrator Password page to change his domain account password. This page can only be used to change the local administrator's account password.

When you change the administrator password, there is no explicit confirmation page. However, the password is successfully changed if no error message appears after you have submitted the change.

**NOTE**

CHANGING THE ADMINISTRATOR PASSWORD: You cannot change the administrator password if you are logged on as a domain user as it is outside the scope of the server appliance Web UI to make changes to domain user accounts. Domain user accounts are stored on the domain controller, not on the server appliance.

In this context, administrator relates to the user account that is a member of the local administrators group and is used by a current user to log on. It does not refer to the default administrator account, called **administrator**.

If you receive the error message “**The password cannot be changed for this domain account**” or “**The account name cannot be changed for this domain account**” when trying to change the administrator password or account name, you are logged on as a domain user. You must be logged on as the server appliance administrator to change the administrator password.

Administration Web Site Properties Page

This feature allows you to change the IP address and port that can be used to access the administration Web site on the server appliance.

The default IP address to which the server appliance responds, or listens, is typically changed when the server appliance is only managed on a certain subnet or a separate management network.

The default listen ports for both encrypted and non-encrypted access can be modified as needed to work with existing network software and configurations, for example, when no traffic above a given port number is allowed.

Figure #29 Administration Web Server Properties

SNMP Service Configuration Page

From the SNMP Service Configuration page, you can edit the values as needed on the Agent, Traps and Security tabs. Double-click **SNMP Service** to access the SNMP Service Properties page.

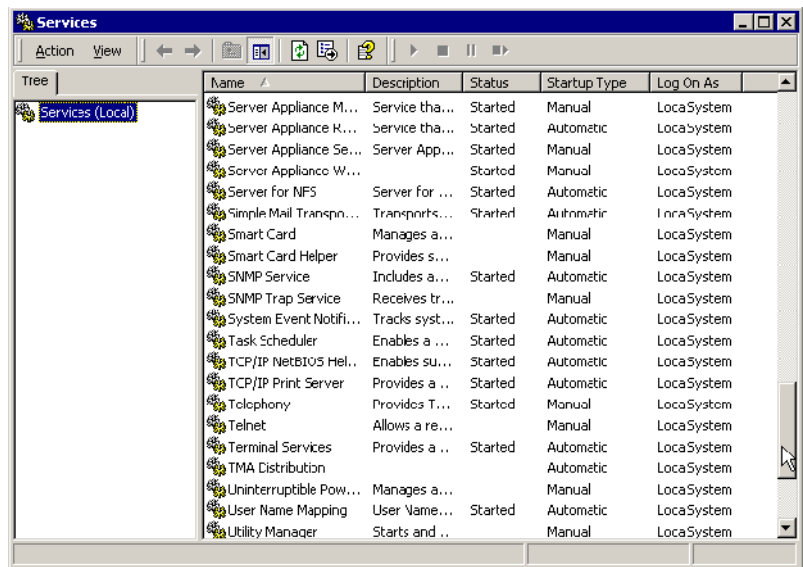


Figure #30 SNMP Service Configuration Screen

Related Topics

- See the *Appendix - SNMP Management System* for detailed information about SNMP features and functions.

Telnet Page

The Telnet page allows you to administer your Windows-Powered server appliance from a remote system using the Telnet protocol. You can log onto the system from a remote Telnet client and run character-mode applications on the server appliance. The Telnet server included with your server appliance supports a maximum of two Telnet clients at any time, unless otherwise specified by your server appliance hardware manufacturer.

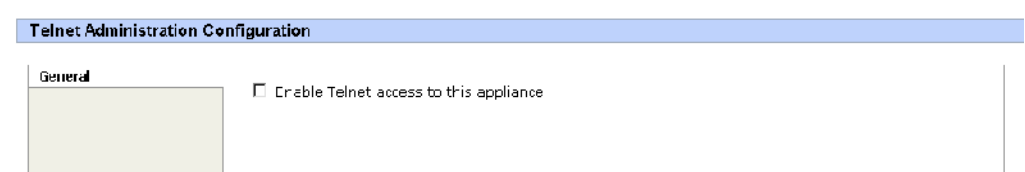


Figure #31 Telnet Administration Screen

NIC Configuration Page

- The Network Interface Card (NIC) adapters supplied with the MaxAttach NAS 6000 can vary, depending on which adapters were ordered and whether the system has been upgraded.

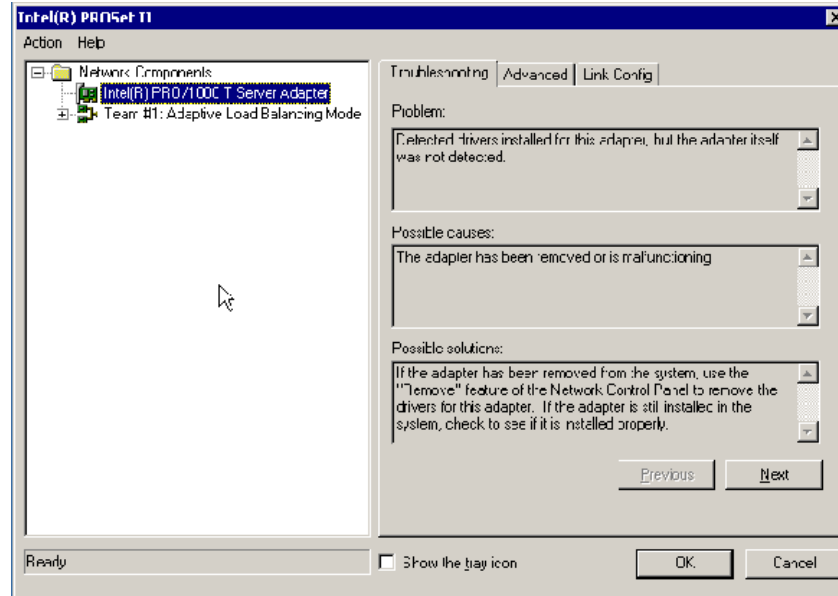


Figure #32 NIC Configuration Screen

In addition to the Base Unit chassis 10/100 Mb/s Ethernet adapter network port on the CPU I/O panel, the system is equipped with two additional NICs

- a gigabit Ethernet NIC with copper wire connections
- a gigabit speed Ethernet NIC with fiber optic connections

To determine which NICs are installed in your system, locate the card cage at the back of the MaxAttach NAS 6000 and match the connector patterns with those shown in the diagram.

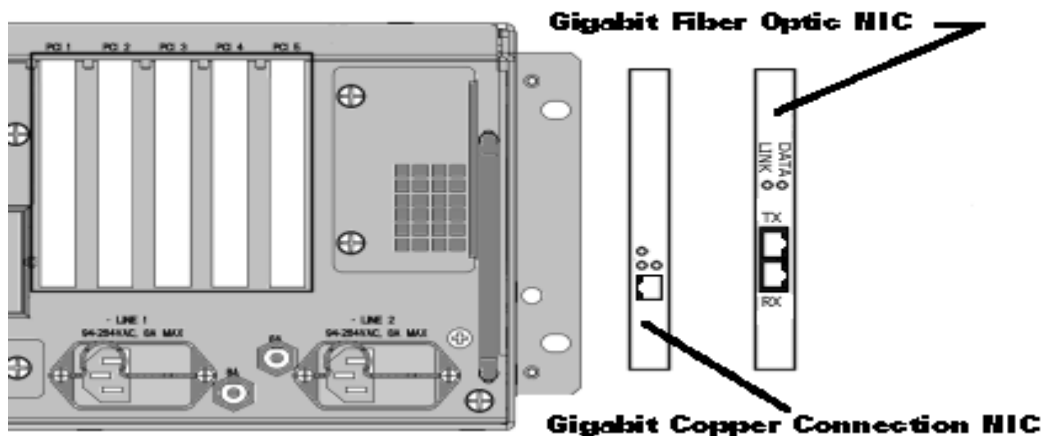


Figure #33 Base Unit Back Panel NIC Identification

Base Unit Network Port

Every system is equipped with a standard IEEE 802.3/IEEE 802.3U-LAN-compliant 10BaseT/100BaseTX Ethernet port. It is supplied on the CPU I/O Panel of the Maxtor MaxAttach NAS 6000 Base Unit chassis.

The LAN connector for this port is a standard RJ-45 type, compatible with standard CAT 3, 4, and 5 UTP cabling for 10BaseT operation (10 Mb/s) and Cat-5 UTP cabling for 100BaseTX operation (100 Mb/s).

Standard NIC Configuration

The software drivers for each NIC have been pre-installed at the factory. There is no user configuration required other than entering local area network parameters (IP address, server name, domain and workgroup, etc.).

Every installed NIC should be connected to a separate subnet and be assigned a unique IP address. The architecture of the network permitting, clients can access the MaxAttach with any of its IP addresses.

All NICs are initially configured as DHCP clients at the factory so that they will get their IP addresses and other network parameters from a DHCP server. If there is no DHCP server on your network, the administrator must assign fixed network parameters to each NIC.

When you start the Maxtor MaxAttach NAS 6000 for the first time and it does not find a DHCP server, it assigns itself a temporary IP address (169.254.*nn.mm*, where *nn* and *mm* are random integers in the range of 0 - 255). Use MaxNeighborhood Discovery and Setup Wizard to discover the MaxAttach NAS 6000's temporary IP address, then use Internet Explorer running on a client computer to access the Maxtor MaxAttach NAS 6000 at its temporary IP address and follow the steps of the O/S First Time Setup Wizard to set the required network parameters.

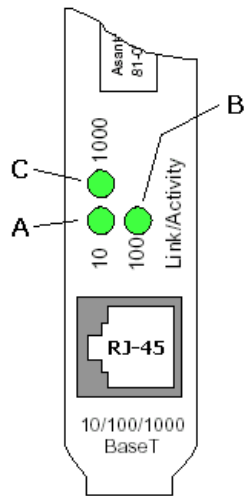
**NOTE**

Initially, connect only one MaxAttach NIC to the network. MaxNeighborhood should be run on a client computer attached to the same network subnet, since it may not see a MaxAttach (with IP 169.254.*nn.mm*) across a network router or switch.

All other setup operations for the installed network interfaces are automatic. There are no other user controls or adjustments. The devices automatically detect the network speed and configure themselves for optimum throughput.

Gigabit Ethernet NIC with Copper Connections

The gigabit network interface card is a full-duplex gigabit Ethernet interface that is fully compliant with IEEE 802.3z for UTP and fully compliant with IEEE 802.3ab and IEEE 802.3u. The interface is compatible with all 10/100/1000BaseT hubs, switches and routers. It can provide sustained throughput of up to 1 Gb/s.



LED #A is ON when the adapter is at 10 Mbits/second.

LED #B is ON when set to 100 Mbits/second.

LED #C is ON when set to 1000 Mbits/second.

LED steady ON for an established valid network link.

LED slow blinking during transmit or receive network activity.

Figure #34 Gigabit NIC with Copper Connections Status LEDs

The gigabit Ethernet NIC has an RJ-45 connector for connection of Category 5 or 5E copper cabling. The maximum cable length is 100 meters or 328 feet.

There are three LEDs on the gigabit NIC connector plate, one for each port speed option: 10 Mbps (Ethernet), 100 Mbps (Fast Ethernet), and 1000 Mbps (Gigabit Ethernet).

- The A LED is ON when the adapter is at 10 Mb/s.
- The B LED is ON when the adapter is at 100 Mb/s.
- The C LED is ON when the adapter is at 1000 Mb/s.
- A LED is ON when there is a valid network link established.
- A LED flashes slowly during network activity (transmit or receive).

The required software drivers have been pre-installed at the factory and there is no user configuration required.

Gigabit Ethernet NIC with Fiber Optic Connections

The gigabit Ethernet NIC with fiber optic connections connects the MaxAttach NAS 6000 to a gigabit Ethernet network via a standard fiber interface. It is fully interoperable with existing Ethernet equipment and operates at 1 gigabit per second (Gb/s) in full-duplex mode when connected to a gigabit Ethernet port.

The NIC supports standard Ethernet minimum and maximum frame sizes (64 to 1518 bytes), frame format, and IEEE 802.2 LLC specifications. The underlying NIC technology ensures high performance and maximum bandwidth availability to prevent server congestion and complies with the IEEE 802.3z full-duplex gigabit Ethernet fiber interface standard and with the IEEE 802.3x frame-based flow control standard.

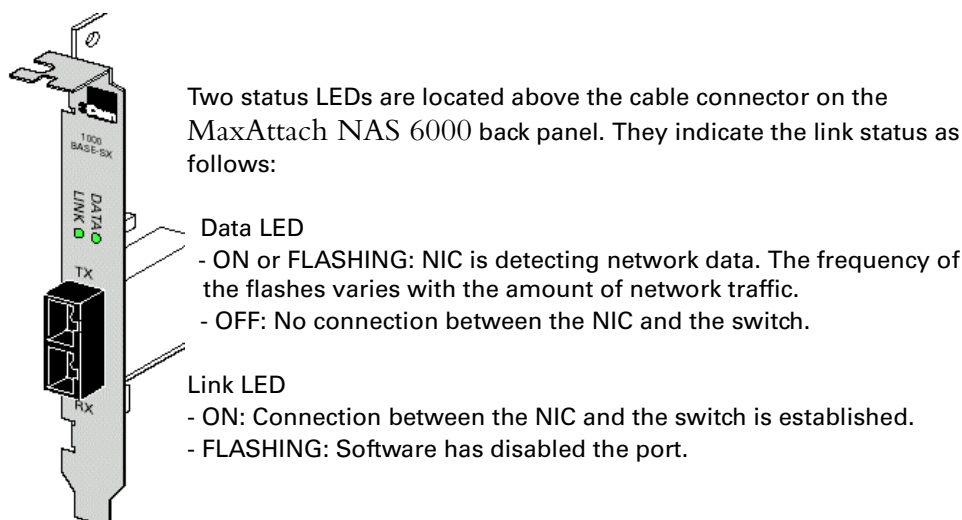


Figure #35 Gigabit Ethernet NIC with Fiber Optic Connections Status LEDs

The gigabit Ethernet NIC with fiber optic connections connects to the network via standard SC/MMF cabling. Compliant cabling types and maximum transmission distances are shown in the table below.:

Table #1 - Cabling Types and Distances					
Signal Type	Connector Type	Cable Type	Cable Diameter (Microns)	Modal Bandwidth (MHz*km)	Maximum Length Feet (Meters)
1000BASE-SX	SC	MMF	62.5	160	722 (220)
Short wavelength (850 nm)	SC	MMF	62.5	200	902 (275)
			50	400	1641 (500)
			50	500	1805 (550)

Two status LEDs are located above the cable connector on the MaxAttach NAS 6000 back panel. They indicate the link status as follows:

- Data LED

- On or flashing: NIC is detecting network data. The frequency of the flashes varies with the amount of network traffic.
- Off: No connection between the NIC and the switch.
- Link LED
 - On: Connection between the NIC and the switch is established.
 - Flashing: Software has disabled the port.
 - Off: No connection between the NIC and switch.

The required software drivers have been pre-installed at the factory and there is no user configuration required.

Disks and Volumes



NOTE

For detailed procedures within O/S Disks and Volumes Configuration, see **Chapter #6 - O/S 2.0 - Disk and Volume Properties** on page 168.

Disks Page

From the Disks page, you can:

- Configure the properties of individual disks and volumes residing on the MaxAttach NAS 6000.
- Configure disk quotas for volumes on the MaxAttach NAS 6000.
- Use Persistent Storage Manager to take point-in-time snapshots of selected volumes.
- Defragment the disks
- Configure the disk array using the Mylex GAM software.

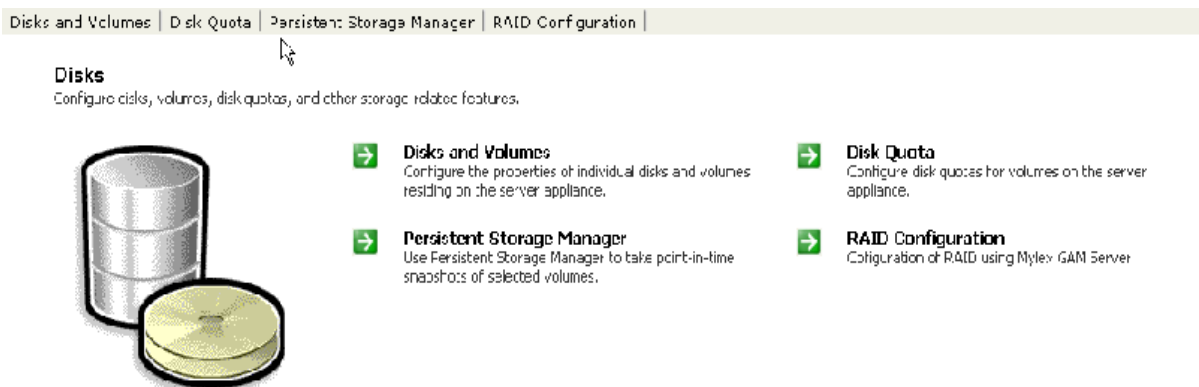


Figure #36 Disks Page Screen

Disks and Volumes

From the Disks and Volumes page, you can choose to configure the disks or volumes on the server appliance. To manage disks and volumes on the server appliance you need to log on to Terminal Services Advanced Client.

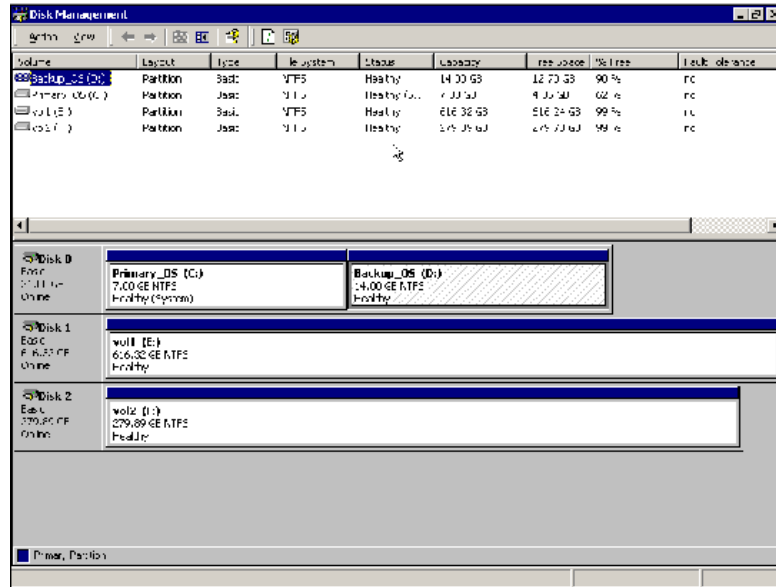


Figure #37 Disks and Volumes Page Screen

Terminal Services Advanced Client

Terminal Services Advanced Client is a general purpose tool that gives you full access to your server appliance. When accessed using the Disks and Volumes page, the Terminal Services Advanced Client assumes a dedicated mode and can only be used to manage disks and volumes on your server appliance.

Terminal Services Advanced Client supports only two concurrent connections. Additionally, if you navigate to another page during an open session, the client will be disconnected but the session will be preserved.

Disk Quotas Page

Disk quotas track and control disk space use in volumes. You can configure the volumes on your server appliance to perform the following tasks:

- Prevent further disk space use and log an event when a user exceeds a specified disk space limit.

- Log an event when a user exceeds a specified disk space warning level.

Volumes and Quotas

Select a volume, and then choose a task. To create a new quota entry for a user, select a volume and choose Quota Entries.

Search:

Volume Name	Total Space	Free Space	Tasks
<input checked="" type="radio"/> bkup_os (D:)	5122 MB	130 MB	<input type="button" value="Quota..."/>
<input type="radio"/> prim_os (C:)	5122 MB	2033 MB	<input type="button" value="Quota Entries..."/>
<input type="radio"/> raid5 (E:)	271305 MB	271231 MB	

Figure #38 Disk Volumes and Quotas Page Screen

Disk Quota Page - Quota Link

When you enable disk quotas, you can set both the disk quota limit and the disk quota warning level. The disk quota limit specifies the amount of disk space a user is allowed to use. The warning level specifies the point at which a user is nearing his or her quota limit. For example, you can set a user's disk quota limit to 50 megabytes (MB), and the disk quota warning level to 45 MB. In this case, the user can store no more than 50 MB on the volume. If the user stores more than 45 MB on the volume, you can have the disk quota system log a system event.

Default Quota for raid5 (E:)

☐ Enable quota management

☒ Deny disk space to users exceeding quota limit

Select the default quota limit for new users on this volume:

☒ Do not limit disk usage

☐ Limit disk space to:

Set warning level to:

Log the quota limit event:

☐ When user exceeds their quota limit

☐ When user exceeds their warning level

Figure #39 Default Quota Page Screen

In addition, you also can specify that users can exceed their quota limit. Enabling quotas and not limiting disk space use is useful when you do not want to deny users access to a volume, but want to track disk space use on a per-user basis. You can also specify whether or not to log an event when users exceed either their quota warning level or their quota limit.

When you enable disk quotas for a volume, volume usage is automatically tracked from that point forward, but existing volume users have no disk quotas applied to them. You can apply disk quotas to existing volume users by adding new quota entries on the Quota Entries page.

Disk Quotas Page - Quota Entries

When you enable disk quotas on a volume, every user's disk volume usage is monitored and treated differently depending on the quota management settings for the specific user. For example, users who have write access to the volume and who have not exceeded their quota limit can store data on the volume. The first time a user writes data to a quota-enabled volume, default values for the disk space limit and the warning level are automatically assigned by the quota system.

Quota Entries on raid5 (E:)

Select a quota entry, then choose a task. To create a new quota entry for a user, choose New.

<input type="checkbox"/> Logon Name ▾	Status	Space Used	Quota Limit	Warning Limit	Tasks
					New..
					Delete
					Properties...

Figure #40 Quota Entries Page Screen

The Quota Entries page allows you to add, delete, or configure disk quotas for any server appliance user. Quotas are managed using the Object/Task Selector, which has the following columns:

- **Logon Name** - This column displays the logon name of each user with registered access to the server appliance.
- **Status** - This column indicates whether or not the user has exceeded the assigned quota limit.
- **Amount Used** - This column indicates the amount of disk space currently being used

by a given user.

- Quota Limit - This column indicates the maximum amount of disk space that a user can occupy on a volume.
 - How the server appliance behaves when the quota limit is exceeded depends on the settings on the Quota property page, accessible through the Disk Quota tab.
 - If the Deny disk space to users exceeding quota limit check box is selected, the user will not be able to exceed this limit.
 - If the Log event when a user exceeds their quota limit check box is selected, an event log message will be logged.
 - If neither option is selected, no action is taken.
- Warning Level - This column indicates the maximum amount of disk space that a particular user can use before a warning appears indicating that the quota has nearly been reached.



NOTE

QUOTA LIMIT WARNING: A warning will only be generated if the user exceeds the warning limit specified on the Quota Entries page, and if a Log event is selected on the Default Quota page. If the Log event check box is not selected, no warning will be generated and this column will remain empty. Typically the Warning Limit value is set slightly fewer than the Quota Limit value.

Persistent Storage Manage Page

Persistent Storage Manager allows you to create snapshot images of volumes on the server appliance. These snapshots, called persistent images, preserve data on selected volumes in case of a system or power failure. Each persistent image is saved as a volume on the file system to allow clients read-only or read/write permission. You can create a persistent image immediately through this configuration system or schedule it as a one-time or recurring event.

The Persistent Storage Manager page allows you to:

- Set the global parameters
- Configure each volume
- Create one-time or recurring persistent image schedules of scheduled volumes
- Create or view persistent images and their properties

■ Use existing persistent images to recover data

Persistent Storage Manager

Create, manage, and restore snapshots of selected volumes to protect against data loss.



Global Settings

Select the global parameters for Persistent Storage Manager.



Volume Settings

Configure each Persistent Storage Manager volume.



Schedules

Create one-time or recurring persistent image schedules of selected volumes.



Persistent Images

Create or view persistent images and their properties.



Restore Persistent Images

Use existing persistent images to recover data.



Figure #41 Persistent Storage Manager Home Page Screen

Once created, a persistent image of a volume appears as a directory on the original volume. The image inherits permission rights from the original volume. Images are used the same as conventional system volumes. However, unlike conventional volumes, persistent images can be restored to the precise content of the original volume at the time the snapshot was created.

Persistent Storage Manager is fully integrated with Microsoft Windows Scheduler, allowing complete unattended management of persistent image creation and rotation on a periodic basis.

Use Persistent Storage Manager to control system resource usage, optimization, and Persistent image management.

Persistent Storage Manager Global Settings Page

The Global Settings page allows you to modify overall settings for the Persistent Storage Manager. Some options will be disabled if there are already active persistent images. The Restore Defaults button will reset the system defaults.

Persistent Image Global Settings

Maximum persistent images:

Inactive period:

Inactive time-out:

Image directory:

Figure #42 Persistent Storage Manager Image Global Settings Page Screen

You can view or change the following global settings:

Maximum Persistent Images

Specifies the maximum number of active persistent images the server will support to a maximum of 250. If adding another persistent image would exceed this number, the system will delete the oldest existing persistent image.

Inactive Period

Specifies the amount of time a volume must be dormant before a persistent image is created. Prior to starting a persistent image, the system will wait for the volume to be imaged to become inactive. The default value will allow systems to start an image with a consistent file set and a minimal time-out. Administrators can change this value for system optimization. Reducing the inactive period will allow you to create persistent images even on busy systems, but with possible synchronization problems within applications which are concurrently writing to multiple files.

Inactive Time Out

Specifies how long the server should try to create a persistent image. A persistent image will not begin until a period of relative inactivity set by the Inactive period has passed. If an interval passes that is longer than the Inactive timeout period, the persistent image will not be created and a notice generated to the system event log.

Image Directory

Specifies the root directory used for the persistent image. Each persistent image appears as a subdirectory of the volume that is being imaged. The entire content of the volume as it existed at the moment the persistent image was created will appear under this directory.

Persistent Storage Manager Volume Settings Page

The Volume Settings page allows you to view the Persistent Storage Manager attributes for each volume and change the volume settings using the Tasks list.

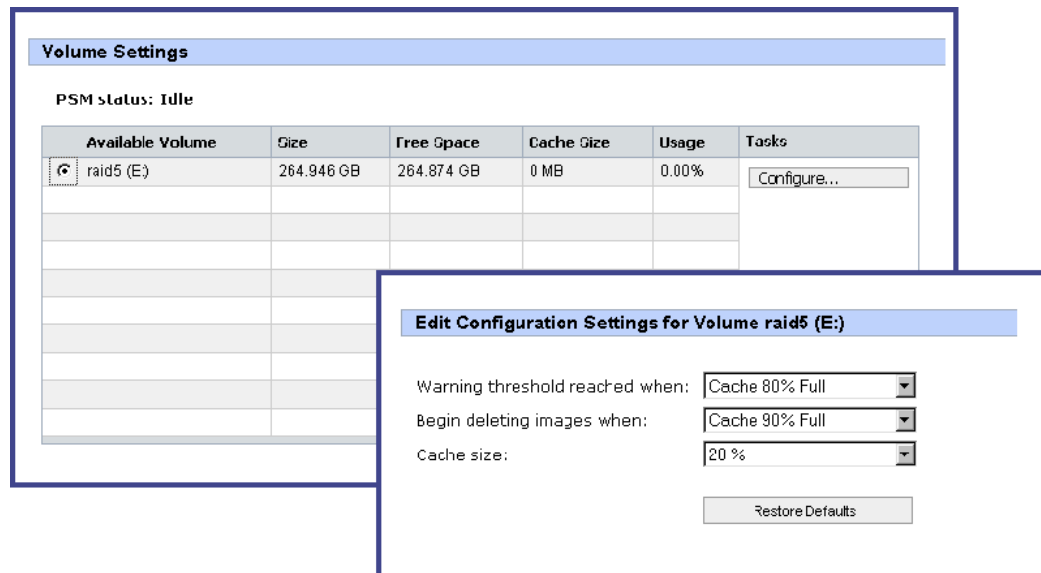


Figure #43 Persistent Storage Management Volume Configuration Screens

This page displays the following information:

- Available Volume - Lists each volume that can support persistent images. You can select the volume you want to configure.
- Size - Displays the size of the volume.
- Free Space - Displays the available storage size of the volume.
- Cache Size - Specifies the amount of space allocated to the cache file. Increasing this value will allow more and larger persistent images to be maintained.
- Usage - Displays the current cache file use as a percentage of the Cache Size.

Persistent Storage Management Configure Volume Settings Page

The Configure Volume Settings page, allows you to modify the various aspects of the Persistent Storage Manager volume attributes. Some of the fields will appear read-only if there are active persistent images. The Restore Defaults button will re-establish the system defaults.

You can view or change the following settings:

- Warning threshold reached when - Defines the percentage of cache space which, when consumed, will trigger warning messages to the system event log.

- Begin deleting images when – Defines the percentage of cache space which, when consumed, will trigger the automatic deletion of the oldest persistent image on the system. Automatic persistent image deletions are recorded in the system log.
- Cache size – Specifies the amount of space allocated to the cache file. Increasing this value will allow more and larger persistent images to be maintained. Make sure that adequate space is available on the drive where persistent images are stored.

Persistent Storage Management Schedules Page

The Schedules page displays a list of scheduled persistent images and associated tasks.

Each scheduled persistent image contains information such as its scheduled time, day, frequency, starting date, and group name.

The Schedules page allows you to create new schedules, delete existing schedules, and edit schedule properties.

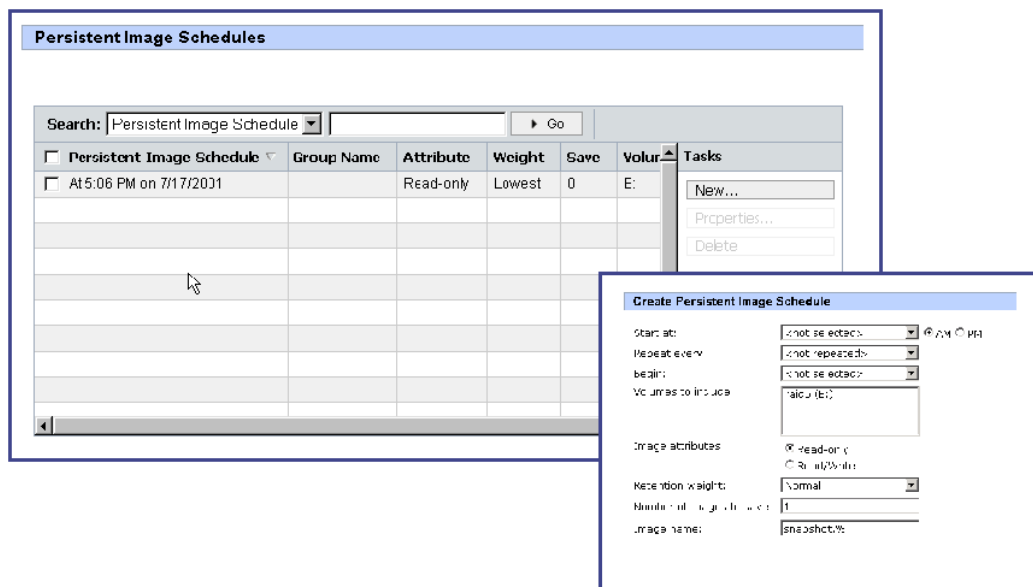


Figure #44 Persistent Storage Manager Image Schedule Screens

Create Schedule

To create a new schedule, you must supply a starting time, repeat period, starting day, volume, and the number of persistent images to make available to users.

Persistent Images Page

The Persistent Images page allows you to create, delete, edit properties and undo changes made to the persistent image.

Persistent Images

PSM status: Creating files

Search:

<input type="checkbox"/> Timestamp ▾	Image Name	Attribute	Weight	Volumes	Tasks
					New...
					Properties...
					Delete
					Undo

Figure #45 Persistent Storage Manager Images Page Screen

The page displays the following information:

- Time Stamp – Displays date and time the image was created.
- Image Name – Displays the name of the image.
- Attributes – Displays the read-only or read/write attribute of the image.
- Weight – Displays the relative retention weight of the image.
- Volumes – Displays the volume that was imaged.

Restore Persistent Images

The Persistent Images to Restore page displays a list of all persistent images. You can choose to view an image or restore your server appliance to an image you have previous created.

Persistent Images to Restore

Restore status: Idle

Search:

Persistent Image ▾	Date and Time	Age	Volumes	Tasks
				Details
				Restore

Figure #46 Persistent Storage Manager Restore Images Page Screen

Disk Defragmenter Page

The Disk Defragmenter allows access to the native Windows 2000 disk defragmenter through the Web UI. Select the disk you want to defragment and click **Defragment**.

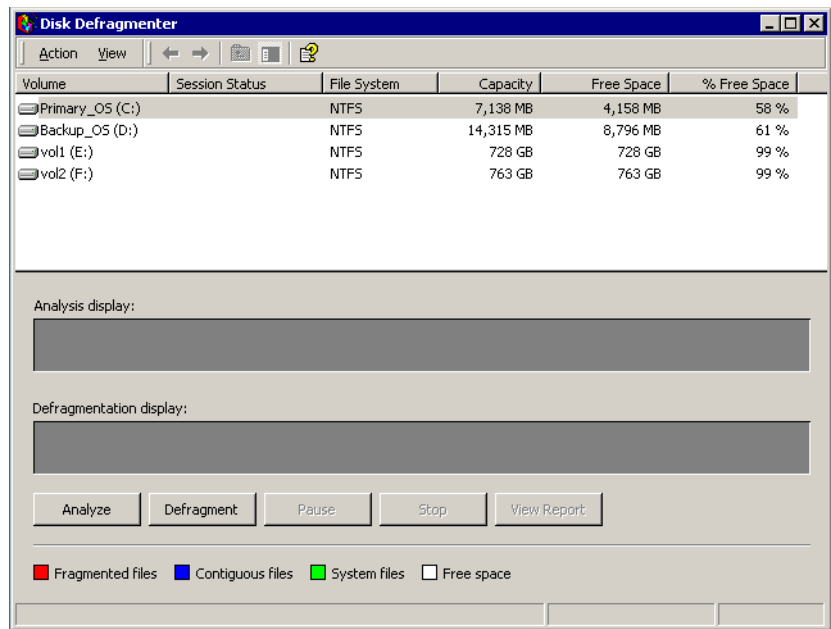


Figure #47 Disk Defragmenter

Users and Groups



NOTE

For detailed procedures within O/S Users and Groups Configuration, see **Chapter #9 - O/S 2.0 - Users and Groups** on page 222.

Users Page

From the Users page you can create, edit, and delete local users and groups. You can also change the members of each group. If the MaxAttach NAS 6000 is a member of a domain, you will not want to create any users on the MaxAttach NAS 6000 itself. The primary purpose of this page is to add one or more domain members to the local group.

You may also want to use domain user and group accounts to control access to resources on the MaxAttach NAS 6000. You may also want to use domain management tools to manage domain users and domain groups.

Users

Manage local users and groups on the server appliance.



Local Users

Create, edit, and delete local users on the server appliance.



Local Groups

Create, edit, and delete local groups on the server appliance.

Figure #48 Users Page Screen

Local Users Page

The Local Users on Server Appliance page displays an Object/Task Selector, which has the following parts:

- Name - This column lists the local user name. To delete, set password or configure the properties of a user, click the radio button next to the user name you want to modify.
- Full Name - This column lists the local user's full name.
- Account is disabled - This column indicates whether or not the local user account is

disabled.

Local Users on Server Appliance

Select a user, then choose a task. To create a new user, choose New...

Search: Name [] Go [] [] []

Name	Full Name	Account is disabled	Tasks
<input type="checkbox"/> Administrator		No	New...
<input type="checkbox"/> Guest		Yes	Delete
<input type="checkbox"/> IUSR_MAXATTACH4...	Internet Guest Account	No	Set a Password...
<input type="checkbox"/> IWAM_MAXATTACH4...	Launch IIS Process Account	No	Properties...
<input type="checkbox"/> sfuuser	sfuuser	No	
<input type="checkbox"/> Supervisor		No	
<input type="checkbox"/> TsInternetUser	TsInternetUser	No	

Figure #49 Local Users On Server Appliance Page Screen

A local user account is an account that exists on the server appliance itself and grants users access to its resources. The MaxAttach NAS 6000 can also be configured to grant access to domain users and groups. Domain users and groups are those that exist in a Microsoft Windows NT 4 or Microsoft Active Directory™ domain

Users are important in Microsoft Windows Powered security because you can assign permissions to limit the ability of users to perform certain actions. A permission is a rule associated with an object, usually a file, folder, or share, that regulates which users, and in what manner those users can access the object.

Please remember the following when creating local users on the MaxAttach NAS 6000:

- A user name cannot be identical to any other user or group name on the computer being administered.
- A user name can contain up to 20 uppercase or lowercase characters except for the following: “ / \ [] : ; | = , + ? < > .
- A user name cannot consist solely of periods (.) or spaces.

Passwords

You can type a password containing up to 127 characters. However, if you are using Microsoft® Windows® 2000 on a network that also has computers using Microsoft Windows 95 or Microsoft Windows 98, consider using passwords that contain fewer than 14 characters. Windows 95 and Windows 98 support passwords that contain up to 14 characters. If your password is longer, you may not be able to log on to your network from those computers.

Enabling the Guest Account

By default, the guest account is disabled. For workgroups that have Windows 95 and Windows 98 client computers, enabling the guest account is the quickest way to provide access to resources on a server appliance. By enabling the guest account, however, any user connected to the network will have access to resources on the appliance. An alternative is to create a user account for every user on the network

Local Groups Page

The Local Groups on Server Appliance page displays an Object/Task Selector, which has the following parts:

- Name - This column lists the local group name. To delete or configure the properties of a group, click the radio button next to the group name you want to modify.
- Description - This column lists the description of the group.

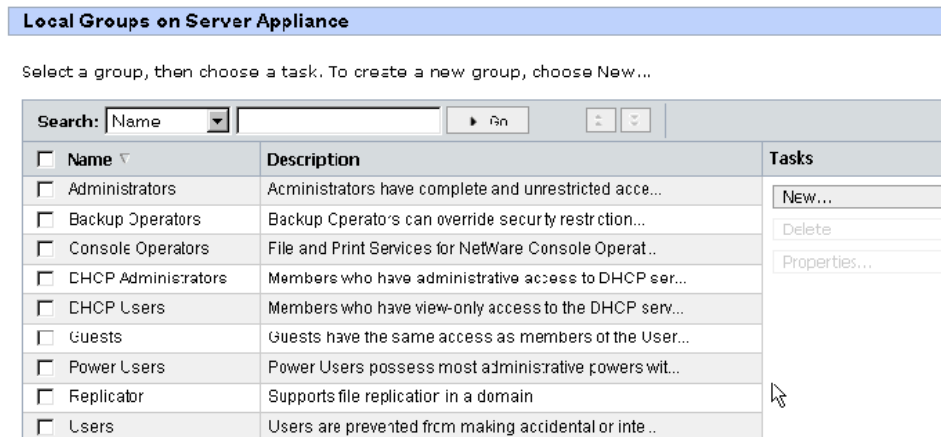


Figure #50 Local Groups on Server Appliance Page Screen

A local group account is an account that exists on the MaxAttach NAS 6000 itself and grants groups access to its resources. The MaxAttach NAS 6000 can also be configured to grant access to domain groups. Domain groups are those that exist in a Microsoft Windows NT® 4 or Microsoft Active Directory™ domain. You can add local users, domain users, and domain groups to local groups.

Groups are important in Microsoft Windows Powered security because you can limit the ability of groups to perform certain actions by assigning them permissions. Any local or domain user who is a member of the local administrator group on the MaxAttach NAS 6000 has administrative privileges for the MaxAttach NAS 6000. Likewise, any member of a group that has been assigned to the administrator group on the local computer has administrative privileges for that computer. For example, you could assign the TeamLeads

group, consisting of Tom, Mary, Hazel, and Jim to the administrative group on the MaxAttach NAS 6000. Each of these TeamLeads group members would then have administrative privileges on the MaxAttach NAS 6000.

Local Groups Members Page

The Members page allows you to add local or domain users to the local group.

The screenshot shows the 'Users Group Properties' dialog box with the 'Members' tab selected. On the left, under 'Members', there is a list containing 'INTERACTIVE', 'Authenticated Users', 'sfuuser', and 'MNS3\Domain Users'. To the right of this list are 'Add' and 'Remove' buttons. Further right is a list titled 'Add user or group:' containing 'Everyone', 'CREATOR OWNER', 'CREATOR GROUP', 'DIALUP', 'NETWORK', 'BATCH', and 'INTERACTIVE'. Below these lists, there are instructions: 'To add a user or group, select from the list above, then choose Add.' and 'To add a domain user or group to this group, enter a name in the format domain\user, then choose Add:'. There is a text input field for this format and an 'Add' button. At the bottom, there are fields for 'Username:' and 'Password:' with a note: 'If you are logged on with an account that does not have access to this domain, enter the domain\user of an account which does have access:'.

Figure #51 User Group Properties Page Screen - Members Tab



NOTE

ADDING TO LOCAL USER GROUP: Local users created through the Web UI are not automatically added to the Local Users group. You will need to add these users manually.



NOTE

ADDING DOMAIN GROUPS: You cannot add domain groups to local groups via the Web UI. You can add them through Terminal Services.

Folders and Shares



NOTE

For detailed procedures within O/S Folders and Shares Configuration, see **Chapter #8 - O/S 2.0 - Folders and Shares** on page 184.

Shares Page

From the Shares page, you can:

- Create folders, manage attributes and set permissions.
- Create, delete and edit the properties of each share exported by the MaxAttach NAS 6000.
- Enable, disable and configure the file sharing protocols.

Shares

Manage local folders, and create or modify file shares.



Folders

Create folders, manage attributes, and set permissions.



Shares

Create, delete, and edit the properties of each share exported by the server appliance.



Sharing Protocols

Enable, disable, and configure file sharing protocols.

Figure #52 Shares Page Screen

Volumes Page

The Volumes page allows you to open, or share, a number of network volumes.

Volumes

Select a volume, and then choose a task. To view folders in a volume, choose Open. To create a share, choose Share...

Search: Go	Volume Name ▾	Total Size	Free Space	Share Type	Tasks
<input checked="" type="checkbox"/>	raid5 (E:)	264 GB	264 GB		<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">Open</div> <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">Share...</div> <div style="border: 1px solid #ccc; padding: 2px;">Manage Shares...</div>

Figure #53 Folders Volumes Page Screen

The page displays an Object/Task Selector that has the following columns:

- Volume Name
 - Lists each volume by name.
 - To create, open, delete, or configure the properties of a given volume, select the check box next to the name of the volume you want to modify.
- Total Size-Shows the total size of the volume.
- Free Space-Shows the amount of free space available on the volume.
- Share Type-Indicates the type of sharing in effect for the folder:
 - - W = Windows (CIFS) Sharing
 - - U = UNIX (NFS) Sharing
 - - F = FTP Sharing
 - - H = HTTP Sharing
 - - A = AppleTalk Sharing
 - - N = NetWare Sharing

Folders Page

The Folders page allows you to create, open, delete, or configure folders.

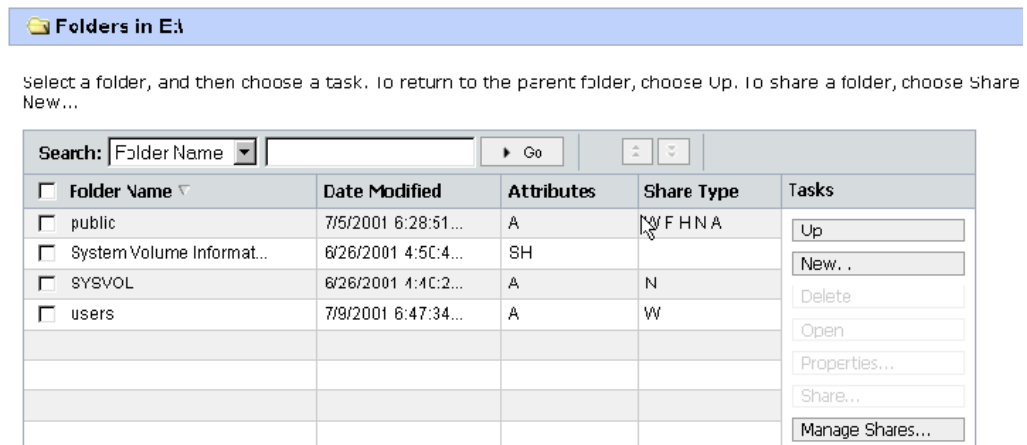


Figure #54 Shared Folders Page Screen

The Object/Task Selector displays the following columns:

- Name - This column lists each folder by name. To create, open, delete, or configure the properties of a given folder, click the radio button next to the name of the folder you want to modify.
- Modified - This column shows the date the folder was last modified.
- Attributes - This column shows the folder attributes:
 - - R = Read only

- - A = Ready for archiving
- - H = Hidden
- - C = Compressed
- - S = System folder

When the page is initially displayed, the Object/Task Selector contains a list of root folders for each volume. Use the Object/Task Selector to select a folder, then click on the task to perform from the Tasks list to perform the appropriate task.

Navigating Among Folders

The Object/Task Selector lists up to the first 100 folders found. To navigate among the list of folders using the Object/Task Selector, you can search by the fields available in the Search list, and then enter the search criteria in the box to the left of the Go button, or you can scroll through the list. In addition, if there are more than 100 folders, you can view folders in batches of 100 using the Page Up and Page Down buttons to the right of the Go button.

Shared Folders Page

The Shared Folders allows you to create, delete or configure shares on the MaxAttach NAS 6000.

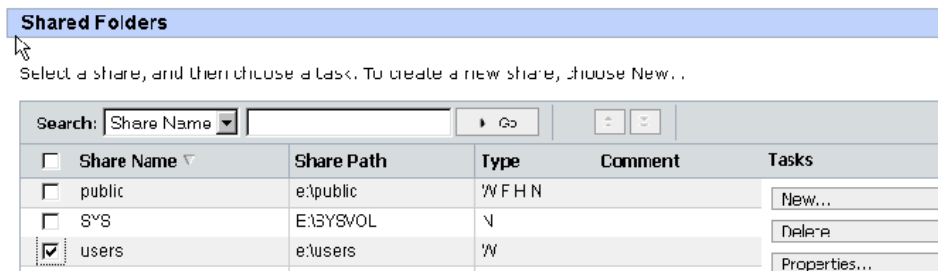


Figure #55 Shared Folders Page Screen

The Object/Task Selector displays the following columns:

- Shared Folder - This column lists each shared folder by name. To create, open, delete, or configure the properties of a given share, click the radio button next to the name of the share you want to modify.
- Shared Path - This column displays the share path.
- Type - This column indicates the share type:
 - - W = Windows (CIFS)
 - - U = UNIX (NFS)
 - - F = FTP

- - H = HTTP
- - A = AppleTalk
- - N = Netware
- Description - This column displays a brief description of the share, if one has been provided.

Use the Object/Task Selector to select a share, then click the task you want to perform from the Tasks list.

Shared Properties - General Tab

To create a share, you must supply a share name that is unique across all shares and the share path. Some protocols also support the inclusion of a comment or brief description of the share. The Microsoft Windows (CIFS) is automatically enabled.

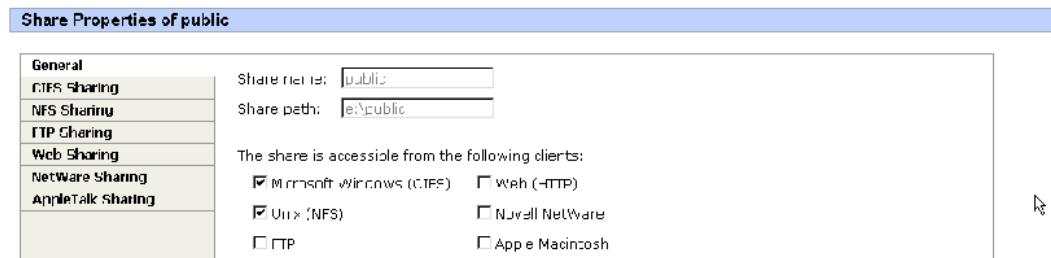


Figure #56 Share Properties Page Screen - General Tab

While a single user interface is provided to create a share for all protocols, in actuality, a separate share is created for each protocol. You can remove individual sharing protocols from a share, without removing the share itself. However, removing all sharing protocols from a share will delete all versions of the share.

Shared Properties - CIFS Sharing Tab

The CIFS Sharing page is used to change the number of users who have access to a share, change the caching options relative to the share, and set or change user permissions.

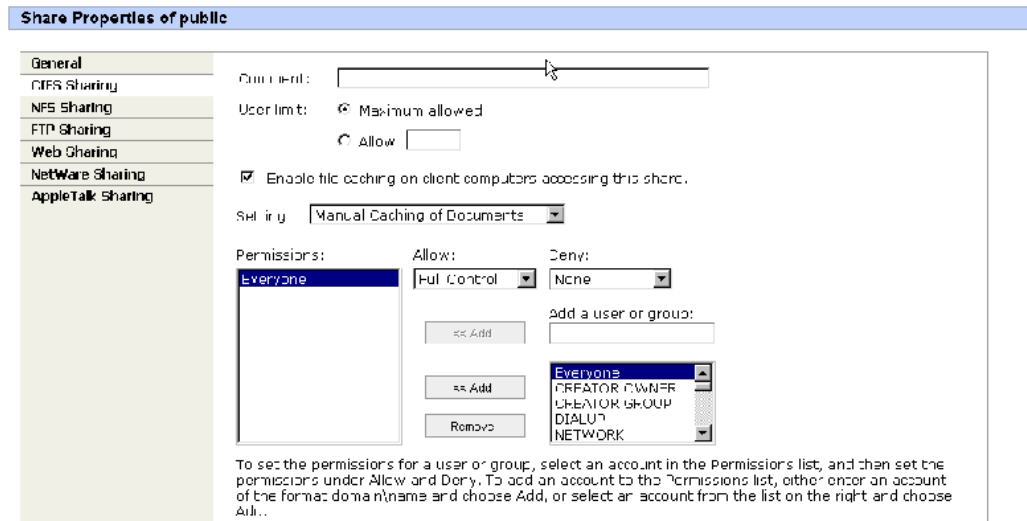


Figure #57 Share Properties Page Screen - CIFS Tab

The types of permissions that can be set on CIFS shares are:

- Read. Read permission allows you to:
 - - View file and subfolder names.
 - - Traverse to subfolders.
 - - View data in files.
 - - Run program files.
- Change/Read. The Change/Read permission allows all of Read permissions, plus:
 - - Adding files and subfolders.
 - - Changing data in files.
 - - Deleting subfolders and files
- Full Control. Full Control is the default permission applied to any new shares you create. It allows all Change/Read permissions plus:
 - - Changing permissions (NTFS files and folders only).
 - - Taking ownership (NTFS files and folders only).
- Change and None. The Change and None permission allow you to view the share. When you try to access the share, you will receive an “access denied” error message. It is recommended that you don’t use the Change option.

Shared Properties Page - NFS Sharing Tab

The NFS Sharing page is used to specify which NFS clients are granted access to each share. Access can be granted or denied on the basis of client host name. Access can also be granted or denied on the basis of client groups, where a client group contains one or more client host names.

Share Properties of public

General
CIFS Sharing
NFS Sharing
FTP Sharing
Web Sharing
NetWare Sharing
AppleTalk Sharing

Share path: e:\public

Select a client or a client group: [Empty box]

Enter the NFS client computer name or IP address, then choose Add: [Empty box]

ALL MACHINES Read-Write

Add Remove

Type of access: Read-Write

☐ Use EUC-JP encoding for this share

Figure #58 Share Properties Page Screen - NFS Tab

Shared Properties Page - FTP Sharing Tab

The FTP Sharing page is used to specify the share access permission granted to FTP clients.

Share Properties of public

General
CIFS Sharing
NFS Sharing
FTP Sharing
Web Sharing
NetWare Sharing
AppleTalk Sharing

Allow the following access permissions:

☒ Read

☐ Write

Log visits ☒

Figure #59 Share Properties Page Screen - FTP Tab

Shared Properties Page - Web Sharing Tab

The Web Sharing page is used to specify the share access permission granted to HTTP clients.

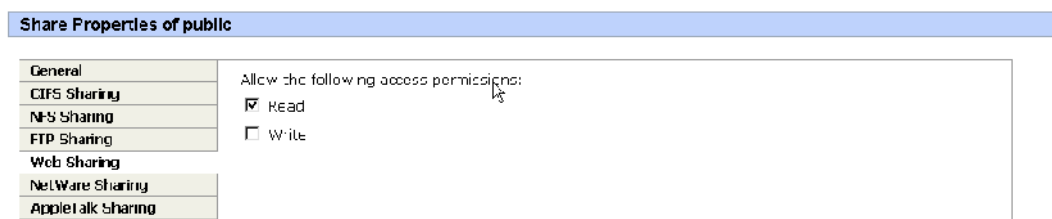


Figure #60 Share Properties Page Screen - Web Sharing Tab

Shared Properties Page - NetWare Sharing Tab

NetWare Sharing is set via Terminal Services.

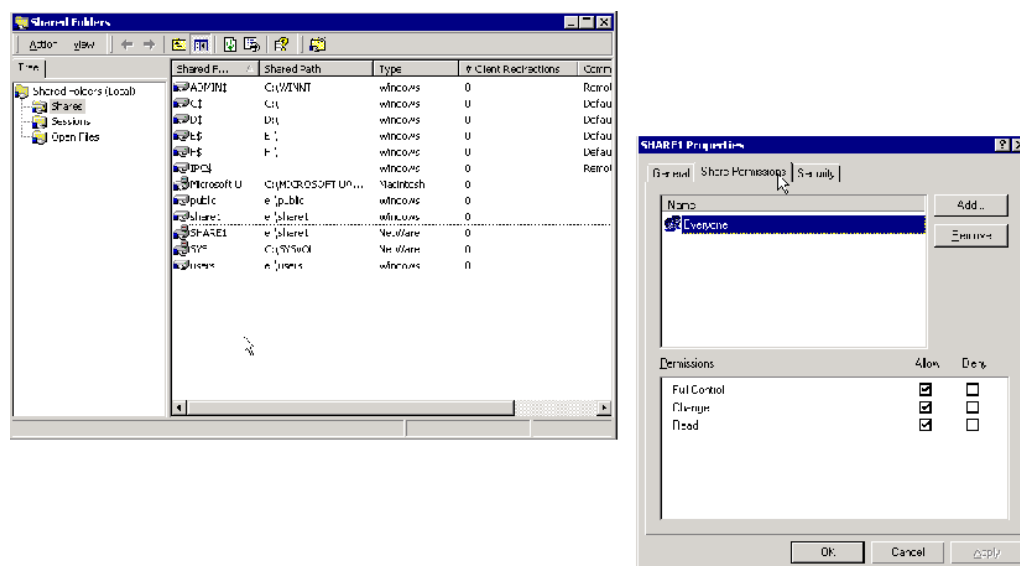


Figure #61 NetWare Share Properties Via Terminal Services

The types of permissions that can be set on NetWare shares are:

- **Read.** Read permission allows you to:
 - - View file and subfolder names.
 - - Traverse to subfolders.
 - - View data in files.
 - - Run program files.
- **Change.** The Change permission allows all of Read permissions, plus:

- - Adding files and subfolders.
- - Changing data in files.
- - Deleting subfolders and files
- Full Control. Full Control is the default permission applied to any new shares you create. It allows all Change/Read permissions plus:
 - - Changing permissions (NTFS files and folders only).
 - - Taking ownership (NTFS files and folders only).

Shared Properties Page - AppleTalk Sharing Tab

AppleTalk Sharing is set via Terminal Services..

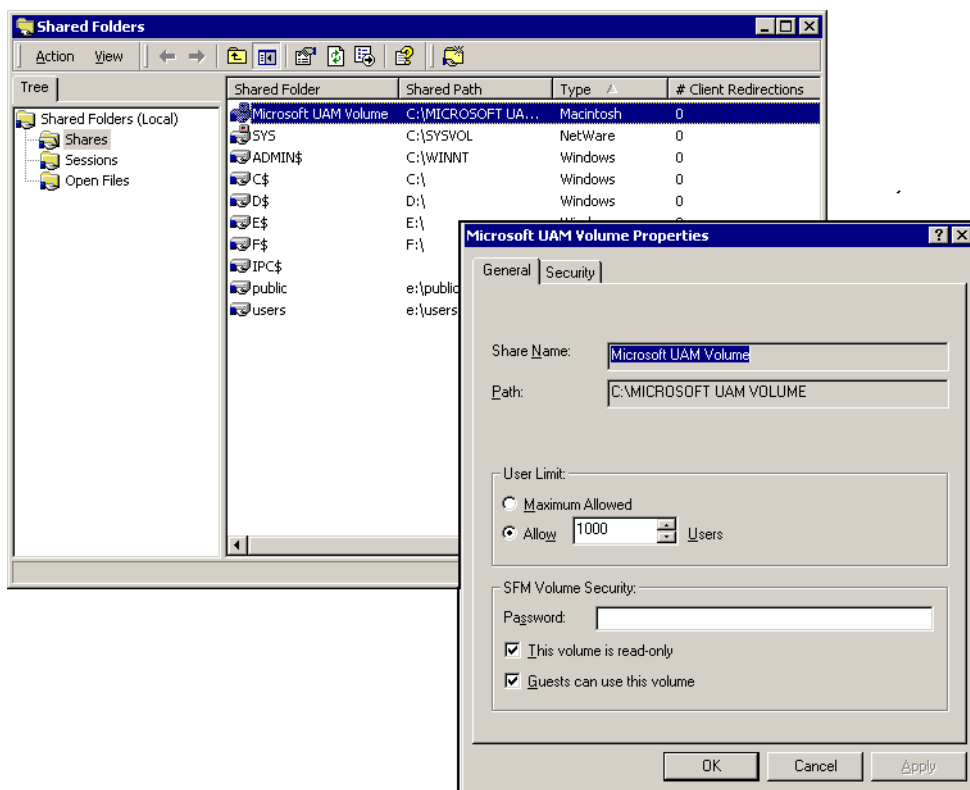


Figure #62 AppleTalk Share Properties Via Terminal Services

On the General tab of the share's properties page, you can:

- Set the maximum number of users allowed to simultaneously access the share
- Set the volume password
- Select read/write or read-only status
- Choose whether guest users can use the volume. (If you enable the **Guests can use this volume** checkbox, you may also need to enable the Guest user account. If the

Guest user account is disabled, there will be no Guest to access your share.)

On the Security tab, you can:

- Add or remove users and groups who have permission to access the share
- Assign permission rules for selected users and groups
- Access advanced security options including permission inheritance rules

Sharing Protocols Page

The Sharing Protocols page allows you to enable, disable, stop, or configure relevant network protocols.







File Sharing Protocols				
Select a protocol in the table and then choose a task.				
Name	Status	Startup Type	Description	Tasks
 AppleTalk Protocol	Running	Automatic	Allows access to data shares from Apple Macintosh clients	Enable Disable Properties...
 CIFS Protocol	Running	Automatic	Allows access to data shares from Windows Common Internet File System clients	
 FTP Protocol	Running	Automatic	Allows access to data shares from FTP clients	
 HTTP Protocol	Running	Manual	Allows access to data shares from Web browsers.	
 NetWare Protocol	Running	Automatic	Allows access to data shares from NetWare clients	
 NFS Protocol	Running	Automatic	Allows access to data shares from Unix network file system clients	

Figure #63 File Sharing Protocols Page Screen

The Sharing Protocol page displays the Object/Task Selector with the following columns:

- Name—Lists each protocol by name. To enable, disable, or change the properties of a given protocol, select the button next to the protocol you want to modify.
- Status—Indicates that the protocol is Running, Stopped, or Paused.
- Startup Type—Indicates whether the protocol should start automatically when the server appliance boots, be invoked manually, or be disabled.
- Description—Displays a brief description of the protocol. The Tasks list is located next to the Object/Task Selector. Use the Name column of the Object/Task Selector to select a protocol. To perform a task, choose the appropriate task from the Tasks list.

AppleTalk Service Properties Page

Microsoft Windows 2000 Server AppleTalk network integration allows you to share files and printers among the MaxAttach NAS 6000 and any Apple Macintosh clients that are connected to your network.

With AppleTalk network integration, Macintosh computers need only the Macintosh OS software to function as clients; no additional software is required.

AppleTalk network integration simplifies administration by maintaining just one set of user accounts instead of separate user accounts, for example, one on the Macintosh server and another on the computer running Windows 2000 Server.

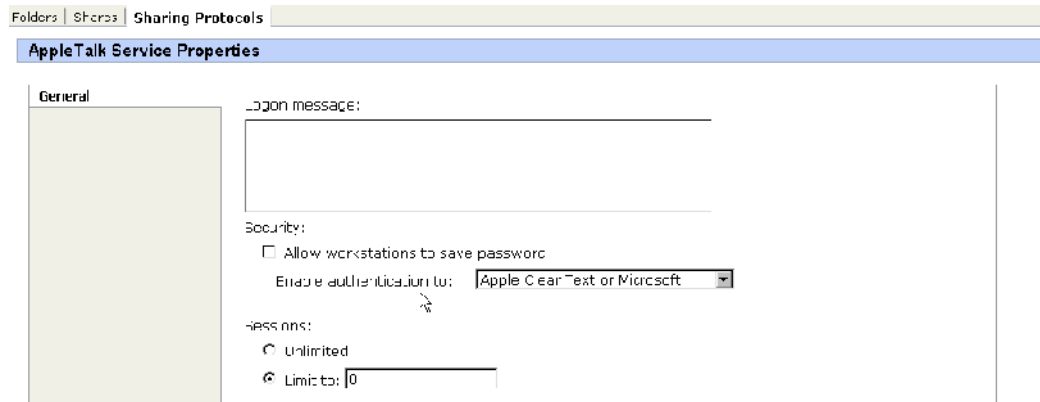


Figure #64 AppleTalk Service Properties Page Screen

FTP Service Properties Page

The File Transfer Protocol (FTP) is integrated with the Windows security model. Users connecting using FTP are authenticated based on the user accounts on the Windows Powered server appliance. They receive access based on those user profiles. Keep in mind, however, that the FTP server relies on the ability to send user passwords over the network without data encryption. As a result, a user with physical access to the network could examine user passwords during the FTP validation process.

FTP supports all Microsoft Windows FTP client commands, when a server appliance is running FTP, other computers using the FTP utility can connect to the server and transfer files. On the other hand, non-Microsoft versions of FTP clients might contain commands that are not supported by the FTP server protocol.



Figure #65 FTP Service Properties Page Screen

Enabling FTP Logging

You can log incoming FTP connections to the FTP log by enabling FTP Logging. By default, FTP logs are stored by in %windir%\system32\logfiles\msftpsvc1.

Administrators can access these files from their workstation by either accessing an administrative share—for example, \\appliance\admin\$\winnt\system32 or by creating a new share for this folder.

FTP Anonymous Access

Allowing anonymous access to the FTP server enables users to connect with the user name anonymous-or ftp, which is a synonym for anonymous. A password is not necessary, but the user is prompted to supply an e-mail address as the password. By default, anonymous connections are allowed.



NOTE

ACCESSING THE FTP SERVER: You cannot access the FTP server from a Microsoft Windows Powered user account with the name anonymous. The anonymous user name is reserved in the FTP server for the anonymous logon function. Users logging on to the server with the user name anonymous receive permissions based on the FTP server configuration for anonymous logons.

After the FTP protocol software is installed on your computer, you must configure the software to operate. Your FTP server protocol settings will result in one of the following configurations:

- No anonymous FTP connection to the server allowed. In this case, each user must provide a valid Windows user name and password. To configure the FTP server protocol for this setting, clear the Enable anonymous connection check box on the FTP Protocol Properties page.
- Allow both anonymous and Windows users to connect to the FTP server. This configuration allows a user to use either an anonymous connection or a Windows user name and password. To configure the FTP server protocol for this setting, select only the Enable anonymous connection check box in the FTP Protocol Properties page.
- Allow only anonymous FTP connections to the server. In this case, a user cannot connect to the FTP server using a Windows user name and password. To configure the FTP server protocol for this setting, select both the Enable anonymous connections and the Allow only anonymous access check boxes in the FTP Protocol Properties page.

If anonymous connections are allowed, you must supply the Windows user name and password that will provide anonymous access to the FTP server. When an anonymous FTP transfer occurs, Windows verifies the user name assigned in this dialog box to determine whether access is allowed to the files.

Adding Custom FTP Messages

You can create customized welcome and exit messages that are sent to users when they connect or disconnect from the server appliance.

HTTP - Hypertext Transfer Protocol Service Properties Page

The HTTP is the Internet protocol used by World Wide Web browsers and servers to exchange information. The protocol defines what actions Web servers and browsers should take in response to various commands, thus making it possible for a user to use a client program to enter a URL, or choose a hyperlink, and retrieve text, graphics, sound, and other digital information from a Web server. All URLs of files on Web servers begin with http://.

The screenshot shows the 'HTTP Service Properties' dialog box with the 'General' tab selected. The dialog has a title bar and a main content area. On the left, there is a large, empty light blue rectangular area. To the right of this area, there is text that reads: 'Select the IP address(es) and port that can be used to access the data shares on this server appliance.' Below this text are two radio buttons: 'All IP addresses' (which is selected) and 'This IP address only'. To the right of the 'This IP address only' radio button is a text box containing the IP address '134.6.38.95'. Below the IP address text box is a 'Port:' label followed by a text box containing the number '80'. At the bottom of the dialog, there is a small text box containing the warning: 'Changing these settings may affect users currently accessing data shares on this server appliance.'

Figure #66 HTTP Service Properties Page Screen

Web HTTP Protocol

The hypertext transfer protocol (HTTP) is a communications protocol designed to transfer hypertext documents between computers over the Web. HTTP defines what actions Web servers and browsers should take in response to various commands.

World Wide Web Server

The commands used by the Web are defined in HTTP.

To specify the location of a resource, HTTP uses Uniform Resource Locators (URLs). URLs follow a naming convention that uniquely identifies the location of a computer, directory, or file on the Internet. The URL also specifies the Internet protocol-FTP, HTTP, for example- needed to retrieve the resource. If you know the URL of a resource, you can provide the URL, or you can link to it from a document you want to make available to Web users.

The HTTP protocol supports anonymous access, as well as basic and Windows authentication.

NetWare Protocol Service Properties Page

The MaxAttach NAS 6000 Implements File and Print Services for NetWare (FPNW). FPNW emulates a NetWare 3.12 server, enabling the MaxAttach NAS 6000 to seamlessly integrate into an existing NetWare-based network requiring no changes to the NetWare clients. The NetWare clients do not know they are accessing the MaxAttach NAS 6000.

NFS Protocol Properties Page

With the NFS protocol, the MaxAttach NAS 6000 can act as a Network File System (NFS) server. Users can then share files in a mixed environment of computers, operating systems, and networks.

Users on computers running NFS client software can access shares on the server appliance by connecting, or mounting, those shares to their computers.

UNIX computers follow advisory locking for all lock requests. This means that the OS does not enforce lock semantics on a file, and applications that check for the existence of locks can use these locks effectively. However, the NFS Protocol implements mandatory

locks even for those locking requests that are received through NFS. This ensures that locks acquired through NFS are visible through the Server Message Block (SMB) protocol and to applications accessing the files locally. The O/S enforces mandatory locks.

NFS Service

Allows access to data shares from UNIX-based NFS clients.



Client Groups

Manage NFS Client Groups.



Locks

Manage NFS Service locks.



User and Group Mappings

Manage User Name Mapping that associates Windows and UNIX user names.

Figure #67 NFS Service Page Screen

Maintenance Page



NOTE

For detailed procedures within O/S Maintenance Operations, see **Chapter #10 - O/S 2.0 - Maintenance** on page 232.

From the Maintenance page, users can perform the following general MaxAttach NAS 6000 maintenance tasks:

- Update software
- Change date and time
- Shutdown the system
- Examine, store, and print system logs
- Backup the system
- Use Terminal Services to access the server console and desktop
- Set and configure alert email
- Set the language used by the Maxtor MaxAttach NAS 6000
- Add and remove programs
- Manage local or remote computers with a single desktop tool
- Specify how the MaxAttach NAS 6000 is to respond to a boot failure
- Set the maintenance session time out period
- Re-image the system drive

- Re-image the system drive after a failure.

Maintenance

Provides essential configuration and maintenance tools. Also accesses the Terminal Services Advanced Client, which provides full control over the server appliance. Tasks that cannot be performed with this tool can be performed with the Terminal Services Advanced Client.



Software Update
Apply a software update.



Date/Time
Set the date and time on the server appliance.



Shutdown
Shut down or restart the server appliance immediately or at a scheduled time.



Logs
View, clear, download, and configure logs.



Backup
Back up or restore the server appliance operating system.



Terminal Services
Use the Microsoft Windows 2000 Terminal Services Advanced Client to manage the server appliance.



Alert E-Mail
Set alert e-mail on the server appliance.



Language
Change the language used by the server appliance.



Add/Remove Programs
To Add/Remove Programs



Computer Management
Use to manage local or remote computers using a single, consolidated desktop tool.



System Recovery Option
Specify how the system to respond to a boot failure.



Session Timeout
Set the Session Timeout period



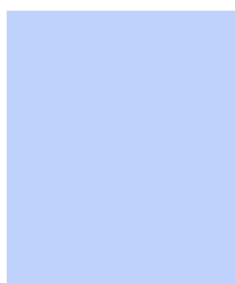
Re-image System Drive
Write a new image to restore the system (boot) drive.

Figure #68 Maintenance Page Screen

Software Update Page

The Software Update page is used to apply software updates to the MaxAttach NAS 6000. You should only apply software upgrades that have been approved by Maxtor.

Software Update Wizard



Welcome to the Software Update Wizard

This wizard helps you modify software on the server appliance.

To continue, click Next.

Figure #69 Software Update Wizard Page Screen

Date and Time

The Date and Time page is used to set the date, time, and time zone for the MaxAttach NAS 6000.

Set Date and Time

Year: 2001
 Month: April
 Date: 27
 Time: 9 : 48 AM
 Time zone: ((GMT-08:00) Pacific Time (US & Canada); Tijuana)

☒ Automatically adjust clock for daylight saving time

Note:
 Windows(R) Powered server appliance date and time settings do not affect the date and time on your computer.

Figure #70 Data and Time Page Screen

Shutdown

The Shutdown page is used to shut down, restart, or to schedule a shutdown or restart of the MaxAttach NAS 6000. The restarting page checks periodically to determine whether the appliance is back online. If the restarting page detects that the MaxAttach NAS 6000 is online, it automatically returns to the default page.

Shutdown
 Shut it down or restart the server appliance immediately or at a scheduled time.

Restart
 Immediately shut down and then automatically restart the server appliance.

Shut Down
 Immediately shut down and power off the server appliance.

Scheduled Shutdown
 Schedule a shutdown or restart to occur later.

Figure #71 Shutdown Page Screen

Logs

A log file is a file that stores messages, or event logs generated by an application, service, or Microsoft Windows. These messages are used to track the operations performed in the server appliance.

You can use the Logs feature to view, clear, download, and configure the following types of event logs provided by the system:

- **Application Logs:** ■ The application log contains events logged by applications or programs. For example, a word-processing program might record a file error in the

application log. The events that are recorded are dependent upon the application.

- **FTP Logs:** ■The FTP log contains events logged by the FTP server.
- **NFS Logs:** ■The NFS log contains events logged by the NFS server.
- **System Log :** ■The system log contains events logged by the Microsoft Windows 2000 system components. For example, the failure of a driver or other system component to load during startup is recorded in the system log.
- **Security Log:** ■The security log can record security events such as valid and invalid logon attempts as well as events related to resource use such as creating, opening, or deleting files. An administrator can specify what events are recorded in the security log.
- **Web (HTTP) Shares Logs:** ■The Web (HTTP) shares log contains events logged by the Web server related to accessing HTTP shares.
- **Managing Web Administration Logs:** ■The Web administration log contains events logged by the Web server related to accessing the administration Web site.



Figure #72 Logs Screen Page

Backup Page

The Backup page is used to backup or restore MaxAttach NAS 6000 volumes or logical drives and is use primarily for backing up and restoring drives with user data rather than O/S images.

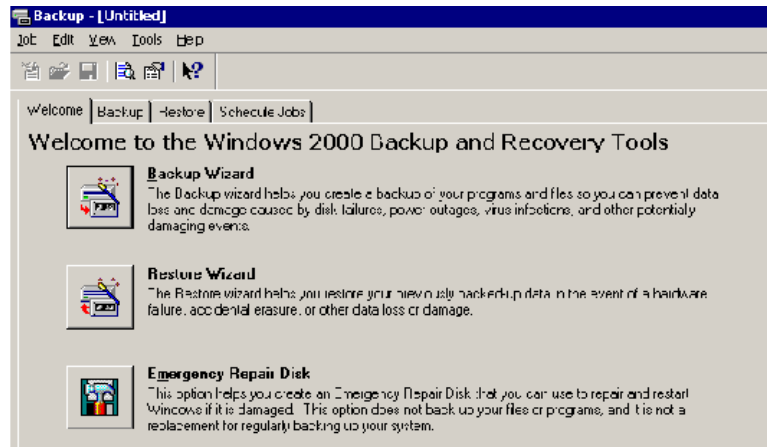


Figure #73 Backup Page Screen



NOTE

BACKUP SCHEDULE: You must specify a backup schedule. Do not select the On Demand backup as it will time-out and not perform its backup.

Related Topics

- For summary information on O/S backup and recovery, see any of the following sections below:
 - Add/Remove Programs
 - System Recovery Options
 - Re-Image System Drive
- For detailed information and procedures, see **Chapter #10 - O/S 2.0 - Maintenance** on page 232.

Terminal Services

The MaxAttach NAS 6000 comes with Terminal Services for Remote Administration (TSRA). It allows two concurrent connections and provides functionality similar to a terminal-based, centralized host, or mainframe, environment in which multiple terminals connect to a host computer. Each terminal provides a conduit for input and output

between a user and the host computer. A user can log on at a terminal, and then run applications on the host computer, accessing files, databases, network resources, and so on. Each terminal session is independent, with the host operating system managing conflicts between multiple users contending for shared resources. In summary, TSRA provides remote access for administering the MaxAttach NAS 6000 from virtually anywhere on your network, giving system administrators a method of remotely managing the MaxAttach NAS 6000 from any client.

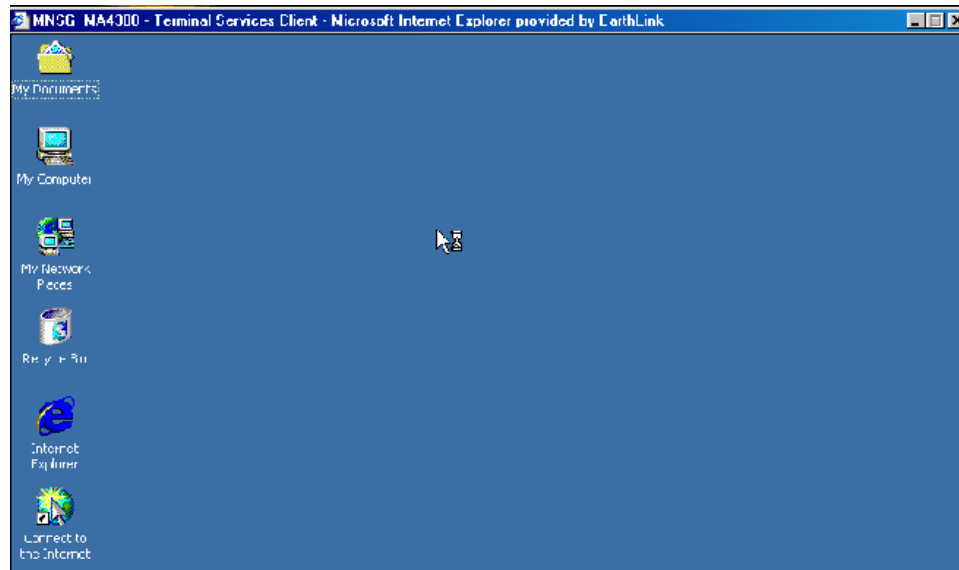


Figure #74 Terminal Services - MaxAttach NAS 6000 Desktop After Log In

Terminal Services Advanced Client (TSC) is the component running on the client machine; in the case of a MaxAttach NAS 6000, the TSC ActiveX component is automatically installed when the user selects this task.

The primary difference between TSC and the traditional mainframe environment is that the dumb terminals in a mainframe environment only provide character-based input and output. A TSC or emulator provides a complete graphical user interface, including a Microsoft Windows desktop and support for a variety of input devices (such as keyboard and mouse).

In the Terminal Services environment, an application runs entirely on the terminal server. The TSC performs no local processing of application software. The terminal server transmits the graphical user interface to the client, and the client transmits your input back to the server.

With TSC, you have full access to the MaxAttach NAS 6000 desktop and can manage it as if you are sitting in front of a monitor attached to the MaxAttach NAS 6000. All Microsoft Windows management tools can be used, and the Windows 2000 online Help can be accessed.

When a user opens TSC, she or he connects to the MaxAttach NAS 6000 and starts a session. When he or she is finished, he or she can either disconnect, and leave the session running (to enable connecting to this session again later) or log off, which will terminate the session and disconnect the client. Only two simultaneous sessions are allowed. Leaving a session running takes up one license and can affect other users. If two sessions are already running, new users will be denied access. Finally, TSC requires all connecting users to be authenticated, which is why users must log on each time they start a session.

**NOTE**

CLOSING TERMINAL SERVICES SESSION: Using the X in the upper right hand corner of the screen to close the TSC does not free up the TSC session. To correctly close a TSC, go to Start > Shutdown > Log off Administrator.

Alert Email

When an error condition occurs, the MaxAttach NAS 6000 can send an alert email message to a designated email address. You can enable or disable alert emails, and you can select which category of alert email you want the system to send.

Set Alert Email

Alert Email Settings:

☐ Disable sending alert email

☒ Enable sending alert email

☒ Send critical alert email

☒ Send warning alert email

☒ Send informational alert email

To: (Administrator's email address)

With: (SMTP server name or IP address)

Figure #75 Alert Email Configuration Page Screen

MaxAttach NAS 6000 Web UI Alerts

The MaxAttach NAS 6000 Web UI provides alert messages to warn you of conditions that may require your intervention. At the top of the interface, under the server name, is a Status line that tells you the alert level of the highest current level. There are three types of alerts and three alert levels:

- **Information:** Message regarding a condition that does not require any immediate intervention.
- **Warning:** Message regarding a condition that may require some administrator attention.
- **Critical:** Message requiring immediate administrator action to insure proper functionality of the MaxAttach NAS 6000 unit.

The MaxAttach NAS 6000 Web UI messages can also be sent as E-mail messages. You can specify which level(s) of messages should be sent, the E-mail address, and the SMTP server name, FQDN or IP address. Also, you need to make sure that the Exchange server you are using has the Internet Mail Connector running.

LED Alerts

The MaxAttach 6000 has front-panel LED indicators that provide a quick-look status of the major system components, including:

- Activity and condition of the hard disk drive modules
- Status of the unit's power supplies
- Over-all system status

For information about LED alerts, see the MaxAttach online Help.

Language Page

- The Language page is used to set the language of the Web UI. At this time, only English and Japanese are available. Future releases of the Windows Powered software will include French, German and Spanish.

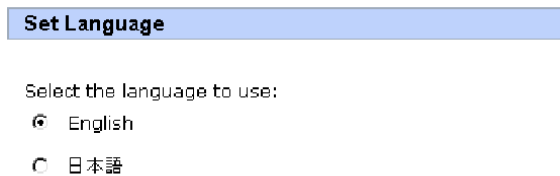
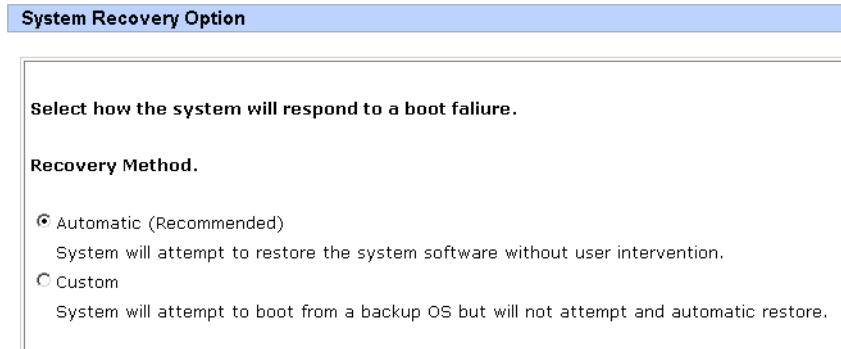


Figure #76 Set Language Page Screen

System Recovery Option Page

Boot failover recovery consists of writing a new copy of the O/S to the C:\ drive from a backup O/S copy located on drive D:\. You can set this to occur manually or automatically in the event of a corrupt O/S.



System Recovery Option

Select how the system will respond to a boot failure.

Recovery Method.

☒ Automatic (Recommended)
System will attempt to restore the system software without user intervention.

☐ Custom
System will attempt to boot from a backup OS but will not attempt and automatic restore.

Figure #77 System Recovery Option Screen

Session Timeout Options Page

This screen allows you to set the length of time in minutes before a web or Terminal Services management session times out. You are given the option of having a session never time out, which is especially useful during initial system set up and configuration.

**NOTE**

BEST PRACTICES RECOMMENDATION: After initial setup, keep the time out value low to prevent unauthorized administrator privileges access.

Session Timeout

Session Timeout Interval (Minutes)

Enter 0 to disable.

Enter 1 to 1440 Minutes.

Warning: Session timeout is a security feature. To prevent unauthorized access keep the value low.

Figure #78 Session Timeout Options Page

Re-Image System Drive Page

Allows you to re-image the system boot or C:\ drive with either the default factory configuration or with the most recently saved image along with its configuration settings including users, disks, volumes, and shares.



WARNING

LOSS OF ALL BOOT DRIVE DATA: This procedure will destroy all data on the boot C:\ drive.

Re-Image System Drive

Warning: Re-Imaging your system (boot) drive will completely overwrite all data.

Select an image to write to the system (boot) drive:

- ☒ Original factory-shipped image
- ☐ Most recently saved system image

Figure #79 Re-Image System Drive Screen and Options

Services for UNIX

Overview

The MaxAttach NAS 6000 implements Services for UNIX. This allows the MaxAttach NAS 6000 to act as an NFS server. When the MaxAttach NAS 6000 is configured as an NFS server, file access and administrative tasks are performed through the Web UI.

You can use the NFS Service to manage

- Client Groups
- Locks
- User and Group Mappings

NFS
Configure the properties of the NFS service.

➔

Client Groups
Manage NFS Client Groups.

➔

Locks
Manage NFS Service Locks.

➔

User and Group Mappings
Manage User Name Mapping that associates Windows and UNIX user names.

Figure #80 NFS Configuration Page Screen



NOTE

CREATING NFS SHARES: NFS shares are created from the Folders and Shares section of the Web UI.

NFS Client Groups

The NFS Client Groups page allows you to create, delete and edit client groups

NFS Client Groups

Select a NFS Client Group, then choose a task. To create a new Client Group, choose New...

NFS Client Groups ▾	Tasks
	New...

Figure #81 NFS Client Groups Configuration Page Screen

NFS Locks

NFS locks allows a process to have exclusive access to all or part of a file. File locking is implemented both on the MaxAttach NAS 6000 and the client. When a file is locked, the buffer cache is not used for that file, and each write request is immediately sent to the server.

After a system failure, when the MaxAttach NAS 6000 is restarted, the MaxAttach NAS 6000 attempts to restore the file lock status to the previous condition. If the client fails, the MaxAttach NAS 6000 releases the file lock. However, after the client restarts, it has a short period of time to reclaim the file lock.

NFS Locks

Current locks: Select a client to release its locks

Wait period, in seconds:

This specifies the length of time that the server will wait for a client to re-establish a lock following a restart of the appliance.

Figure #82 NFS Locks Configuration Page Screen

User & Group Mappings

In order to provide security for MaxAttach NAS 6000 files accessed from a UNIX environment, the NFS service requires the system administrator to map UNIX user or group accounts to their twin accounts on the MaxAttach NAS 6000. Users then have equivalent access rights under UNIX as they have under Microsoft Windows.

User and Group Mappings lets you create maps between Windows and UNIX user and group accounts even though the user and group names in both environments may not be identical.

In addition to one-to-one mapping between Windows and UNIX user and group accounts, User and Group Mappings permits one-to-many mapping. This lets you associate multiple Windows accounts with a single UNIX account or vice-versa.

To use the User and Group Mappings, you need to obtain UNIX user, password and group information from one or more NIS servers, or from imported password and group files from a single UNIX client (PCNFS).

Figure #83 User and Group Mappings Page Screen - General Tab

The types of mappings that can be set up are:

- Simple Maps
- Explicit User Maps
- Explicit Group Maps

Simple Maps

Simple maps create automatic mappings between the MaxAttach NAS 6000 and UNIX users that both share the same user name. In a simple user map, users on the MaxAttach NAS 6000 are implicitly mapped one-to-one to UNIX users on the basis of user name.

Figure #84 User and Group Mappings Page Screen - Simple Mapping Tab

Explicit Maps

Explicit user and group maps allows you to create inter- and cross-platform maps among the MaxAttach NAS 6000 and UNIX user and group accounts, even when the user and group names in both environments are not identical. This lets you associate multiple UNIX accounts with a single MaxAttach NAS 6000 account or vice-versa.

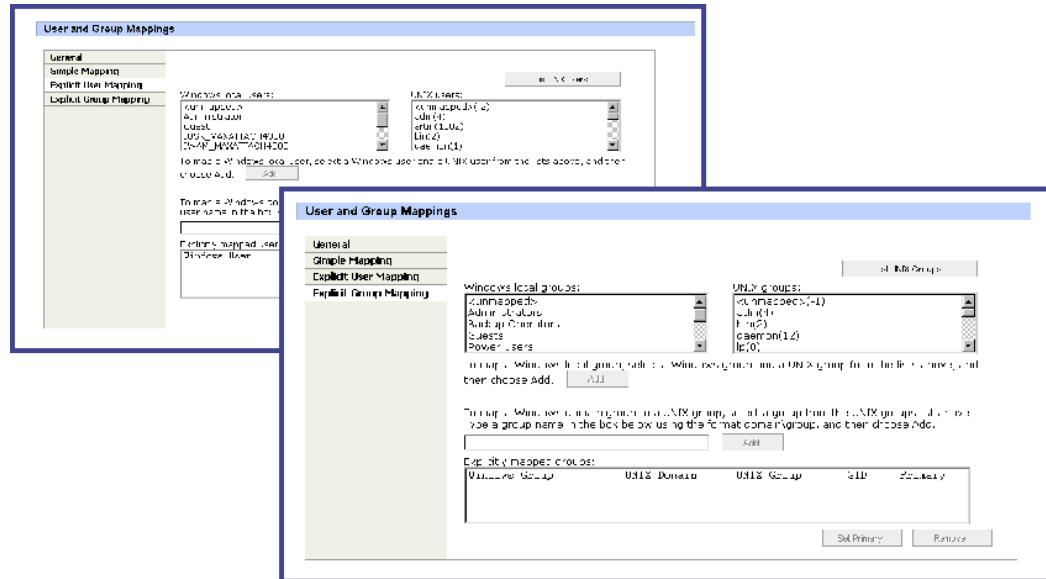


Figure #85 User and Group Mapping Page Screen - Explicit User & Explicit Group Tabs

Services for Netware

Overview

The MaxAttach NAS 6000 implements File and Print Services for NetWare (FPNW). FPNW emulates a NetWare 3.12 server, enabling the MaxAttach NAS 6000 to seamlessly integrate into an existing NetWare-based network requiring no changes to the NetWare clients. The Netware clients do not know they are accessing the MaxAttach NAS 6000.

NetWare Users

When you try to access shares on the MaxAttach NAS 6000, you will be prompted to enter a user name and password. The default user name is supervisor with a blank password. However, you can create users on the MaxAttach NAS 6000 and synchronize them with the NetWare users.

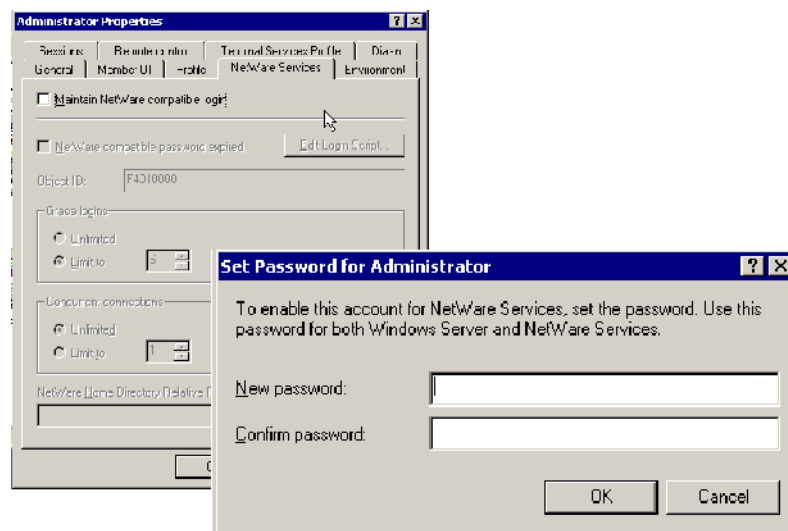


Figure #86 NetWare Users Configuration Screens

Help Pages

The O/S Web UI comes with a comprehensive help system available as a tab on the navigation bar. In addition, clicking the “?” link on the right side of the navigation bar will provide you with context-sensitive help for every screen. The starting page for the help system is shown below.



Figure #87 Help Page Screen

In addition to the online help system, you are also provided with a standalone version of the help files on your MaxNeighborhood Software and Documentation CD that came with your MaxAttach NAS 6000. The standalone version is designed to either run from the CD or be installed on a client workstation.

Chapter #4 - Overview - NAS 6000 Disk Array

Chapter Outline

- Standard configuration disk drive array
- Benefits
- Optional user-defined drive configurations
- Drive organization: logical, physical, SCSI, and raid
- Role of the Mylex Global Server and Client Array Manager
- Best practices, notes, warnings, and cautions



NOTE

If you need additional information on disk and RAID arrays, see **Chapter #11 - Appendix - Disk Array RAID Concepts** on page 254.

Standard Disk Array Configuration

A fully equipped Maxtor MaxAttach NAS 6000 consists of a Base Unit and two Expansion Unit equipment shelves. Each shelf is filled with 12 hard disk drives for a maximum system configuration of 36 hard disk drives. Depending on the type of drive used and the RAID configuration of the system, storage capacities starting at over 5 Terabytes (Tbytes) can be obtained.

Use the web user interface to find you system's exact capacity and current disk space utilization.

To see total system space and total space used

1. Log into the system.

2. At the Welcome page, click on the Status tab on the main navigation bar.
3. At the Status menu, click the System Status tab.
4. The system displays the following information:
 - Number of physical disks:
 - This is actually the number of Volumes or Logical Drives available in the system.
 - In default RAID configuration, it will be four drives for a Base Unit only; six drives for a Base and one Expansion Unit; eight drives for a Base and two Expansion Units.
 - Total hard disk drive space:
 - The amount of space in your system in GB (Gigabytes or Gbyte – 1,000 Gbytes = 1 Tbyte).
 - Total free hard drive space:
 - The amount of free space in your system in GB.

To see total system space for each volume or logical drive

1. Log into the system.
2. At the Welcome page, click on the Status tab on the main navigation bar.
3. At the Status menu, click the System Health tab.
4. Scroll down about a two pages to the status Drives section.
5. The system displays the following information in a table:
 - Device ID:
 - The volume or logical drive identification starting with C:\.
 - A fully factory-default configured system will have C:\, D:\, E:\, F:\ G:\, H:\, I:\ and J:\ drives.
 - Drive capacity:
 - The total drive capacity per drive in GB.
 - Free space:
 - The total drive free space in GB.
 - Used space:
 - Used space as a percentage of total space.

Disk Drive Array Organization

In order to fully understand the operation and capabilities of the MaxAttach disk drive array, the disks should be viewed in their logical, physical, SCSI, and RAID configurations, each of which provides additional insight into the system capabilities.

Throughout this section, the emphasis is on the “factory default configuration.” This refers to the “as-shipped” configuration the Base Units in all systems, and, if equipped, the recommended factory default configuration for Expansion Unit/s.

Logical Drive Organization

A fully equipped MaxAttach consisting of a Base Unit and two Expansion Units has the following logical drives available in its default configuration. The size of each volume or logical drive is dependent on the disk drives shipped with the system.

Table #1 - MaxAttach NAS 6000 Logical Drives

Logical Drive Name & Location	Function
Base Unit Logical Drives / Volumes	
Drive C:\ - Base Unit	Primary operating system (O/S) logical drive. Drive C:\ is not available for user data. Through a drive partition, its physical disks are shared with drives D:\ and E:\.
Drive D:\ - Base Unit	Mirror of O/S logical drive. Drive D:\ is not available for user data. Through a drive partition, its physical disks are shared with drives C:\ and E:\.
Drive E:\ - Base Unit	User data logical drive. Through a drive partition, its physical disks are shared with drives C:\ and E:\. The RAID configuration of this user logical cannot be changed.
Drive F:\ - Base Unit	User data drive. Can be reconfigured to other RAID or JBOD types.
First Expansion Unit	
Drive G:\ - First Expansion Unit	User data drive. Can be reconfigured to other RAID or JBOD types.
Drive H:\ - First Expansion Unit	User data drive. Can be reconfigured to other RAID or JBOD types.
Second Expansion Unit	
Drive I:\ - Second Expansion Unit	User data drive. Can be reconfigured to other RAID or JBOD types.
Drive J:\ - Second Expansion Unit	User data drive. Can be reconfigured to other RAID or JBOD types.

The exact system storage capacity depends on the number of expansion enclosures used, number of user data logical drives and drive arrays created, the RAID array used in each array, and if hot standby disks have been implemented.

SCSI Channel Structure

The figure below shows the relationship between the physical drives and the underlying SCSI bus communication system, along with the identification of each drive as to SCSI Channel, SCSI ID, and shelf mounting location.

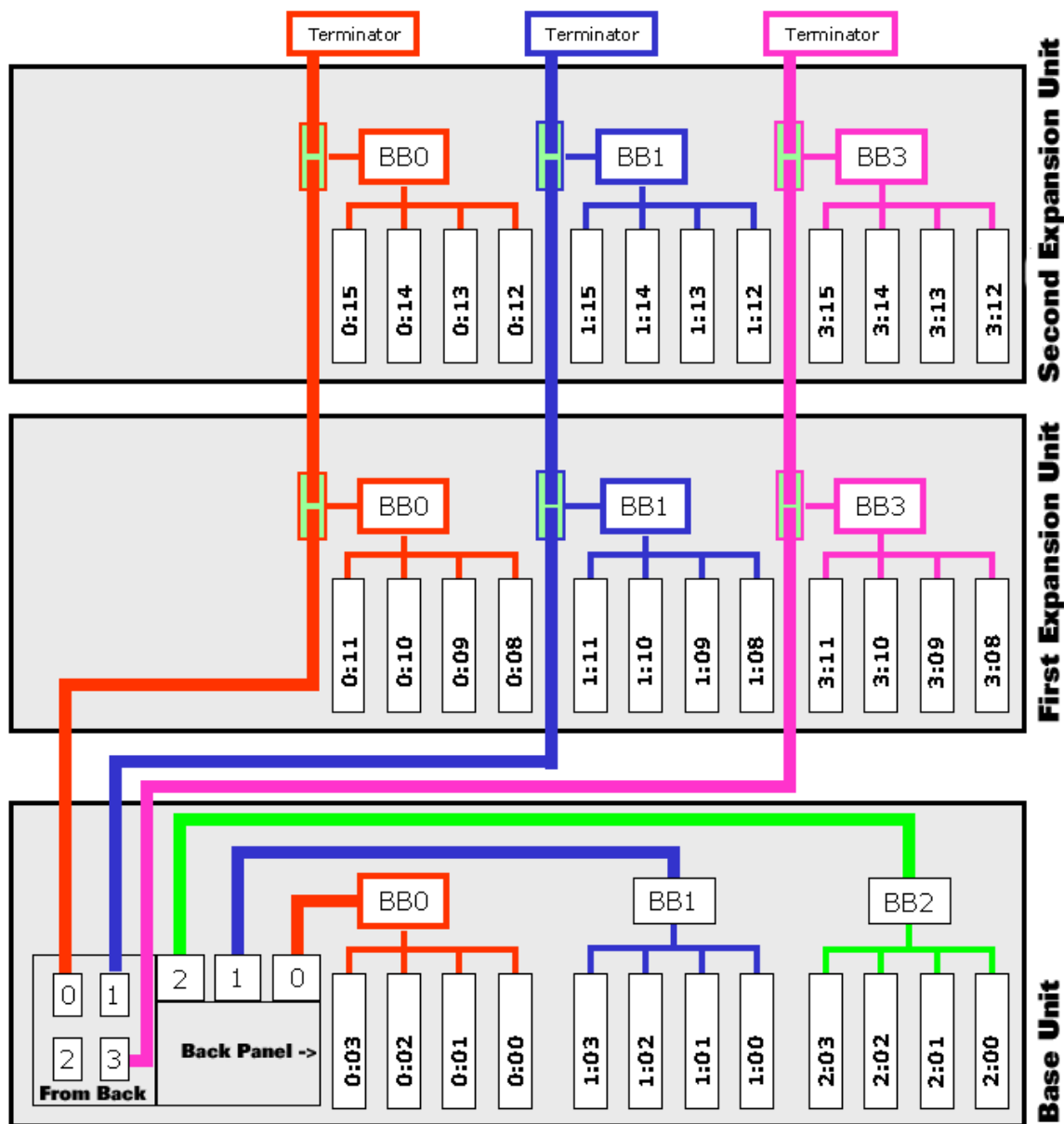


Figure #5 SCSI Bus Components and ID Number Assignments

Notes on SCSI Channels

1. SCSI Channel 2 is only used on the Base Unit.
2. SCSI cable runs to Base Unit drives are all internal within the chassis.
3. SCSI cable runs between the Base and the Expansion Units are all external cabling.
4. The last Expansion Unit also has one SCSI Terminator Plug for each Channel.

SCSI Bus and Target LUN IS Assignments

The SCSI drive assignments for the system disks are:

Table #2 - Disk Array Components by SCSI Bus & ID Number (Sheet 1 of 2)		
SCSI Bus:ID	Component Name	Component Location - Drive Number from Left
0-0	Hard disk drive	Base Unit, Drive 4
0-1	Hard disk drive	Base Unit, Drive 3
0-2	Hard disk drive	Base Unit, Drive 2
0-3	Hard disk drive	Base Unit, Drive 1
0-4	Channel-0 SCSI Bridge Board	All Units - ID shared by all Channel 0 Bridge Boards
0-5 & 0-6	Not Used	
0-7	SCSI Controller Card - Channel 0	Mylex SCSI RAID Controller is located in the Base Unit card cage. ID 0-7 controls all devices on Bus 0.
0-8	Hard Disk Drive	First Expansion Unit, Drive 4
0-9	Hard Disk Drive	First Expansion Unit, Drive 3
0-10	Hard Disk Drive	First Expansion Unit, Drive 2
0-11	Hard Disk Drive	First Expansion Unit, Drive 1
0-12	Hard Disk Drive	Second Expansion Unit, Drive 4
0-13	Hard Disk Drive	Second Expansion Unit, Drive 3
0-14	Hard Disk Drive	Second Expansion Unit, Drive 2
0-15	Hard Disk Drive	Second Expansion Unit, Drive 1
1-0	Hard Disk Drive	Base Unit, Drive 8
1-1	Hard Disk Drive	Base Unit, Drive 7
1-2	Hard Disk Drive	Base Unit, Drive 6
1-3	Hard Disk Drive	Base Unit, Drive 5
1-4	Channel-1 SCSI Bridge Board	All Units - ID shared by all Channel 0 Bridge Boards
1-5 & 1-6	Not Used	
1-7	SCSI Controller Card - Channel 1	Mylex SCSI RAID Controller is located in the Base Unit card cage. ID 1-7 controls all devices on Bus 1
1-8	Hard Disk Drive	First Expansion Unit, Drive 4
1-9	Hard Disk Drive	First Expansion Unit, Drive 3
1-10	Hard Disk Drive	First Expansion Unit, Drive 2
1-11	Hard Disk Drive	First Expansion Unit, Drive 1
1-12	Hard Disk Drive	Second Expansion Unit, Drive 4

Table #2 - Disk Array Components by SCSI Bus & ID Number (Sheet 2 of 2)

SCSI Bus:ID	Component Name	Component Location - Drive Number from Left
1-13	Hard Disk Drive	Second Expansion Unit, Drive 3
1-14	Hard Disk Drive	Second Expansion Unit, Drive 2
1-15	Hard Disk Drive	Second Expansion Unit, Drive 1
2-0	Hard Disk Drive	Base Unit, Drive 12
2-1	Hard Disk Drive	Base Unit, Drive 11
2-2	Hard Disk Drive	Base Unit, Drive 10
2-3	Hard Disk Drive	Base Unit, Drive 9
2-4 to 2-6	Not Used	
2-7	SCSI Controller Card - Channel 2	Mylex SCSI RAID Controller is located in the Base Unit card cage. ID 2-7 controls all devices on Bus 2.
2-8 to 2-15	Not Used	
3-0 to 3-3	Not Used	
3-4	Channel-3 SCSI Bridge Board	Base and Expansion Units. ID shared by all Channel 3 Bridge Boards. One Channel 3 Bridge board is located on each Expansion Unit. There is no Channel 3 Bridge board in the Base Unit.
3-5 & 3-6	Not Used	
3-7	SCSI Controller Card - Channel 3	Base Unit - Mylex SCSI RAID Controller is located in the Base Unit card cage. ID 3-7 controls all devices on Bus 3.
3-8	Hard Disk Drive	First Expansion Unit, Drive 12
3-9	Hard Disk Drive	First Expansion Unit, Drive 11
3-10	Hard Disk Drive	First Expansion Unit, Drive 10
3-11	Hard Disk Drive	First Expansion Unit, Drive 9
3-12	Hard Disk Drive	Second Expansion Unit, Drive 12
3-13	Hard Disk Drive	Second Expansion Unit, Drive 11
3-14	Hard Disk Drive	Second Expansion Unit, Drive 10
3-15	Hard Disk Drive	Second Expansion Unit, Drive 9

RAID Array Organization

The system logical drives are default configured as Redundant Arrays of Independent Disks (RAID). the RAID methodology and technique used varies with the function of the logical drive. The RAID techniques used in each logical drive are:

Base Unit Drive C:\ - System O/S:

- Factory configured
- A first RAID 1 striped across a partition on three drives with a second RAID 1 striped across another partition on three different drives.
- The two RAID 1 arrays above are combined into a RAID 0 mirrored array.
 - This array cannot be changed without damaging the O/S image.

Base Unit Drive D:\ - System Backup O/S:

- Factory configured
- The array setup is identical to drive C:\
- A first RAID 1 is striped across a partition on three drives with a second RAID 1 striped across another partition on three different drives.
- The two RAID 1 arrays above are combined into a RAID 0 – Mirrored array.
- This array cannot be changed without damaging the O/S image.

Base Unit Drive E:\ - User Data:

- Factory configured
- A RAID 5 striping with parity check array.
- Drive E:\ is set across the same six disk drives used by Drives C:\ and D:\ but in separate partitions.
- This array cannot be changed without damaging the O/S images.

Base Unit Drive F:\ - User Data:

- Factory configured
- Default configuration is a RAID 5 – Striping with parity check array.
- Drive F:\ is set across the remaining six drives in the Base Unit enclosure.
- The drive configuration can be modified to suit user needs.
- Drives can be set to any combination of RAID 0, RAID 1, RAID 0+1, RAID 3, RAID 5, JBOD, and/or a Hot Standby Drive.

First Expansion Unit Drive G:\ - User Data:

- User configured at installation
- Drive G:\ configuration and options are as drive F:\ above.

First Expansion Unit Drive H:\ - User Data:

- User configured at installation
- Drive H:\ configuration and options are as drive G:\ above.

Second Expansion Unit Drive I:\ - User Data:

- User configured at installation
- Drive I:\ configuration and options are as drive G:\ above.

Second Expansion Unit Drive J:\ - User Data:

- User configured at installation
- Drive J:\ configuration and options are as drive G:\ above.

Base Unit Operating System Arrays

The MaxAttach NAS 6000 operating system is Microsoft Windows-Powered Max Operating System Version 2.0 and is located on drive C:\. An duplicate backup O/S image located on drive D:\. The diagram below illustrated the O/S drive mapping.

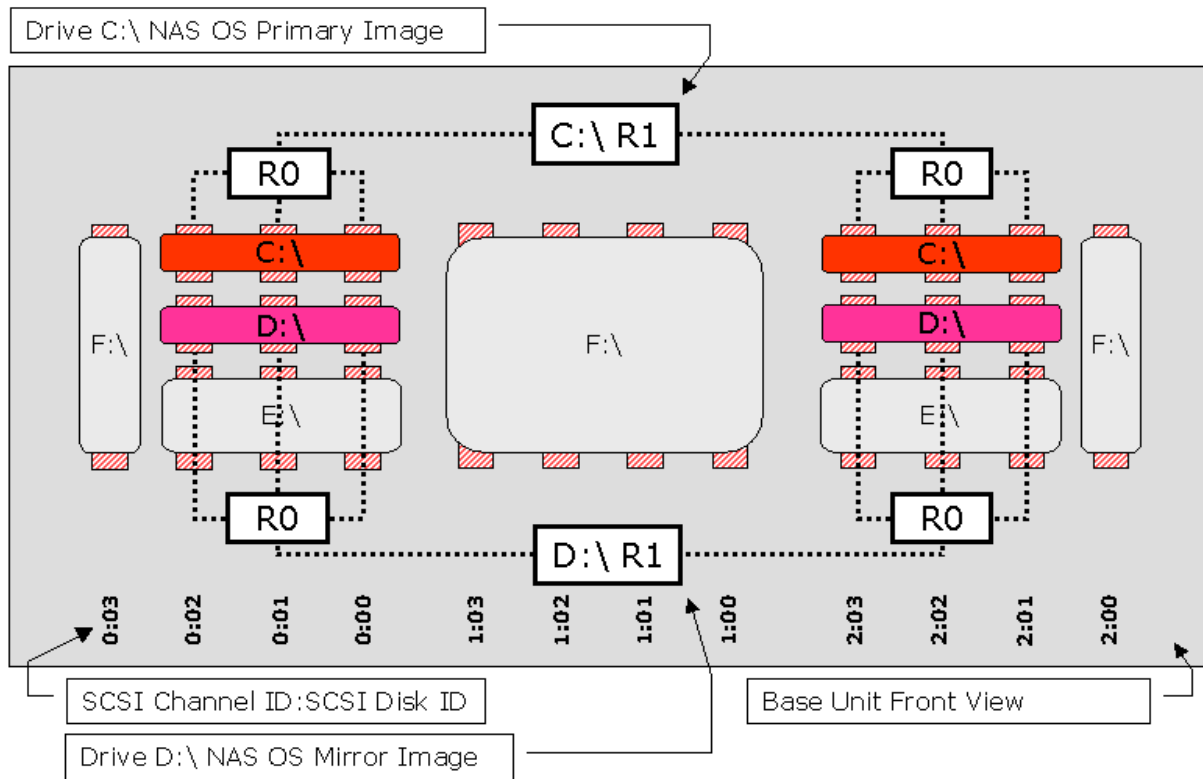


Figure #6 Base Unit OS Drive Arrays

Drive C:\

Each C:\ drive OS image is made up of partitions across three drives (RAID-0 Striping) which are mirrored on three other drives (RAID-1 Mirroring). The combination of these two techniques is called RAID 0+1.

Drive D:\

Similarly, the D:\ drive OS back up image is also made of up or partitions across three drives which are also mirrored on three other drives.

Base Unit User Data Arrays

The remainder of the MaxAttach NAS 6000 Base Unit disk space is for user data arrays. The array for drive E:\ cannot be changed because it shares physical disks with the operating system logical drives. Drive F:\ can be changed.

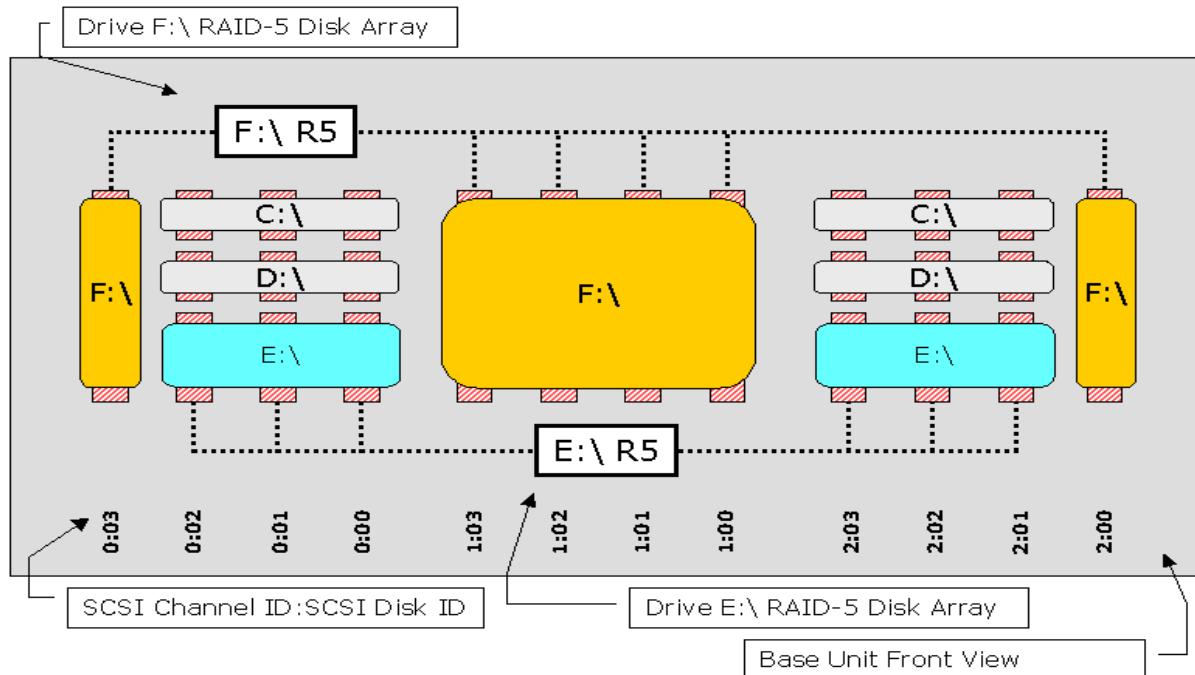


Figure #7 Base Unit User Data Drive Arrays

Drive E:\

Drive E:\ is available for user data but cannot be changed in size or configuration from the factory configured RAID 5 - Striping with distributed parity.

Drive F:\

Drive F:\ is available for user data and CAN be changed in size or configuration from the factory configured RAID 5. Possibilities include RAID 0 - Striping, RAID 1 - Mirroring, RAID 0+1 - Striping with mirroring, RAID 3 - striping with dedicated drive parity, or set to JBOD (just a bunch of disks), or create smaller arrays with one or more Hot Standby Drives.

First Expansion Unit User Data Arrays

- The first Expansion Unit comes unconfigured from the factory.
- At the end of the installation process, the drives are configured using the Mylex Global Array Manager (GAM) software that comes with the MaxAttach NAS 6000.
- The figure below shows the drives in the recommended default RAID 5 configuration.

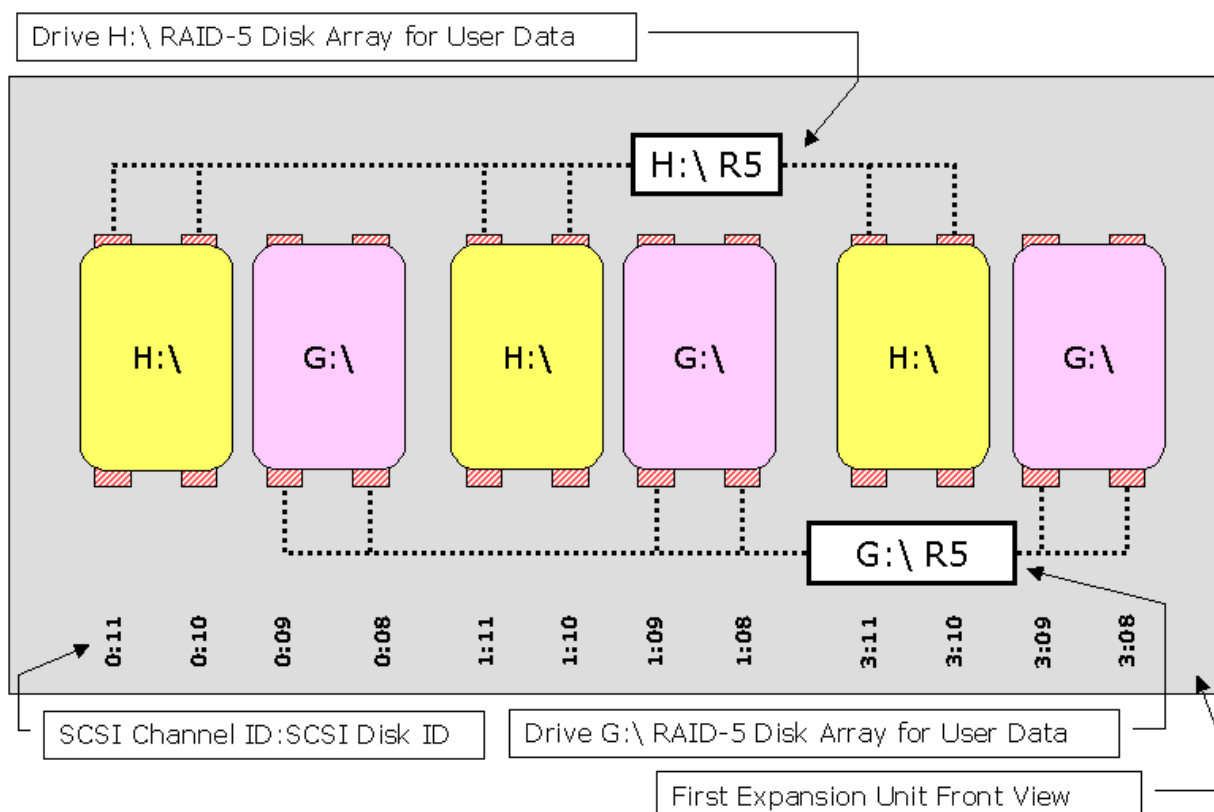


Figure #8 Expansion Unit One User Data Drive Arrays

Drive G:\ and Drive H:\

Drives G:\ and H:\ are available for user data. The recommended default configuration for both drives RAID 5. The RAID 5 arrays for both or either drives can be changed to other RAID configurations.

Second Expansion Unit User Data Arrays

The configuration recommendations and options for the second Expansion Unit are identical to those for the first Expansion Unit.

- The second Expansion Unit is The second Expansion Unit comes unconfigured from the factory.
- At the end of the installation process, the drives are configured using the GAM.
- The figure below shows the drives in the recommended default RAID 5 configuration

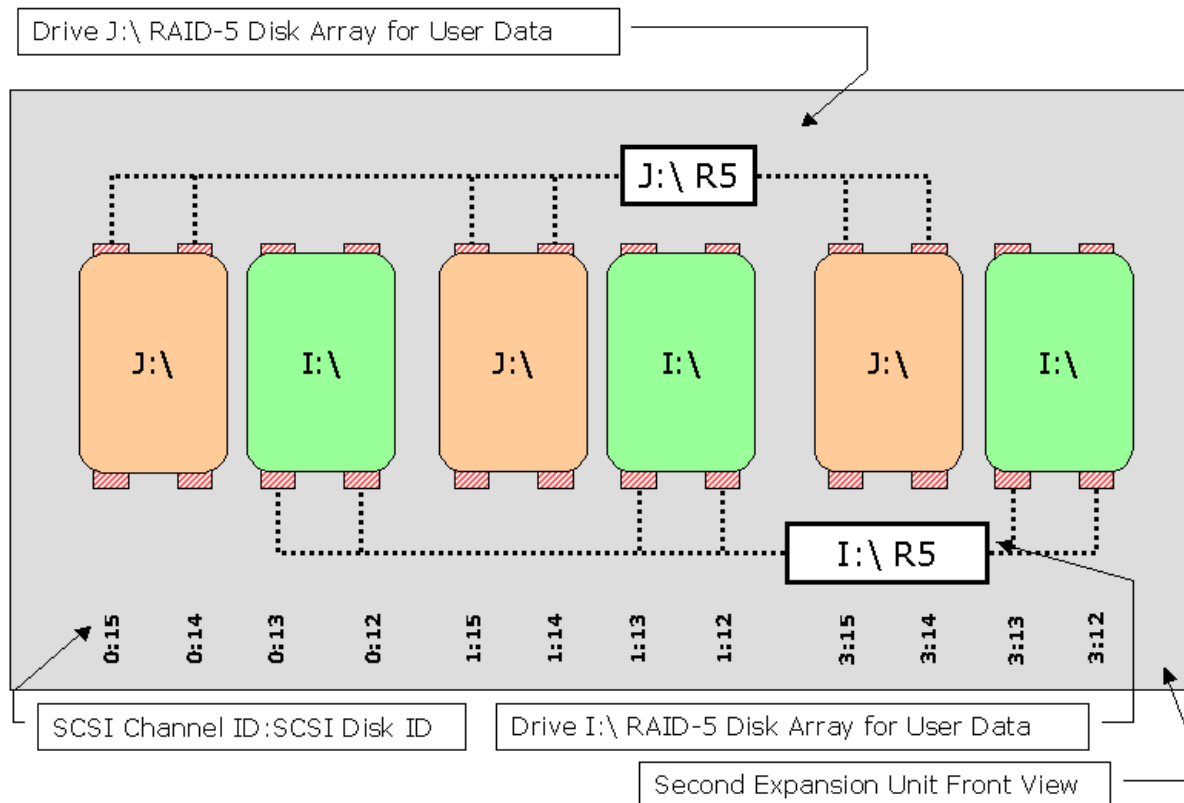


Figure #9 Expansion Unit Two User Data Drive Arrays

Drive I:\ and Drive J:\

Drives I:\ and J:\ are available for user data. The default configuration for both drives is RAID 5. The RAID 5 arrays for both drives can be changed to other RAID configurations.

Re-Configuring Your MaxAttach NAS 6000 Drive Arrays



WARNING

Any change to your RAID configuration can lead to loss of all user data, system lock up, or both. Before considering any RAID changes, completely read the appropriate sections of this manual.

Before performing any RAID re-configuration, ALWAYS back-up your data.

The RAID array configuration can be changed in all logical drives except C:\ and D:\ which are reserved for Max OS 2.0 and drive E:\ which shares the same physical drives in a separate partition.

Best Practices

System disk management best practices recommend several key tips for optimizing your disk arrays:

- Identify as many of your major disk uses as possible before allowing users on the system.
- If necessary, consider areas for high performance read/write operations where RAID 0 + 1 arrays may be appropriate.
- If necessary, consider areas for maximum reliability where RAID 1 arrays may be appropriated.
- To minimize the time an array is in a critical state due a single array disk drive failure, consider freeing up one or two physical hard disk drives and designating them as Hot Standby Drives. This is especially important if the system is located a long distance from the administration personnel. When an array is in a critical state, the failure of any additional array drive member will lose all user data in the array. With Hot Standby, the failed drive will be replaced and the rebuild process started immediately.
- If largest possible disk volume size is required, consider RAID 5 for optimum solutions. For absolute solutions, consider RAID 0.
- For additional security where absolute maximum size is not required, you may need JBOD.
- Regardless of the RAID configuration selected, make the arrays as large as possible so that they don't have to be changed.
- If you know that some arrays will be changed in the future, make them the last arrays to be configured. The GAM requires a LIFO approach to decommissioning drives and disassembling arrays. The last array built must be the first to be decommissioned. If you must reconfigure your first array, you will have to decommission all higher arrays before working on the first array.
- Think long term. Configure your arrays as large as possible and then leave them alone.

From there on, use the web user interface and the O/S to administer user needs.

To re-configure the disk RAID arrays

1. Read the *Administration Guide* for the MaxAttach NAS 6000.
2. Understand disk array concepts and the benefits and limitations of each disk array option.
3. Define your data volume needs as well as those of your users.
4. Read and understand the entire reconfiguration procedure.
5. Back up all your data.
6. Perform a test data recovery to make sure your back up image is correct and functional.
7. Load the GAM Client software onto your administrative workstation desktop.
8. Use the GAM Client software to modify the arrays to suit your needs.



WARNING

You cannot reconfigure the Max O/S drives on C:\ and D:\. In addition, you should not attempt to reconfigure the RAID 5 array on logical drive E:\. These three drives share the same physical disks on separate partitions. To do so would destroy the O/S image making the system non-functional and require a certified field representative to reimaging the system.

DO NOT CONSIDER USING any portion of C:\ or D:\ for local application or user data.

9. Allow ample time for the de-configuration and re-configuration process.
 - Each new array takes approximately six hours to rebuild. Time to completion varies with the size of the array, the number of physical disks involved, the total system load for background rebuilds, and whether the rebuild is running a background or foreground process.
10. Always consider the configuration and use of at least one Hot Standby Drive.
11. Arrays must be disassembled on a last in first out basis.
 - For example, consider a system where you a factory configured system with two Expansion Units providing user data on drives E:\, F:\, G:\, H:\, and I:\, and J:\.

- If you want to reconfigure drive H:\, you must first disassemble drive J:\, then drive I:\, and finally drive H:\. The disassembly process takes the drives out of their previous arrays and leaves them in the system with an “unconfigured status.”
 - During this process, all user data on the array is destroyed.
 - At this point, you can now reconfigure drive H:\ into a new configuration.
 - Then you would have to reconfigure drive I:\ to its original configuration followed by reconfiguring drive J:\.
12. Once the drive arrays have been reconfigured, use the Max O/S Web User Interface (UI) to reconfigure network, users, group, folder, and share option.

Chapter #5 - O/S 2.0 - Network Configuration

Chapter Outline

- Network initial setup
- Identification
 - Server Appliance Name
 - Global settings
 - DNS Name Resolution
 - TCP/IP Hosts
 - NetBIOS LMHOSTS file
 - IPX Settings
- Network adapter interfaces
 - Renaming a Connection
 - Apple Talk Local Area Network Connection
 - IP Address Configuration
 - DNS Configuration
 - WINS Configuration
- Change administrator password
- Administration web site
- Telnet
- Server configuration
- Network Interface Cards

Network Configuration Overview

From the Network page, you can choose which of the following network-related properties of the server appliance to configure:

- **Identification:** Set the name and domain membership of the server appliance.
- **Global Settings:** Configure network settings that apply to all network adapters on the server appliance.

- **Interfaces:** Configure the properties of each network adapter on the server appliance.
- **Administrator:** Change the password of the user account you are using to access the server appliance administration Web site.
- **Administration Web Site:** Specify which IP address(es) and port are used to access the administration Web site.
- **Telnet:** Configure Telnet to administer the server appliance.

Network Identification

The server appliance must be given a name. Client computers use this name to access the file shares that reside on this server appliance.

The server appliance can be configured as a member of one of the following groups:

- Microsoft® Windows NT® 4 domain
- Microsoft Active Directory™ domain
- Workgroup

If no workgroups exist on the network, for example, if this is a UNIX environment, the workgroups option should be selected and any arbitrary name used.

User accounts may also be created locally on the server appliance; however, using a domain or directory eliminates the need to create local user accounts for every user of the server appliance.

A good practice after joining a domain is to add one or more domain users to the local administrators group, then reconnect under those user names to administer the server appliance.

To set the name and domain membership of the server appliance

1. On the primary navigation bar, choose Network.
2. Choose Identification.
3. In the boxes provided, type the appropriate server appliance name and Domain Name System (DNS) suffix. The DNS suffix is appended to the host name to create the fully qualified machine name.

**NOTE**

Adding a DNS suffix is optional; however, if you want to set or change the name of your server appliance, this is the only box from which you can do so.

4. Select whether the client computer will be part of a workgroup or a domain.
5. If the machine will be part of a domain, type the user name and password of the person who has permission to add client computers to the domain.
6. If the server appliance is accessible to AppleTalk or NetWare clients, type the AppleTalk or NetWare name in the appropriate box.
7. By default:
 - The AppleTalk name of your server appliance will be the same as the standard server appliance name
 - The NetWare name must be different from the server appliance name.
 - The NetWare name will be the server appliance name with _NW appended to it.
8. Any changes to the server appliance name will update the Netware and AppleTalk names as well.
9. Choose OK.
10. When prompted to reboot the server appliance, you may either accept or cancel the reboot.
 - If you choose OK, the server appliance will reboot and the Restarting page will appear. When the server appliance has restarted, the Home Page of the Web user interface (UI) will display and your changes will be in effect.
 - If you choose Cancel, the changes to the server appliance identity will not take effect until the next reboot.

Related Topics

- DNS Name Resolution
- DNS Suffixes
- Domain
- Server Appliance Name
- Workgroup

Server Appliance Name

The server appliance name is the name of the MaxAttach NAS 6000 on a network. The server appliance name must be unique and must meet certain requirements. The new server appliance name cannot be the same as another computer or the name of a Microsoft Windows domain.

Server names recommendations are:

- It is recommended that you use names that are 15 characters or fewer.
- The server appliance name can be a maximum of 63 characters but should only contain the numbers 0–9, the uppercase letters A–Z, the lowercase letters a–z, or hyphens.
- You may use other characters, but doing so may prevent other users from finding your computer on the network. If your network is using the Microsoft DNS server, you can use any characters except periods.
- If other networking protocols are installed without TCP/IP, the server appliance name is limited to 15 characters.
- If you specify a server appliance name longer than 15 characters and you want longer names to be recognized by the Microsoft Active Directory domain, the domain administrator must enable registration of DNS names that are 16 characters or longer

Domain

Your server appliance can be in a workgroup, active directory environment, or Windows NT 4 domain. In Microsoft Windows NT 4 and Microsoft Active Directory environments, a domain is a collection of computers defined by the administrator of a network that share a common directory database.

Utilized for Windows user and group information, Windows domains have a unique name and provide access to the centralized user accounts and group accounts maintained by the domain administrator. Each domain has its own security policies and security relationships with other domains, and each domain represents a single security boundary of a Windows computer network. Active Directory is made up of one or more domains, each of which can span more than one physical location.

For DNS, a domain is any tree or subtree within the DNS name space. Although the names for DNS domains often correspond to Active Directory domains, DNS domains should not be confused with Microsoft Windows and Active Directory networking domains.

By default a domain user must enter domain\username when logging into a Web server appliance or a NAS with a Netscape browser.

To set the default domain used for login

1. On the primary navigation bar, choose Maintenance.
2. Choose Terminal Services.
3. Log onto Terminal Services.
4. Right-click My Computer and choose Manage.
5. Open Internet Information Services (IIS).
6. Right-click Administration Web site and choose Properties.
7. Select Directory Security.
8. In the Anonymous access and authentication control area, choose Edit.
9. In the Basic Authentication area, choose Edit.
10. Type the default domain name you want to use for authentication.

Related Topics

- Identification
- Server Appliance Name
- Workgroup
- UNIX (NFS)

Workgroup

A workgroup is a simple grouping of computers, intended only to help users find such things as printers and shared folders within that group. Your server appliance can be in a workgroup, active directory environment, or Windows NT 4 domain. Workgroups in Microsoft Windows 2000 do not offer the centralized user accounts and authentication offered by domains.

A workgroup name must not duplicate the computer name. A workgroup name can have as many as 15 characters, but cannot contain any of the following characters:
; : " < > + = \ | ? , .

To set or change the workgroup membership of the server appliance

1. On the primary navigation bar, choose Network.
2. Choose Identification.
3. Select the Workgroup button and type the name of the workgroup to join.
 - If the server appliance belonged to a domain before you joined the workgroup, the server appliance will be disjoined from the domain and the computer account will be disabled.
4. Choose OK.
5. You will be asked to reboot the server appliance.
6. Choose whether to reboot the server appliance.
 - If you choose OK, the server appliance will reboot and a page will appear indicating that the server appliance is restarting.
 - When the server appliance is back online, the default page of the Web UI will display and your changes will be in effect.
 - If you choose Cancel, the changes to the server appliance identity will not take effect until the next reboot.

Network Global Settings

From this page, you can change the overall network settings for your server appliance by configuring the IPX settings as well as specifying the DNS suffixes and the LMHOSTS and HOSTS file to use. These files can be used to resolve the names of any computer or device. Note that the DNS suffix used here applies when the server appliance is trying to resolve a host or domain name.

To automatically set or change DNS suffixes

1. On the primary navigation bar, choose Network.
2. Choose Global Settings.
3. Select the DNS Resolution tab.
4. Select the Append primary DNS suffix button.
5. Optional: you may choose to Append parent suffixes of the primary DNS suffix by selecting the check box.

6. Choose OK.

To manually add specific DNS suffixes

1. On the Network page, choose Global Settings.
2. Select the DNS Resolution tab.
3. Select the Append the following DNS suffixes, in order of use button.
4. In the Domain suffix box, type the DNS suffix you want to add, and then choose Add.
5. Choose OK.

To manually remove specific DNS suffixes

1. On the Network page, choose Global Settings.
2. Select the DNS Resolution tab.
3. Select the Append the following DNS suffixes, in order of use button.
4. Use the Up and Down buttons to scroll through the list of domain suffixes. Select the suffix you want to delete, and then choose Remove.
5. Choose OK.

Related Topics

- DNS Configuration (below)
- DNS Name Resolution (above)
- DNS Suffixes (above)
- NetBIOS LMHOSTS File (below)

DNS Name Resolution

So that people can reach your Web site on an intranet or the Internet, you must have a unique IP address that identifies your computer on the network. This address consists of a long string of numbers separated by dots, for example, 172.16.255.255. Because a numeric address is difficult for people to remember, text names, or friendly names, are used to

provide visitors with an easy-to-remember address, such as `www.microsoft.com`. Name resolution involves supplying the correct numerical address from the friendly name that was typed into a client browser.

Name Resolution Systems

Windows networking components rely on the NetBIOS naming convention. In contrast, TCP/IP components rely on a naming convention known as the Domain Name System (DNS). Under Windows, the DNS host name of your server appliance defaults to the same name as the NetBIOS computer name. The mapping of computer names to IP addresses can be accomplished using one of the following two methods:

- **Static:** The system administrator creates either a text file for DNS names, called a HOSTS file, or an LMHOSTS file for NetBIOS names, and enters each computer's name and IP address. The file is then distributed on the network. When a request for a connection to another computer is made, the file is used to resolve the name to the correct IP address. This system works well for simple networks that change infrequently.
- **Dynamic:** When a client computer connects to a network with a DHCP server, the DHCP server assigns an address and sends the IP address assignment to a Windows Internet Name Service (WINS) server. The WINS server registers the computer's name, and when a request is made for a NetBIOS computer name, the WINS server resolves the name to the correct IP address. This automatic recognition and mapping of computer names and addresses eases the administrative burden of large or frequently changing networks.

DNS names are typically resolved using static information. The DNS server contains a portion of the static database listing host names and addresses. If the requested name is not in the DNS server's portion of the database, it sends a query to other DNS servers to get the requested information. The DNS server that runs on Windows can be configured to query a WINS server for name resolution of the lower levels of the DNS hierarchical naming structure. Because WINS assigns computer names dynamically, this effectively changes DNS from a static system to a dynamic system.

DNS Configuration

The domain name system (DNS) is a static, hierarchical name service for TCP/IP hosts. The network administrator configures the DNS with a list of host names and IP addresses. This allows users on the network to query the DNS to specify remote systems by host names rather than IP addresses.

**NOTE**

The purpose of this property page is to allow you to enter the addresses of external DNS servers. The server appliance does not contain a DNS server.

For example, a workstation configured to use DNS name resolution could use the command ping remotehost rather than ping 1.2.3.4 if the mapping for the system named remotehost was contained in the DNS database. DNS domains should not be confused with Microsoft Windows domains.

In the DNS client-server model, the server containing information about a portion of the DNS database, the portion that makes computer names available to clients, queries for name resolution across the Internet.

To set the server appliance to automatically obtain DNS server information from a DHCP server

1. On the primary navigation bar, choose Network.
2. Choose Interfaces.
3. Select the network connection you want to modify.
4. In the Tasks list, choose DNS.
5. Select the Obtain configuration from DHCP server button.
6. Choose OK.

To manually set the DNS servers to be used by the server appliance

1. On the Network page, choose Interfaces.
2. Select the network connection you want to modify.
3. In the Tasks list, choose DNS.
4. Select the Configure manually button.
5. Type the appropriate IP address in the box next to the Add button, and then choose Add.
6. To add another DNS server, repeat step 5.

7. When you are finished adding DNS servers, choose OK.

**NOTE**

If you set the IP address to be obtained from DHCP, and you set DNS manually, the system will accept the manual input, and the properties on the server appliance will automatically be set to Configure manually. However, the Current Configuration column of the Object/Task Selector on the Interfaces page will still show DHCP as the source of the IP address. You can go back into the DNS settings properties page to confirm that the manual configuration has been saved.

Related Topics

- DNS Suffixes.
- DNS Name Resolution.

TCP/IP Hosts

Windows networking components rely on the NetBIOS naming convention. In contrast, TCP/IP components rely on a naming convention known as the Domain Name System (DNS). Under Windows, the DNS host name defaults to the same name as the NetBIOS computer name. The mapping of computer names to IP addresses can be accomplished using one of the following two methods:

- **Static:** The system administrator creates either a text file for DNS names, called a HOSTS file, or an LMHOSTS file for NetBIOS names, and enters each computer's name and IP address. The file is then distributed on the network. When a request for a connection to another computer is made, the file is used to resolve the name with the correct IP address. This system works well for simple networks that change infrequently.
- **Dynamic:** When a client computer logs on, a DHCP server assigns an address and sends the IP address assignment to a Windows Internet Name Service (WINS) server. The WINS server registers the computer's name, and when a request is made for a NetBIOS computer name, the WINS server resolves the name to the correct IP address. This automatic recognition and mapping of computer names and addresses eases the administrative burden of large or frequently changing networks.

DNS names are typically resolved using static information. The DNS server contains a portion of the static database listing host names and addresses. If the requested name is not in the DNS server's portion of the database, it sends a query to other DNS servers to get the requested information. The DNS server that runs on Windows can be configured to query

a WINS server for name resolution of the lower levels of the DNS hierarchical naming structure. Because WINS assigns computer names dynamically, this effectively changes DNS from a static system to a dynamic system.

If you are setting up multiple Web or FTP sites on a single server, each with its own IP address, you might encounter problems with automatic DNS registration. To ensure correct IP binding and DNS registration, disable Windows 2000 Server automatic DNS registration and manually configure DNS registration for the Web sites. For more information about disabling automatic DNS registration and manually configuring DNS registration, see the Windows 2000 Server documentation.

If you want to assign multiple names to one server appliance, you must use a static name assignment for the server appliance. On one computer you can map multiple names to one IP address or you can use multiple names, each one mapped to its own IP address.

To edit the Hosts file

1. On the **Network** page, choose **Global Settings**.
2. Select the **TCP/IP Hosts** tab. By default, the **Hosts file** box contains the current Hosts file configuration.
3. Change the Hosts file by clicking in the box and editing the information.
4. Choose **OK**.

Related Topics

- NetBIOS LMHOSTS File
- DNS Configuration
- DNS Name Resolution
- DNS Suffixes

NetBIOS LMHOSTS File

For people to reach your Web site, you must have a unique IP address that identifies your computer on the network. This address is a long string of numbers separated by dots, for example, 172.16.255.255. Because a numeric address is difficult for people to remember, text names or friendly names, are used to provide visitors with an easy-to-remember address, such as \\MyStoredFiles. Name resolution involves interpreting the correct numerical address from the friendly name a user types into a client browser. This section describes different name resolution systems.

The use of an LMHOSTS file is optional. If an LMHOSTS file is not used, however, you cannot use friendly text names. Instead, you must use IP addresses. This can be a disadvantage because Web sites on the Internet usually use the DNS. If you register a domain name for your Web site, users can contact your Web site by typing its domain name in a browser.

The LMHOSTS file is read when WINS or broadcast name resolution fails and resolved entries are stored in a system cache for later access. When the computer uses the replication service and does not use WINS, LMHOSTS file entries are required on import and export servers for any computers on different subnetworks participating in the replication.

You can use Microsoft Notepad or any text editor to edit the sample LMHOSTS.sam file that is automatically installed in the Windows directory. The following rules apply for entries in the LMHOSTS file:

- Each entry should be placed on a separate line.
- The IP address should begin in the first column, followed by the corresponding computer name. Entries in the LMHOSTS file are case-insensitive.
- The address and the computer name should be separated by at least one space or tab.
- The number (#) sign is typically used to mark the start of a comment. However, this character can also be used to designate special keywords, as described in this section.
- The keywords listed in the following table can be used in the LMHOSTS file. Notice, however, that LAN Manager 2.x treats these keywords as comments.

Table #1 - LMHOSTS Keywords and Definition

LMHOST Keywords	Keyword Definitions
#PRE	Causes an entry to be preloaded into the name cache. This keyword is added after an entry. The #PRE keywords in the LMHOSTS file are looked up and cached prior to WINS lookup. #PRE must be appended for entries that also appear in #INCLUDE statements; otherwise, the entry in #INCLUDE is ignored.
#DOM: <i>domain</i>	Associates an entry with the domain specified by <i>domain</i> . This keyword is added after an entry, and it affects how the browser and logon services behave in routed TCP/IP environments. To preload a #DOM entry, you must also add the #PRE keyword to the line.
#INCLUDE <i>filename</i>	Forces the system to seek the specified <i>filename</i> and parse it as if it were local. Specifying a universal naming convention (UNC) <i>filename</i> allows you to use a centralized LMHOSTS file on a server. You must map the server before its entry in the #INCLUDE section, and also append #PRE to ensure that it is preloaded (otherwise the #INCLUDE will be ignored).
#BEGIN_ALTERNATE	Groups multiple #INCLUDE statements. Any single successful #INCLUDE statement causes the group to succeed.

Table #1 - LMHOSTS Keywords and Definition

LMHOST Keywords	Keyword Definitions
#END_ALTERNATE	Marks the end of an #INCLUDE grouping.
\0xnn	Supports nonprinting characters in NetBIOS names. Enclose the NetBIOS name in quotation marks and use \0xnn hexadecimal notation to specify a hexadecimal value for the character. This allows custom applications that use special names to function properly in routed topologies. However, LAN Manager TCP/IP does not recognize the hexadecimal format, so you surrender backward compatibility if you use this feature. Notice that the hexadecimal notation applies only to one character in the name. The name should be padded with blanks so the special character is placed as the last, or 16th, character in the string).

The following example below shows how these keywords are used.

```

102.54.94.98      localsrv      #PRE
102.54.94.97      trey          #PRE #DOM:networking #net group's PDC
102.54.94.102     "appname     \0x14" #special app server
102.54.94.123     popular      #PRE      #source server
#BEGIN_ALTERNATE
#INCLUDE \\localsrv\public\LMHOSTS      #adds LMHOSTS files from this server
#INCLUDE \\trey\public\LMHOSTS          #adds LMHOSTS files from this server
#END_ALTERNATE

```

Note the following points from the example above:

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

Guidelines for LMHOSTS Files

When you use a host table file, be sure to keep it up-to-date and organized. Use the following guidelines:

- Update the LMHOSTS file whenever a computer is changed or removed from the network.
- Use **#PRE** statements to preload popular entries into the local computer's name cache. Also use **#PRE** statements to preload servers that are included with **#INCLUDE** statements.
- Because LMHOSTS files are searched from the beginning one line at a time, you can increase the search speed for the most commonly-used entries by placing statements for the most frequently-used servers near the top of the file. Follow these with statements for less frequently-used servers, and then follow these server statements with remote **#INCLUDE** statements. Type the **#PRE** entries at the end of the file because these

statements are preloaded into the cache at system startup time and are not accessed later. Remember that comment lines add to parsing time because each line is processed individually.

To edit the LMHOSTS file

1. From the primary navigation bar, choose Network.
2. Choose Global Settings.
3. Select the NetBIOS LMHOSTS tab.
4. Select the Enable LMHOSTS lookup check box.
 - By default, the box below the check box contains the current LMHOSTS file configuration; however, if there are no entries to be seen, the box will be empty.
5. Edit the LMHOSTS file by clicking in the box and changing the information.
6. Choose OK.

IPX Settings

Internetwork Packet Exchange (IPX) is the native NetWare protocol used on many earlier Novell networks.

To be accessible from clients running NetWare, your server appliance must provide an IPX address.

To configure the IPX address

1. From the primary navigation bar, choose Network.
2. Choose Global Settings.
3. Select the IPX Settings tab.
4. Enter a value in the Internal network number box, or leave the parameter's default value at 00000000.
5. Choose OK.

Network Adapter Interface

A network adapter provides the physical interface, or connector, and the hardware to let a computer access a network. A network adapter is also called an adapter card, a network interface card (NIC), or simply a card.

From the **Interfaces** page of the server appliance Web UI, you can perform one of the following tasks:

- Change the name of the connection.
- Set or change the Internet Protocol (IP) addresses, gateway addresses, subnet masks, and metrics.
- Set or change how the server appliance resolves DNS names.
- Set or change the configuration of the Windows Internet Naming Service (WINS) clients.
- Configure AppleTalk, if enabled by your server appliance manufacturer.

Configuring a Network Adapter

To configure a network adapter

1. Select the adapter you want from the **Description** column.
2. Select the task you want from the **Tasks** list.
3. On the **Task** page, use the tabs in the left pane to display the configuration of the network adapter you chose.

Related Topics

- IP Address Configuration
- DNS Configuration
- WINS Configuration
- Initial NAS Server Appliance Configuration
- Initial Web Server Appliance Configuration

Renaming a Connection

To rename an interface connection

1. From the primary navigation bar, choose **Network**.
2. Choose **Interfaces**.
3. Select the interface connection you want to rename.
4. In the **Tasks** list, choose **Rename**.
5. In the **New connection name** box, type the new name of the interface connection.
6. Choose **OK**.

AppleTalk Local Area Network Connection

Use the AppleTalk LAN Connection page to specify which network adapter can receive inbound AppleTalk connections and in which AppleTalk zone the MaxAttach will appear.

Configuring an AppleTalk Network Connection

To configure a network interface for AppleTalk

1. Log in to the MaxAttach as administrator.
2. Click **Network** on the main menu bar.
3. Select **Interfaces**. The Interfaces page displays.
4. Select the interface you want to configure by clicking a radio button in the Description column.
5. On the Tasks list, click **AppleTalk**. The AppleTalk Configuration page displays.
6. Set the **Enable inbound AppleTalk connections on this adapter** checkbox to permit the adapter to accept inbound AppleTalk traffic. Note that only one adapter per system can be so enabled. If another adapter is already enabled for inbound AppleTalk traffic, it will be automatically disabled.
7. If your network is organized into AppleTalk zones, use the pull-down list to select

the zone in which this system will appear.

Related Topics

- Setting AppleTalk Sharing Properties
- AppleTalk Service Properties

IP Address Configuration

Each computer on the network must have a unique IP address to send and receive data. You can use the **IP Address Configuration** page to have your server appliance automatically obtain the IP address configuration from the Dynamic Host Configuration Protocol (DHCP) server. Alternately, you can configure the IP address/es manually.

In addition, you can use the **IP Address Configuration** page to specify one or more *gateway addresses*. A gateway address is the address of a local IP router residing on the same network as the server appliance that is used to forward traffic to destinations beyond the local network. The value in each field must be a number from 0–255.



NOTE

Changing the IP address may cause the client to lose its connection with the server appliance. To reconnect, the user must either use the new IP address or wait until the DNS server is updated.

Changing IP General Tab Settings

To set or change the IP settings on the General tab

1. On the primary navigation bar, choose **Network**.
2. Choose **Interfaces**.
3. Select the network connection you want to modify.
4. In the **Tasks** list, choose **IP**.
5. Select the **General** tab.
6. Select whether to obtain the configuration automatically from the DHCP server, or to statically configure the IP address(es).
7. If you choose to obtain the configuration from the DHCP server, choose **OK**.

8. If you have chosen to use static IP settings, enter the IP address, Subnet mask, and Default gateway in the boxes provided.

Changing IP Settings on the Advanced Tab

To set or change the IP settings on the Advanced tab

1. On the primary navigation bar, choose **Network**.
2. Choose **Interfaces**.
3. Select the network connection you want to modify.
4. In the **Tasks** list, choose **IP**.
5. Select the **Advanced** tab.
6. In the **IP address** box on the right, type the IP address, and then choose **Add**.
7. If you have a local area connection, type the appropriate mask information in the **Subnet mask** box.
 - A *subnet mask* is a 32-bit number that is notated by using four numbers from 0–255, separated by periods.
 - Typically, default subnet mask numbers use either 0 or 255 as values, such as 255.255.255.0.
 - However, other numeric values can appear, indicating that the subnet is configured for a single TCP/IP network.
 - This number, with a value other than 0 or 255, is combined with the IP address number to identify the network on which your computer resides.
8. If necessary, update the **IP Connection Metric**.
 - The metric indicates the cost of using the routes associated with this connection and becomes the value in the Metric column for those routes in the IP routing table.
 - If there are multiple routes to a destination the route with the lowest metric is used. The default value is 1.
9. Repeat steps 1–3 for any other IP addresses you wish to add.

Changing Gateway Address Settings

To set or change the gateway address settings

1. In the **Gateway** and **Metric** boxes, type the IP address of both the default gateway and the metric, and then choose **Add**.
2. Repeat step 1 for each default gateway you want to add.
3. When you are finished modifying the configurations on this screen, choose **OK**.
 - at the subnet is configured for a single TCP/IP network.
 - This number, with a value other than 0 or 255, is combined with the IP address number to identify the network on which your computer resides.
4. If necessary, update the IP Connection Metric.
 - The metric indicates the cost of using the routes associated with this connection and becomes the value in the Metric column for those routes in the IP routing table.
 - If there are multiple routes to a destination the route with the lowest metric is used.
 - The default value is 1.
5. Repeat steps 1–3 for any other IP addresses you wish to add.

DNS Configuration

The domain name system (DNS) is a static, hierarchical name service for TCP/IP hosts. The network administrator configures the DNS with a list of host names and IP addresses. This allows users on the network to query the DNS to specify remote systems by host names rather than IP addresses.



NOTE

The purpose of this property page is to allow you to enter the addresses of external DNS servers. The server appliance does not contain a DNS server.

For example, a workstation configured to use DNS name resolution could use the command ping remotehost rather than ping 1.2.3.4 if the mapping for the system named remotehost was contained in the DNS database. DNS domains should not be confused with Microsoft Windows domains.

In the DNS client-server model, the server containing information about a portion of the DNS database, the portion that makes computer names available to clients, queries for name resolution across the Internet.

Obtaining IP Address from DHCP Server

To set the server appliance to automatically obtain DNS server information from a DHCP server

1. On the primary navigation bar, choose **Network**.
2. Choose **Interfaces**.
3. Select the network connection you want to modify.
4. In the **Tasks** list, choose **DNS**.
5. Select the **Obtain configuration from DHCP server** button.
6. Choose **OK**.

Manually Setting DNS Server to Use

To manually set the DNS servers to be used by the server appliance

1. On the **Network** page, choose **Interfaces**.
2. Select the network connection you want to modify.
3. In the **Tasks** list, choose **DNS**.
4. Select the **Configure manually** button.
5. Type the appropriate IP address in the box next to the **Add** button, and then choose **Add**.
6. To add another DNS server, repeat step 5.
7. When you are finished adding DNS servers, choose **OK**.

**NOTE**

If you set the IP address to be obtained from DHCP, and you set DNS manually, the system will accept the manual input, and the properties on the server appliance will automatically be set to **Configure manually**. However, the **Current Configuration** column of the **Object/Task Selector** on the **Interfaces** page will still show DHCP as the source of the IP address. You can go back into the **DNS settings** properties page to confirm that the manual configuration has been saved.

Related Topics

- For more information about DNS suffixes, see DNS Suffixes.
- For more information about DNS name resolution, see DNS Name Resolution.

WINS Configuration

This property page allows you to enter the addresses of external WINS servers. The server appliance does not contain a WINS server. For the purpose discussed here, the server appliance is a WINS client.

WINS-enabled client computers can be configured to make direct use of a WINS server. Most WINS client computers typically have more than one network basic input/output system (NetBIOS) name that they must register with the network. These names are used to publish various types of network service, such as the Messenger or Workstation Service that each computer can use in various ways to communicate with other computers on the network.

WINS-enabled clients communicate with the WINS server to allow you to complete the following tasks:

- Register client names in the WINS database.
- Renew client names with the WINS database.
- Release client names from the WINS database.
- Resolve names by obtaining mappings from the WINS database for user names, NetBIOS names, DNS names, and IP addresses.

Clients that are not WINS-enabled can use WINS proxies to participate in these processes in a limited way. If you are using a DHCP server to allocate WINS server IP addresses, you do not need to add WINS server addresses.

Keep in mind that the Web UI only allows you to manipulate two WINS addresses, and even then only if you statically assign the IP address for the adapter. If you have DHCP enabled, you can remove one or two existing addresses and add different addresses, but you will not be able to remove all WINS servers from a DHCP-enabled adapter. If you remove two WINS addresses and do not add at least one, DHCP will automatically assign WINS addresses.

WINS clients attempt to register their names with a WINS server when they start or join the network. Thereafter, WINS clients query the WINS server as needed to resolve remote names.

Changing WINS Settings

To change the WINS settings

1. On the primary navigation bar, choose **Network**.
2. Choose **Interfaces**.
3. Select the network connection you want to modify.
4. In the **Tasks** list, choose **WINS**.
5. In the **WINS servers** list, select the IP address of the WINS server you want to delete, and then choose **Remove**.
6. In the **WINS server address** box, type the IP address of the WINS server, and then choose **Add**.
7. Repeat steps 4 and 5 for each WINS server IP address you want to add.
8. Choose **OK**.

Administrator Account and Password

The server appliance comes with a set of default accounts. Only the administrator account has administrative privileges.

**NOTE**

If an administrator adds a domain account to the local administrators group, the domain user may access and administer the server appliance. However, the administrator cannot use the **Change Administrator Password** page to change his domain account password. This page can only be used to change the local administrator's account password.

When you change the administrator password, there is no explicit confirmation page. However, the password is successfully changed if no error message appears after you have submitted the change.

**NOTE**

You cannot change the administrator password if you are logged on as a domain user as it is outside the scope of the server appliance Web UI to make changes to domain user accounts, which are stored on the domain controller, rather than on the server appliance.

In this context, administrator relates to the user account that is a member of the local administrators group and is used by a current user to log on. It does not refer to the default administrator account, called *administrator*.

If you receive the error message **The password cannot be changed for this domain account** or **The account name cannot be changed for this domain account** when trying to change the administrator password or account name, you are logged on as a domain user. You must be logged on as the server appliance administrator to change the administrator password.

Changing Administrator Account Password

To change the administrator account password

1. Log on to the server appliance as **Administrator**.
2. On the primary navigation bar, choose **Network**.
3. Choose **Administrator**.
4. Type the current administrator password in the **Current password** box.
5. Type the new administrator password in the **New password** box.

**NOTE**

The new administrator password must conform to any password complexity rules in effect for the domain to which the server appliance belongs.

6. Retype the new administrator password in the **Confirm new password** box.
7. Choose **OK**.

Changing Administrator Account Name

To change the administrator account name

1. Log on to the server appliance as **Administrator**.
2. Choose **Network**.
3. Choose **Administrator**.
4. Type the new name for the administrator account in the **User name** box.
5. Choose **OK**.

Related Topics

- Configuring Network Attached Storage
- Configuring a Web Server Appliance

Administration Web Site

This feature allows you to change the IP address/es and port that can be used to access the administration Web site on the server appliance.

The default IP address to which the server appliance responds, or listens, is typically changed when the server appliance is only managed on a certain subnet or a separate management network.

The default listen ports for both encrypted and non-encrypted access can be modified as needed to work with existing network software and configurations, for example, when no traffic above a given port number is allowed.

Changing Administration Web Site Properties

To change the administration web site properties

1. On the primary navigation bar, choose **Network**.
2. Choose **Administration Web Site**.
3. On the **Administration Site Properties** page:
4. Specify whether to use **All IP addresses** or **Just this IP address**.
5. If you choose to use **Just this IP address**, use the list to select the IP address you want to use.
6. If changing the port for non-encrypted access, type the new port number in the **Port for non-encrypted access** box.
7. If changing the port for encrypted access, type the new port number in the **Port for encrypted (SSL) access** box.
8. Choose **OK**.

Telnet

The Telnet Administration Configuration feature allows you to administer your Windows® Powered server appliance from a remote system using the Telnet protocol. You can log onto the system from a remote Telnet client and run character-mode applications on the server appliance. The Telnet server included with your server appliance supports a maximum of two Telnet clients at any time, unless otherwise specified by your server appliance hardware manufacturer.

Configuring System for Telnet Administration

To configure the MaxAttach NAS 6000 for Telnet administration

1. On the primary navigation bar, choose **Network**.
2. Choose **Telnet**.
3. Select the **Enable Telnet access to this appliance** check box.
4. Choose **OK**.

Network Adapter Interfaces

A network adapter provides the physical interface, or connector, and the hardware to let a computer access a network. A network adapter is also called an adapter card, a network interface card (NIC), or simply a card.

From the Interfaces page of the server appliance Web UI, you can perform one of the following tasks:

- Change the name of the connection.
- Set or change the Internet Protocol (IP) addresses, gateway addresses, subnet masks, and metrics.
- Set or change how the server appliance resolves DNS names.
- Set or change the configuration of the Windows Internet Naming Service (WINS) clients.
- Configure AppleTalk, if enabled by your server appliance manufacturer.

Configuring Network Adapters

To configure a network adapter

1. Select the adapter you want from the Description column.
2. Select the task you want from the Tasks list.
3. On the Task page, use the tabs in the left pane to display the configuration of the network adapter you chose.

Related Topics

- IP Address Configuration
- DNS Configuration
- WINS Configuration
- Initial NAS Server Appliance Configuration
- Initial Web Server Appliance Configuration

Renaming a Connection

To rename an interface connection

1. From the primary navigation bar, choose Network.
2. Choose Interfaces.
3. Select the interface connection you want to rename.
4. In the Tasks list, choose Rename.
5. In the New connection name box, type the new name of the interface connection.
6. Choose OK.

Apple Talk Local Area Network Connection

Use the AppleTalk LAN Connection page to specify which network adapter can receive inbound AppleTalk connections and in which AppleTalk zone the MaxAttach will appear.

To configure a network interface for AppleTalk

1. Log in to the MaxAttach as administrator.
2. Click Network on the main menu bar.
3. Select Interfaces. The Interfaces page displays.
4. Select the interface you want to configure by clicking a radio button in the Description column.
5. On the Tasks list, click AppleTalk. The AppleTalk Configuration page displays.
6. Set the Enable inbound AppleTalk connections on this adapter checkbox to permit the adapter to accept inbound AppleTalk traffic. Note that only one adapter per system can be so enabled. If another adapter is already enabled for inbound AppleTalk traffic, it will be automatically disabled.
7. If your network is organized into AppleTalk zones, use the pull-down list to select the zone in which this system will appear.

Related Topics

- Setting AppleTalk Sharing Properties

- AppleTalk Service Properties

IP Address Configuration

Each computer on the network must have a unique IP address to send and receive data. You can use the IP Address Configuration page to have your server appliance automatically obtain the IP address configuration from the Dynamic Host Configuration Protocol (DHCP) server. Alternately, you can configure the IP address(es) manually.

In addition, you can use the IP Address Configuration page to specify one or more gateway addresses. A gateway address is the address of a local IP router residing on the same network as the server appliance that is used to forward traffic to destinations beyond the local network. The value in each field must be a number from 0–255.



NOTE

Changing the IP address may cause the client to lose its connection with the server appliance. To reconnect, the user must either use the new IP address or wait until the DNS server is updated.

To set or change the IP settings on the General tab

1. On the primary navigation bar, choose Network.
2. Choose Interfaces.
3. Select the network connection you want to modify.
4. In the Tasks list, choose IP.
5. Select the General tab.
6. Select whether to obtain the configuration automatically from the DHCP server, or to statically configure the IP address(es).
7. If you choose to obtain the configuration from the DHCP server, choose OK.
8. If you have chosen to use static IP settings, enter the IP address, Subnet mask, and Default gateway in the boxes provided.

To set or change the IP settings on the Advanced tab

1. On the primary navigation bar, choose Network.

2. Choose Interfaces.
3. Select the network connection you want to modify.
4. In the Tasks list, choose IP.
5. Select the Advanced tab.
6. In the IP address box on the right, type the IP address, and then choose Add.
 - If you have a local area connection, type the appropriate mask information in the Subnet mask box.
 - A subnet mask is a 32-bit number that is notated by using four numbers from 0–255, separated by periods.
 - Typically, default subnet mask numbers use either 0 or 255 as values, such as 255.255.255.0.
 - However, other numeric values can appear, indicating that the subnet is configured for a single TCP/IP network.
 - This number, with a value other than 0 or 255, is combined with the IP address number to identify the network on which your computer resides.
7. If necessary, update the IP Connection Metric.
 - The metric indicates the cost of using the routes associated with this connection and becomes the value in the Metric column for those routes in the IP routing table.
 - If there are multiple routes to a destination the route with the lowest metric is used.
 - The default value is 1.
8. Repeat steps 1–3 for any other IP addresses you wish to add.

To set or change the gateway address settings

1. In the Gateway and Metric boxes, type the IP address of both the default gateway and the metric, and then choose Add.
2. Repeat step 1 for each default gateway you want to add.
3. When you are finished modifying the configurations on this screen, choose OK.

DNS Configuration

The domain name system (DNS) is a static, hierarchical name service for TCP/IP hosts. The network administrator configures the DNS with a list of host names and IP addresses. This allows users on the network to query the DNS to specify remote systems by host names rather than IP addresses.



NOTE

The purpose of this property page is to allow you to enter the addresses of external DNS servers. The server appliance does not contain a DNS server.

For example, a workstation configured to use DNS name resolution could use the command `ping remotehost` rather than `ping 1.2.3.4` if the mapping for the system named `remotehost` was contained in the DNS database. DNS domains should not be confused with Microsoft Windows domains.

In the DNS client-server model, the server containing information about a portion of the DNS database, the portion that makes computer names available to clients, queries for name resolution across the Internet.

To set the server appliance to automatically obtain DNS server information from a DHCP server

1. On the primary navigation bar, choose Network.
2. Choose Interfaces.
3. Select the network connection you want to modify.
4. In the Tasks list, choose DNS.
5. Select the Obtain configuration from DHCP server button.
6. Choose OK.

To manually set the DNS servers to be used by the server appliance

1. On the Network page, choose Interfaces.
2. Select the network connection you want to modify.
3. In the Tasks list, choose DNS.

4. Select the Configure manually button.
5. Type the appropriate IP address in the box next to the Add button, and then choose Add.
6. To add another DNS server, repeat step 5.
7. When you are finished adding DNS servers, choose OK.

**NOTE**

If you set the IP address to be obtained from DHCP, and you set DNS manually, the system will accept the manual input, and the properties on the server appliance will automatically be set to Configure manually. However, the Current Configuration column of the Object/Task Selector on the Interfaces page will still show DHCP as the source of the IP address. You can go back into the DNS settings properties page to confirm that the manual configuration has been saved.

Related Topics

- DNS Suffixes.
- DNS Name Resolution.

WINS Configuration

This property page allows you to enter the addresses of external WINS servers. The server appliance does not contain a WINS server. For the purpose discussed here, the server appliance is a WINS client.

WINS-enabled client computers can be configured to make direct use of a WINS server. Most WINS client computers typically have more than one network basic input/output system (NetBIOS) name that they must register with the network. These names are used to publish various types of network service, such as the Messenger or Workstation Service that each computer can use in various ways to communicate with other computers on the network.

WINS-enabled clients communicate with the WINS server to allow you to complete the following tasks:

- Register client names in the WINS database.
- Renew client names with the WINS database.
- Release client names from the WINS database.
- Resolve names by obtaining mappings from the WINS database for user names, NetBIOS names, DNS names, and IP addresses.

Clients that are not WINS-enabled can use WINS proxies to participate in these processes in a limited way. If you are using a DHCP server to allocate WINS server IP addresses, you do not need to add WINS server addresses.

Keep in mind that the Web UI only allows you to manipulate two WINS addresses, and even then only if you statically assign the IP address for the adapter. If you have DHCP enabled, you can remove one or two existing addresses and add different addresses, but you will not be able to remove all WINS servers from a DHCP-enabled adapter. If you remove two WINS addresses and do not add at least one, DHCP will automatically assign WINS addresses.

WINS clients attempt to register their names with a WINS server when they start or join the network. Thereafter, WINS clients query the WINS server as needed to resolve remote names.

To change the WINS settings of the server appliance

1. On the primary navigation bar, choose Network.
2. Choose Interfaces.
3. Select the network connection you want to modify.
4. In the Tasks list, choose WINS.
5. In the WINS servers list, select the IP address of the WINS server you want to delete, and then choose Remove.
6. In the WINS server address box, type the IP address of the WINS server, and then choose Add.
7. Repeat steps 4 and 5 for each WINS server IP address you want to add.
8. Choose OK.

Change Administrator Password

The server appliance comes with a set of default accounts. Only the administrator account has administrative privileges.

**NOTE**

If an administrator adds a domain account to the local administrators group, the domain user may access and administer the server appliance. However, the administrator cannot use the Change Administrator Password page to change his domain account password. This page can only be used to change the local administrator's account password.

When you change the administrator password, there is no explicit confirmation page. However, the password is successfully changed if no error message appears after you have submitted the change.

**NOTE**

You cannot change the administrator password if you are logged on as a domain user as it is outside the scope of the server appliance Web UI to make changes to domain user accounts, which are stored on the domain controller, rather than on the server appliance.

In this context, administrator relates to the user account that is a member of the local administrators group and is used by a current user to log on. It does not refer to the default administrator account, called administrator.

If you receive the error message “**The password cannot be changed for this domain account**” or “**The account name cannot be changed for this domain account**” when trying to change the administrator password or account name, you are logged on as a domain user. You must be logged on as the server appliance administrator to change the administrator password.

To change the administrator account password

1. Log on to the server appliance as Administrator.
2. On the primary navigation bar, choose Network.
3. Choose Administrator.
4. Type the current administrator password in the Current password box.
5. Type the new administrator password in the New password box.

**NOTE**

Note The new administrator password must conform to any password complexity rules in effect for the domain to which the server appliance belongs.

6. Retype the new administrator password in the Confirm new password box.
7. Choose OK.

To change the administrator account name

1. Log on to the server appliance as Administrator.
2. Choose Network.
3. Choose Administrator.
4. Type the new name for the administrator account in the User name box.
5. Choose OK.

Related Topics

- [Configuring Network Attached Storage](#)
- [Configuring a Web Server Appliance](#)

Administration Web Site

This feature allows you to change the IP address(es) and port that can be used to access the administration Web site on the server appliance.

The default IP address to which the server appliance responds, or listens, is typically changed when the server appliance is only managed on a certain subnet or a separate management network.

The default listen ports for both encrypted and non-encrypted access can be modified as needed to work with existing network software and configurations, for example, when no traffic above a given port number is allowed.

To change the administration web site properties

1. On the primary navigation bar, choose Network.
2. Choose Administration Web Site.
3. On the Administration Site Properties page:
4. Specify whether to use **All IP addresses** or **Just this IP address**.
5. If you choose to use **Just this IP address**, use the list to select the IP address you want to use.
6. If changing the port for non-encrypted access, type the new port number in the Port for non-encrypted access box.
7. If changing the port for encrypted access, type the new port number in the Port for encrypted (SSL) access box.
8. Choose OK.

Telnet

The Telnet Administration Configuration feature allows you to administer your Windows® Powered server appliance from a remote system using the Telnet protocol. You can log onto the system from a remote Telnet client and run character-mode applications on the server appliance. The Telnet server included with your server appliance supports a maximum of two Telnet clients at any time, unless otherwise specified by your server appliance hardware manufacturer.

To configure your NAS 6000 appliance for Telnet administration

1. On the primary navigation bar, choose Network.
2. Choose Telnet.
3. Select the Enable Telnet access to this appliance check box.
4. Choose OK.

Network Interface Cards

The MaxAttach can support up to three network interface ports. In addition to the Base Unit Network Port, the system is configured with two additional network interface cards (NICs):

- a gigabit Ethernet NIC with copper wire CAT-5E connections
- a gigabit Ethernet NIC with fiber optic connections.

Standard Configuration

Every installed NIC must be assigned a unique IP address. Clients attached to a particular network type (10BaseT/100BaseTX, Gigabit copper, Gigabit fiber) access the MaxAttach at the IP address assigned to each LAN adapter.

The software drivers for each NIC have been pre-installed at the factory. There is no user configuration required other than entering local area network parameters (IP address, etc.).

All setup operations for the installed network interfaces are automatic. Once the cables are attached, there are no user controls or adjustments. The devices automatically detect the network speed and configure themselves for optimum throughput.

Base Unit Network Port

Every system is equipped with a standard IEEE 802.3/IEEE 802.3U-LAN-compliant 10BaseT/100BaseTX Fast Ethernet port. It is supplied on the CPU motherboard of the MaxAttach Base Unit. the port is accessible on the Base Unit Back Panel in the CPU I/O Panel area.

The LAN connector for this port is a standard RJ-45, compatible with standard CAT 3, 4, and 5 UTP cabling for 10BaseT operation (10 Mb/s) and Cat-5 UTP cabling for 100BaseTX operation (100 Mb/s).

Simple Network Management Protocol - SNMP



NOTE

For detailed information on Simple Network Management Protocol (SNMP) and its use with the MaxAttach NAS 6000, see **Chapter #12 - Appendix - SNMP** on page 270.

The Maxtor MaxAttach NAS 6000 SNMP service provides SNMP (Simple Network Management Protocol) agents that can participate in remote, centralized management via SNMP management consoles.

Chapter #6 - O/S 2.0 - Disk and Volume Properties

Chapter Outline

- Disks and volumes
- Disk quota
- Establish default quotas
- Enabling quota management
- Quota entries
- Adding quota entries
- Removing quota entries
- Modifying quota properties
- Persistent storage manager and images

Disks and Volumes

Log on to use Windows 2000 Disk Management Snap-in. When you are finished, close the snap-in window. This will automatically close the Terminal Services Client Session

Disk Quota Management

Disk quotas track and control disk space use in volumes. You can configure the volumes on your server appliance to perform the following tasks:

- Prevent further disk space use and log an event when a user exceeds a specified disk space limit.
- Log an event when a user exceeds a specified disk space warning level.

When you enable disk quotas, you can set both the disk quota limit and the disk quota warning level. The disk quota limit specifies the amount of disk space a user is allowed to use. The warning level specifies the point at which a user is nearing his or her quota limit. For example, you can set a user's disk quota limit to 50 megabytes (MB), and the disk quota

warning level to 45 MB. In this case, the user can store no more than 50 MB on the volume. If the user stores more than 45 MB on the volume, you can have the disk quota system log a system event.

In addition, you also can specify that users can exceed their quota limit. Enabling quotas and not limiting disk space use is useful when you do not want to deny users access to a volume, but want to track disk space use on a per-user basis. You can also specify whether or not to log an event when users exceed either their quota warning level or their quota limit.

When you enable disk quotas for a volume, volume usage is automatically tracked from that point forward, but existing volume users have no disk quotas applied to them. You can apply disk quotas to existing volume users by adding new quota entries on the Quota Entries page.

Related Topics

- Enabling Quota Management.
- Quota Entries.

Enabling Quota Management

When you enable disk quotas on a volume, every user's disk volume usage is monitored and treated differently depending on the quota management settings for the specific user. For example, users who have write access to the volume and who have not exceeded their quota limit can store data on the volume. The first time a user writes data to a quota-enabled volume, default values for the disk space limit and the warning level are automatically assigned by the quota system.

To enable or disable quota management on a volume

1. On the primary navigation bar, choose Disks.
2. Choose Disk Quota.
3. Select the volume you want to manage.
4. In the Tasks list, choose Quota.
5. On the Quota for Volume (volume) page, select or clear the check box for Enable quota management.
6. Select the default quota limit for new users on this volume

7. Specify which quota events should be logged.
8. Choose OK.

Quota Entries

The Quota Entries page allows you to add, delete, or configure disk quotas for any server appliance user. Quotas are managed using the Object/Task Selector, which has the following columns:

- **Logon Name:** This column displays the logon name of each user with registered access to the server appliance.
- **Status:** This column indicates whether or not the user has exceeded the assigned quota limit.
- **Amount Used:** This column indicates the amount of disk space currently being used by a given user.
- **Quota Limit:** This column indicates the maximum amount of disk space that a user can occupy on a volume.
 - How the server appliance behaves when the quota limit is exceeded depends on the settings on the Quota property page, accessible through the Disk Quota tab.
 - If the Deny disk space to users exceeding quota limit check box is selected, the user will not be able to exceed this limit.
 - If the Log event when a user exceeds their quota limit check box is selected, an event log message will be logged. If neither option is selected, no action is taken.
- **Warning Level:** ■ This column indicates the maximum amount of disk space that a particular user can use before a warning appears indicating that the quota has nearly been reached.



NOTE

A warning will only be generated if the user exceeds the warning limit specified on the Quota Entries page, and if a Log event is selected on the Default Quota page. If the Log event check box is not selected, no warning will be generated and this column will remain empty. Typically the Warning Limit value is set slightly fewer than the Quota Limit value.

To set or change quota entries on the server appliance

1. On the primary navigation bar, choose Disks.
2. Choose Disk Quota.
3. Select the volume you want to manage.

4. From the Tasks list, choose Quota Entries.

Adding Quota Entries

To add a new quota entry

1. On the primary navigation bar, choose Disks.
2. Choose Disk Quota.
3. Select the volume you want to manage.
4. In the Tasks list, choose Quota Entries.
5. In the Tasks list, choose New.
6. Select a local user from the list, or type the name of a domain account in the box, using the <domain name\user name> format.

To allow unlimited disk use

1. Select the Do not limit disk usage button.

To limit disk space

1. Select the Limit disk space to button.
2. In the box, type a numerical value to specify the amount of disk space to assign to a particular user or group. Use the list to indicate kilobytes (KB), megabytes (MB), gigabytes (GB), terabytes (TB), petabytes (PB), or exabytes (EB).
3. Type the amount of disk space which, when filled, will trigger a warning to the user or group member that she is near her disk capacity limit. Use the list to indicate KB, MB, GB, TB, PB, or EB.
4. Choose OK.

Removing Quota Entries

To remove a quota entry

1. On the primary navigation bar, choose Disks.

2. Choose Disk Quota.
3. Select the volume you want to manage.
4. In the Tasks list, choose Quota Entries.
5. From the Quota Entries page, select the logon name from which you want to remove the quota entry.
6. In the Tasks list, choose Delete.
7. Choose OK.

Modifying Quota Properties

To modify the properties of a quota entry

1. On the primary navigation bar, choose Disks.
2. Choose Disk Quota.
3. Select the volume you want to manage.
4. In the Tasks list, choose Quota Entries.
5. On the Quota Entries page for the selected volume, select a user account.
6. In the Tasks list, choose Properties.
7. On the Quota entry for user page, perform one of the following tasks:

To allow unlimited disk use

1. Select the Do not limit disk usage button.

—OR—

To limit disk space

1. Select the Limit disk space to button.
2. In the box, type a numerical value to specify the amount of disk space to assign to a particular user or group. Use the list to indicate KB, MB, GB, TB, PB, or EB.
3. Type the amount of disk space which, when filled, will trigger a warning to the user

or group member that she is near her disk capacity limit. Use the list to indicate KB, MB, GB, TB, PB, or EB.

4. Choose OK.

To modify the properties of multiple quota entries

1. On the primary navigation bar, choose Disks.
2. Choose Disk Quota.
3. Select the volume you want to manage.
4. In the Tasks list, choose Quota Entries.
5. On the Quota Entries page for the selected volume, select multiple user accounts.
6. In the Tasks list, choose Properties.
7. On the Quota entry for user page, perform one of the following tasks:

To allow unlimited disk use

1. Select the Do not limit disk usage button.

—OR—

To limit disk space

1. Select the Limit disk space to button.
2. In the box, type a numerical value to specify the amount of disk space to assign to a particular user or group. Use the list to indicate KB, MB, GB, TB, PB, or EB.
3. Type the amount of disk space which, when filled, will trigger a warning to the user or group member that she is near her disk capacity limit. Use the list to indicate KB, MB, GB, TB, PB, or EB.
4. Choose OK.

Persistent Storage Manager and Images

The Persistent Storage Manager allows the creation and preservation of persistent images, “point-in-time” volume snapshots for the server appliance. Each persistent image (snapshot) is mounted as a volume on the file system to allow read-only or read-write access by clients. A persistent image can be created immediately through this configuration system or scheduled as a one time only or regularly repeated event.

Related Topics

- Although a part of the Disks and Volume navigation page, this topic is covered in the next chapter. For more information, see **Chapter #7 - Persistent Storage Manager** on page 175.

Chapter #7 - Persistent Storage Manager

Chapter Outline

- Persistent Storage Manager Overview
- Persistent Image Manager Overview
- Using Persistent Storage Manager
- Setting up Persistent Storage Manager
- Managing Persistent Storage Manager Schedules
- Managing Persistent Image Schedules
- Restoring a Volume Set from a Persistent Image

Persistent Storage Manager Introduction

Persistent Storage Manager (PSM) allows you to create “snapshot” images of volumes on your Maxtor MaxAttach NAS 6000. These snapshots, called persistent images, preserve data on selected volumes in case of a system or power failure. Each persistent image is saved as a volume on the file system to allow clients read-only or read/write access to the data and volume set. You can create a persistent image immediately through configuration system or schedule it as a one-time or a recurring event.

Once created, a persistent image of a volume appears as a directory on the original volume and can be used the same as the original source volume. However, unlike conventional volumes, persistent images can be restored to the precise content of the original volume at the time the snapshot was created.

PSM is fully integrated with Microsoft Windows Scheduler, allowing complete unattended management of persistent image creation and rotation of a periodic basis.

Use the Persistent Storage Manager page under the Disks and Volumes page to control system resource usage, optimization, and persistent image management.

Persistent Storage Manager and Images

The Persistent Storage Manager allows the creation and preservation of persistent images, “point-in-time” volume snapshots for the server appliance. Each persistent image (snapshot) is mounted as a volume on the file system to allow read-only or read-write access by clients. A persistent image can be created immediately through this configuration system or scheduled as a one time only or regularly repeated event.

Using Persistent Storage Manager

Once created, a persistent image (snapshot) of a volume appears as a directory on the original volume. Access rights and permissions from the original volume are inherited by the image. Images are used exactly the same as conventional system volumes. Unlike conventional volumes, persistent images can record or be restored to the precise content of the originating volume at the time the snapshot was created.

Persistent Image Scheduling

The Persistent Storage Manager is fully integrated with the Windows scheduler allowing complete unattended management of persistent image creation on a periodic basis.

Disaster Recovery

If the need arises, any Persistent Image may be instantly restored to the originating volumes.

Administration

Configuration elements relating to system resource usage and optimization and persistent image management are controlled through this system.

Detailed help is available for each of the Persistent Storage Manager control panels and topics.

Related Topics

- Persistent Storage Manager Overview
- Setting Up Persistent Storage Manager
- Managing Persistent Images
- Creating New Images
- Deleting Existing Images

- Undoing Writes on Read-Write Images
- Viewing and Changing Image Read-Write Attributes and Retention Weight
- View image context within a Schedule Group.
- Managing Persistent Image Schedules
- Creating New Image Schedule Items
- Deleting Existing Schedule Items
- Viewing and Changing Schedule Item Properties
- Using Disaster Recovery
- Restoring a Volume set Image

Setting Up Persistent Storage Manager

Persistent Storage Manager Configuration

From this page, you can modify the various aspects of the Persistent Storage Manager using pull-down selectors. Some of the options will be display-only if any persistent images are active. The Restore Defaults button will re-establish the system defaults.

Configuration Fields

The following fields allow you to configure the timing and characteristics of your persistent image snapshot.

- **Maximum Persistent Images:** Specifies the maximum number of active persistent images supported by the server, up to a maximum of 250. If starting another persistent image would exceed this number the system will delete an old persistent image.
- **Quiescent Period:** Prior to starting a persistent image, the system will wait for a period of relative inactivity on the volume being imaged. The default value will allow systems to start an image with a consistent file set and a minimal time-out. This value may be reduced or increased by experienced administrators for system optimization. Reducing the Quiescent Period will allow persistent images to begin on systems where disk inactivity is rare, at the possible expense of synchronization problems within applications which are concurrently writing to multiple files.
- **Quiescent Time-Out:** Specifies the amount of time the server should retry starting a persistent image. A persistent image won't start until a period of relative inactivity, set by the Quiescent Period. If an interval longer than Quiescent Time-Out passes before the persistent image can begin it will be abandoned.
- **Cache Full Warning Threshold:** Defines the percentage of cache space which, when consumed, will trigger warning messages to the system event log.
- **Begin Persistent Image Deletions:** Defines the percentage of cache space which,

when consumed, will trigger automatic deletion of the oldest persistent image on the system. Automatic persistent image deletions are recorded in the system log.

- **Cache Size:** Specifies the amount of space allocated to the cache file. Increasing this value will allow more and larger persistent image to be maintained. Ensure that adequate space is available on the drive where persistent images are stored.
- **Persistent Image Files Location:** Specifies the server appliance volume which will contain the persistent image data. This file contains an exact image of all data file values which have been preserved as part of a persistent image. This should only altered from the default value if the number, type, or capacity of storage disks has been altered.
- **Persistent image directory name:** Specifies the directory name which will be used for the persistent image mount point. Each persistent image appears as a subdirectory of a volume which is being imaged. The entire content of the volume as it existed at the moment the persistent image was created will appear under this directory.

Managing Persistent Storage Manager Schedules

The Persistent Image List displays all current active persistent images (snapshots). Each entry identifies the date and time the persistent images was created, the Read-Only, Read-Write attribute, preservation weight and the volume it preserves.

Working with Persistent Images

Select an individual persistent image by clicking the radio button to the left of the description. After selecting the persistent image click:

- New to create a new persistent image,
- Delete to delete the image from the system,
- Undo Writes to undo changes to a read-write image,
- Properties to view or change the image read-write attribute or retention weight,
- or Context to view the image context within a schedule group.

Creating a New Persistent Image

Persistent images may be created directly through this page or scheduled for later or repeated execution using the Persistent Image Schedules page.

To create a new persistent image

1. From the Menu bar, click Disks and Volumes, then click Persistent Images.
2. From the Task List list on the Images page, click New...

3. Using the pull-down select one or more Volumes to preserve,
4. Select the Read Only or Read/Write attribute,
5. Select the Retention weight,
6. Enter the Persistent image name.
7. Click OK to create the persistent image or Cancel to abort the operation.

Deleting a Persistent Images

To delete a persistent image (snapshot), you must select an item from the Persistent Image List then click the Delete button.

To delete a persistent image

1. From the Menu bar, click Disks and Volumes, then click Persistent Images.
2. On the Persistent Image List page, click the selector next to the persistent image to be deleted.
3. Click OK to delete the persistent image or Cancel to leave it intact.

Undoing Persistent Image Writes

To undo writes to a persistent image (snapshot), you must select an item from the Persistent Image List then click the Undo Writes button.

To undo persistent image writes

1. From the Menu bar, click Disks and Volumes, then click Persistent Images.
2. On the Persistent Image List page, click the selector next to the persistent image to be restored to its original state.
3. Click OK to restore the image or Cancel to leave it intact.

Editing Persistent Image Properties

To change the read only attribute or preservation weight of an image select an image from the Persistent Image List then click Properties in the task list.

To edit persistent image properties

1. From the Menu bar, click Disks and Volumes, then click Persistent Images,
2. From the Task List list, click Properties,
3. Select the Read Only or Read/Write attribute,
4. Select the Retention weight,
5. Click OK to update the persistent image or Cancel to abort the operation.

Context of Persistent Image Groups

Persistent images which are created from a Schedule Item are members of image groups. The members of the group are all the images which were triggered by a particular schedule item. This page displays the various attributes of the group.

Group Page Field Definitions

- **Image Name and Location on Volume:** Displays the name of the image and associated volume list
- **Persistent Image Group Name:** Displays the name associated with this group
- **Number of Images in Group:** Displays the maximum number of images to be included in the group
- **Volume(s) Included in This Image:** Display the drive volumes in the image
- **Image Attributes:** Displays the read only attribute of the image
- **Retention Weight:** Displays the relative retention weight of the image
- **Most Recent Image in Group:** Displays the date and time of the image most recently added for the group
- **Oldest Image in Group:** Displays the chronologically oldest image in the group
- **Next Image in Group to be Deleted:** Displays the date and time of the image which will be deleted next in order to stay within the Number of Images in group limit

Managing Persistent Image Schedules

The Persistent Image Schedule screen displays a list of all scheduled persistent images (snapshots) and associated tasks.

Each scheduled persistent image is identified by the scheduled time, day, frequency, starting date, and group name.

To work with schedule items

1. Select an individual item by clicking the radio button to the left of the description.
2. After selecting the item you may Add, Delete, or edit item Properties.

Adding Persistent Image Schedule Items

To add a schedule item you must supply a starting time, repeat period, starting day, volume, and number of persistent images to keep on-line.

To add a persistent image to the schedule

1. From the Menu bar, click Disks and Volumes, then click Persistent Storage Manager.
2. From the Task List list on the Schedule page, click Add...
3. Select or enter the
 - Starting time,
 - Repeat every frequency,
 - Beginning day,
 - Volume,
 - Read Only attribute,
 - number of images to Keep count, and
 - persistent image name.
4. Click OK to save or Cancel to discard the new item.

Deleting a Persistent Image Schedule

To delete a persistent image schedule select an item from the Schedule List then click the delete task.

To delete a persistent image schedule

1. From the Menu bar, click Disks and Volumes, then click PSM Schedules.
2. On the Schedule page, click the selector next to the item to be deleted.
3. From the Task List on the Schedule page, click Delete.

4. Click OK to delete the item or Cancel to leave the item intact

Editing Persistent Image Schedule Properties

To edit persistent image schedule properties select an item from the Schedule List then click Properties in the task list.

To edit persistent image schedule properties

1. From the Menu bar, click Disks and Volumes, then click PSM Schedules.
2. From the Task List list on the Schedule page, click Properties
3. Select or enter the
 - Starting time,
 - Repeat every frequency,
 - Beginning day,
 - Volume,
 - Read Only attribute,
 - number of images to Keep count,
 - and persistent image name.
4. Click OK to save the changes or Cancel to discard the changes.

Disaster Recovery

The Disaster Recovery screen displays a list of all persistent images (snapshots).

Each scheduled persistent image is identified by the group name, date and time, age, and protected volumes.

Using disaster recovery

1. Select an individual item by clicking the radio button to the left of the description.
2. After selecting the item you may view:
 - Its group Context, or
 - Select it for Restore.

Restoring a Volume Set from a Persistent Image

To restore a volume(s) from a persistent image (snapshot), you must select the image to be restored.

To restore volumes from a persistent image

1. From the Menu bar, click Disks and Volumes, then click Disaster Recovery.
2. On the Disaster Recovery page, click the selector next to the persistent image to be restored.
3. Click OK to restore the volumes protected by the persistent image or Cancel to leave it intact.

Chapter #8 - O/S 2.0 - Folders and Shares

Chapter Outline

- Overview of Supported Protocols
 - Windows CIFS
 - Network File System (NFS)
 - File Transfer Protocol (FTP)
 - Web Hypertext Transfer Protocol (HTTP)
 - Netware Sharing Protocol
 - AppleTalk Protocol
- Managing Folders
 - Sharing Folders
 - Navigating Folders
 - Adding a Folder
 - Removing a Folder
 - Opening a Folder
 - Modifying Folder Properties
 - Sharing a folder
- Managing Shares
 - Overview
 - Adding a Share
 - Removing a Share
 - Modifying Share Properties
 - Setting Windows CIFS Share Properties
 - Setting NFS Share Properties
 - Setting FTP Share Properties
 - Setting Web HTTP Share Properties
 - Setting NetWare Share Properties
 - Setting Apple Talk Share Properties
- Managing Sharing Protocols

- Enabling Sharing Protocols
- Disabling Sharing Protocols
- Configuring Sharing Protocol Properties
- Setting NFS Sharing Protocols
 - Adding NFS client Groups
 - Editing NFS client groups
 - Removing NFS client groups
 - Setting NFS Locks
 - Setting NFS User and Group Mappings
 - Enabling NFS Simple Maps
 - Configuring NFS Explicit User Maps
 - Configuring Explicit Group Maps
 - Setting FTP Sharing Protocol
 - Setting Web HTTP Sharing Protocol
 - Setting Netware Sharing Protocol
 - Setting AppleTalk Sharing Protocol

Overview of Supported Protocols

A folder on your MaxAttach NAS 6000 can be shared with others on the network, whether those computers are running a Microsoft Windows operating system (OS) or a UNIX OS.

Supported Protocols

The MaxAttach NAS 6000 can support the following protocols:

- **Windows (CIFS):** The Common Internet File System (CIFS) protocol is used by clients running a Windows OS.
- **NFS:** The Network File System protocol is used by clients running UNIX.
- **FTP:** The File Transfer Protocol is an alternative way of accessing a file share from any OS.
- **HTTP:** The Hypertext Transfer Protocol is the protocol for accessing a file share from Web browsers.
- **NetWare:** The protocol for accessing a file share from clients running NetWare.
- **AppleTalk:** The protocol for accessing a file share from Macintosh clients.

When you create a share on the MaxAttach NAS 6000, you can enable any or all of the listed protocols currently enabled or installed on your server appliance.

Microsoft Windows File Sharing Overview

When you share a folder, you can choose permissions that will allow or deny other network users access to the files in that folder. For client computers running Microsoft Windows, you can also specify whether other Windows users will be able to make the shared folder available offline.

To make a shared network file available offline, a version of the file is stored in a reserved portion of client computer disk space called a cache. The computer can access this cache regardless of whether the computer is connected to the network. When sharing files, you can use three caching options:

Manual Caching for Documents

Manual caching for documents provides offline access to only those files that someone using your server appliance shared folder specifically, or manually, identifies. This caching option is ideal for a shared server appliance folder containing files that are to be accessed and modified by several people. This is the default option when a shared folder is set up to be used offline.

Automatic Caching for Documents

Automatic caching for documents makes every file in your shared server appliance folder available offline to others who open the files.

Automatic caching makes the contents of a folder available offline whether someone using your shared server appliance folder specifically chooses to make them available or not. Documents, drawings, program files, and other files will all be available to users.

Only those files that someone opens in your shared server appliance folder will continue to be available to that person when working offline.

Automatic Caching for Programs

Automatic caching for programs provides read-only offline access to shared folder files. This caching option is ideal for making files available offline that are referenced, run, or read, but that should not be changed in the process. Automatic caching for programs reduces network traffic because offline files are opened directly, without accessing the network versions in any way, and generally start and run faster than the network versions.

**CAUTION**

When you use automatic caching for programs, be sure to restrict permissions on the shared folder files to read-only access.

Related Topics

- Managing Folders.
- Managing Shares.
- Adding a Share
- Removing a Share
- Modifying Share Properties
- Setting Windows (CIFS) Sharing Properties
- Setting NFS Sharing Properties
- Setting FTP Sharing Properties
- Setting Web Sharing Properties
- Setting NetWare Sharing Properties
- Setting AppleTalk Sharing Properties

Network File System (NFS) Overview

With the NFS protocol, a server appliance can act as a Network File System (NFS) server. Users can then share files in a mixed environment of computers, operating systems, and networks.

Users on computers running NFS client software can access shares on the server appliance by connecting, or mounting, those shares to their computers.

UNIX computers follow advisory locking for all lock requests. This means that the OS does not enforce lock semantics on a file, and applications that check for the existence of locks can use these locks effectively. However, the NFS Protocol implements mandatory locks even for those locking requests that are received through NFS. This ensures that locks acquired through NFS are visible through the Server Message Block (SMB) protocol and to applications accessing the files locally. The OS enforces mandatory locks.

Related Topics

- Adding a Share

- Removing a Share
- Modifying Share Properties
- Setting Windows (CIFS) Sharing Properties
- Setting NFS Sharing Properties
- Setting FTP Sharing Properties
- Setting Web Sharing Properties
- Setting NetWare Sharing Properties
- Setting AppleTalk Sharing Properties

File Transfer Protocol (FTP) Overview

File Transfer Protocol (FTP) is used to copy files between two computers on the Internet. Both computers must support their respective FTP roles: one must be an FTP client and the other an FTP server.

You can configure your server appliance to act as an FTP server. Client computers can then access the server appliance with Windows® Explorer or an FTP command line program, such as ftp.exe, by typing the URL in the address bar in the format ftp://sitename/.

Related Topics

- Adding a Share
- Removing a Share
- Modifying Share Properties
- Setting Windows (CIFS) Sharing Properties
- Setting NFS Sharing Properties
- Setting FTP Sharing Properties
- Setting Web Sharing Properties
- Setting NetWare Sharing Properties
- Setting AppleTalk Sharing Properties

Web Hypertext Transfer Protocol (HTTP) Overview

The HTTP is the Internet protocol used by World Wide Web browsers and servers to exchange information. The protocol defines what actions Web servers and browsers should take in response to various commands, thus making it possible for a user to use a client

program to enter a URL, or choose a hyperlink, and retrieve text, graphics, sound, and other digital information from a Web server. All URLs of files on Web servers begin with http://.

Related Topics

- Adding a Share
- Removing a Share
- Modifying Share Properties
- Setting Windows (CIFS) Sharing Properties
- Setting NFS Sharing Properties
- Setting FTP Sharing Properties
- Setting Web Sharing Properties
- Setting NetWare Sharing Properties
- Setting AppleTalk Sharing Properties

NetWare Sharing Protocol Overview

You can use the NetWare sharing protocol to share volumes on your server appliance powered by Microsoft® Windows® with NetWare clients.

Related Topics

- Setting Windows (CIFS) Sharing Properties
- Setting NFS Sharing Properties
- Setting FTP Sharing Properties
- Setting Web Sharing Properties
- Setting NetWare Sharing Properties
- Setting AppleTalk Sharing Properties

AppleTalk Protocol Overview

Microsoft Windows 2000 Server AppleTalk network integration allows you to share files and printers among your server appliance and any Apple Macintosh clients that are connected to your network.

With AppleTalk network integration, Macintosh computers need only the Macintosh OS software to function as clients; no additional software is required.

AppleTalk network integration simplifies administration by maintaining just one set of user accounts instead of separate user accounts, for example, one on the Macintosh server and another on the computer running Windows 2000 Server.

Related Topics

- Setting Windows (CIFS) Sharing Properties
- Setting NFS Sharing Properties
- Setting FTP Sharing Properties
- Setting Web Sharing Properties
- Setting NetWare Sharing Properties
- Setting AppleTalk Sharing Properties

Managing Folders

The Volumes page allows you to open, or share, a number of network volumes. The page displays an Object/Task Selector that has the following columns:

- **Volume Name:** Lists each volume by name. To create, open, delete, or configure the properties of a given volume, select the check box next to the name of the volume you want to modify.
- **Total Size:** Shows the total size of the volume.
- **Free Space:** Shows the amount of free space available on the volume.
- **Share Type:** Indicates the type of sharing in effect for the folder:
 - W = Windows (CIFS) Sharing
 - U = UNIX (NFS) Sharing
 - F = FTP Sharing
 - H = HTTP Sharing
 - A = AppleTalk Sharing
 - N = NetWare Sharing

The Object/Task Selector lists up to the first 100 folders found. To navigate among the list of folders using the Object/Task Selector, you can search by the fields available in the Search list, and then enter the search criteria in the box to the left of the Go button, or you can scroll through the list. In addition, if there are more than 100 folders, you can view folders in batches of 100 using the Page Up and Page Down buttons to the right of the Go button.

Sharing Folders

To share folders

1. From the Shares page, choose Folders.
2. Select the volume(s) for which you want to share folders, and then choose Share in the Tasks list.
3. Type the information indicated by the prompts. For more information on completing the property page for a particular file sharing method, see the specific Help file for that sharing protocol.

To manage folders

1. From the Shares page, choose Folders.
2. Select the volume(s) for which you want to view or manage folders or shares, and choose Open from the Tasks list.
3. The Folders page allows you to create, open, delete, or configure a number of network folders. The page displays an Object/Task Selector that has the following columns:
 - Folder Name—Lists each folder by name.
 - Date Modified—Shows the date the folder was last modified.
 - Attributes—Shows any of the following folder attributes:
 - R = Read only
 - A = Ready for archiving
 - H = Hidden
 - C = Compressed
 - S = System folder
 - Share Type—Indicates the type of sharing in effect for the folder.
4. Select a folder, and then choose the task you want to perform in the Tasks list.

Navigating Through Folders

You have the following folder navigation options:

- To navigate to the subdirectories of a root folder, select the root folder and then choose Open in the Tasks list.
- To navigate from a subdirectory to its parent, choose Up in the Tasks list.

- If the root folders are already displayed in the Object/Task Selector, there is no parent folder to choose.
- To navigate among folders, use the Object/Task Selector to navigate among folders.
 - For every folder that has subfolders, there will be an Open task in the Tasks list.
 - For every folder that has a parent folder, there will be an Up task in the Tasks list.

To navigate among folders

1. On the primary navigation bar, choose Shares.
2. Choose Folders.
3. Select the volume with which you want to work, and then choose Open.
4. Select the folder you want.
5. In the Tasks list, choose Open.
6. Select the folder you want to navigate within, and then choose Open from the Tasks list.

—OR—

7. In the Tasks list, choose Up to return to the volume's root directory.

Adding a Folder

You can create as many new folders as you need on the server appliance.

To create a new folder

1. On the primary navigation bar, choose Shares.
2. Choose Folders.
3. Select the volume in which you want to work, and then choose Open.
4. Select the folder to which you want to add a subfolder.
5. Choose New in the Tasks list.
6. On the General tab, type the name of the new folder in the Name box.

7. Set the access attributes by selecting the appropriate check box.
8. Optional: If you want to compress the contents of the new folder to save space, select the Compress tab.
9. Choose OK.
10. The Object/Task Selector now includes the folder you added. If your new folder is not immediately apparent in the table, scroll through the list to find it.

Removing a Folder

You can remove any folder(s) you have created on the server appliance.

To delete folders

1. On the primary navigation bar, choose Shares.
2. Choose Folders.
3. Use the Object/Task Selector to navigate to the folder from which you want to remove the subfolder.
4. Select the folder(s) you want to delete.
5. In the Tasks list, choose Delete.
6. Verify the folder indicated is the one you want to remove.
7. Choose OK.

Opening a Folder

To open a folder

1. On the primary navigation bar, choose Shares.
2. Choose Folders.
3. Select the volume in which you want to work, and then choose Open.
4. Select the folder you want to open.
5. In the Task list, choose Open.

Modifying Folder Properties

From the Folder Properties page, you can set or change the folder name, get details about the folder type, size, and location, as well as compress the data in a folder.

To change the name of a folder

1. On the primary navigation bar, choose Shares.
2. From the Shares page, choose Folders.
3. Use the Object/Task Selector to navigate to the directory containing the folder you want to modify.
4. Select the check box for the folder you want.
5. In the Tasks list, choose Properties.
6. Select the General tab, and then type the new folder name in the Name box.
7. Choose OK.

To compress a folder

1. On the primary navigation bar, choose Shares.
2. From the Shares page, choose Folders.
3. Use the Object/Task Selector to navigate to the directory to which you want to add the new folder.
4. In the Tasks list, choose Properties.
5. Select the Compress tab, and then select the Compress contents of this folder to save disk space check box.
6. Select whether to either Apply changes to this folder only, or to Apply changes to this folder, subfolders, and files.
7. Choose OK.

Sharing a Folder

To share a folder

1. On the primary navigation bar, choose Shares.
2. Choose Folders.
3. Select the volume with which you want to work, and then choose Open.
4. Navigate to the directory containing the folder you want to share.
5. Select the folder to share.
6. In the Tasks list, choose Share.
 - If the folder has not already been shared the New Share page will display.
 - If the folder has been shared, the Share Properties page will display.
 - If the folder has been shared under multiple names, select the Manage Share task.

Related Topics

- Adding a Folder
- AppleTalk Sharing
- FTP Sharing
- Modifying Folder Properties
- Navigating Among Folders
- NetWare Sharing
- NFS Sharing
- Opening a Folder
- Removing a Folder
- Sharing a Folder
- Sharing a Folder
- Modifying Folder Properties
- Web (HTTP) Sharing
- Windows (CIFS) Sharing

Managing Shares

The Shares management page allows you to create, open, delete, or configure a variety of file shares. The Shares page displays an Object/Task Selector that has the following columns:

- **Share Name:** Lists each shared folder by name. To create, open, delete, or configure the properties of a given share, select the check box next to the name(s) of the share you want to modify or delete.
- **Share Path:** Displays the share path.
- **Type:** Indicates one of the following share types:
 - W = Windows (CIFS)
 - U = UNIX (NFS)
 - F = FTP
 - H = HTTP
- **Comment:** Displays a brief description of the share, if you have provided one.

Use the Object/Task Selector to select a share, and then choose the task you want to perform from the Tasks list

Adding a Share

To create a share, you must supply a share name that is unique across all shares and the share path. Some protocols also support the inclusion of a comment or brief description of the share. Additionally, you must enable at least one of the available protocols.

While a single user interface is provided to create a share for all protocols, in actuality, a separate share is created for each protocol. You can remove individual sharing protocols from a share, without removing the share itself. However, removing all sharing protocols from a share will delete all versions of the share.

To add a share

1. On the primary navigation bar, choose Shares.
2. On the Shares page, choose Shares.
3. In the Tasks list, choose New.
4. On the General tab, type the share name and share path.
5. Select the appropriate check box(es) to specify which types of protocols you want to enable.

6. Use the protocol tabs to configure the specific properties of each type of share. CIFS Share Properties

Removing a Share

You can remove shares entirely, or you can simply disable a given protocol. The result is that access to the share is removed, yet the actual files remain on the server appliance.

To remove a share and all its protocols

1. On the primary navigation bar, choose **Shares**.
2. On the **Shares** page, choose **Shares**.
3. Select the share you want to remove.
4. In the **Tasks** list, choose **Delete**.
5. Choose **OK**.

To remove specific protocols

1. On the primary navigation bar, choose **Shares**.
2. On the **Shares** page, choose **Shares**.
3. Select the share for which you want to modify properties.
4. In the **Tasks** list, choose **Properties**.
5. Clear the check box(es) for the protocol(s) you want to remove from the share.
6. Choose **OK**.

Modifying Share Properties

Use the **Shares** page to view and modify share properties.

To modify share properties

1. On the primary navigation bar, choose **Shares**.
2. On the **Shares** page, choose **Shares**.

3. Select the share for which the properties will be modified.
4. In the **Tasks** list, choose **Properties**. For instructions about how to set the sharing properties for each protocol, select a link in the **Related Topics** list, below.
5. Choose **OK**.

Setting Windows CIFS Share Properties

Windows client computers use the Common Internet File System (CIFS) protocol to share files. Use this page to change the number of users who have access to a share, change the caching options relative to the share, and set or change user permissions.

In the User Limit section, you may choose to allow the maximum number of users, or you may specify the number of connections that can be made at a given time.

To set the user limit

1. Select the Maximum allowed button to allow as many people to log on to the server appliance as it can handle.

—OR—

1. Select the Allow users button, and then specify the number of users to allow.
2. If you allow files to be cached in the shared folder, use the Setting list to specify the caching option to use. The caching options are described in Windows (CIFS).

To set user or group permissions

You may also set permissions for users or groups who are granted or denied access to the server appliance.

1. In the Add a user or group box, type the name of a user or group to add to the list of permissions, or select a user from the list below it.
2. You can select local users or local groups from the list.
 - To add domain users or domain groups you must type the account as <domain name\user name> or <domain name\group name>.
3. Choose Add.
4. Use the Allow list to set the degree of control the users who are selected in the

Permissions list will have over files on the server appliance.

- Users may have no control, read-only access, change access, change and read access, or full control.
5. Use the Deny list to deny a level of control to the selected users and groups in the Permissions list.
 6. To remove a user or group from the Permissions list, select the user or group in the list, and then choose Remove.
 7. Choose OK.

Setting NFS Share Properties

Use this page to specify which NFS clients are granted access to each share. Access can be granted or denied on the basis of client host name. Access can also be granted or denied on the basis of client groups, where a client group contains one or more client host names.

To add a new NFS client or client group to a share

1. Create a new client group as described in Adding NFS Client Groups.
2. Follow the steps described in the following procedure to add an existing client or client group.

To add an existing NFS client or client group

1. On the primary navigation bar, choose Shares.
2. On the Shares page, choose Shares.
3. Select the share for which you want to add an NFS client or client group.
4. In the Tasks list, choose Properties.
5. Select the General tab.
6. Select the Unix (NFS) check box.
7. Select the NFS Sharing tab.
8. Select the desired machine or group from the list on the left, or type an NFS client computer name or IP address in the box on the right, and then choose Add.
9. Select the degree of control the specified client can exercise over files in the share

from the Type of access list.

10. Choose OK.

To remove an NFS client

1. On the primary navigation bar, choose Shares.
2. On the Shares page, choose Shares.
3. Select the share for which you want to remove an NFS client or client group.
4. In the Tasks list, choose Properties.
5. Select the General tab.
6. Select the Unix (NFS) check box.
7. Select the NFS Sharing tab.
8. Select the desired client appliance or client group from the list in the center of the page, and then choose Remove.
9. Choose OK.

Setting FTP Share Properties

Use this page to specify which FTP clients are granted access to each share. Access can be granted or denied on the basis of client host name.

To allow clients permission to an FTP share

1. On the primary navigation bar, choose Shares.
2. On the Shares page, choose Shares.
3. Select the share for which you want to add FTP client access, and then choose Properties.
4. Select the FTP tab, and then:
 - Select the Read check box to allow read access.

—OR—

 - Select the Write check box to allow write access.

- You may choose to allow read-only, write-only, or read/write permissions.
5. Choose OK.

To log client visits to an FTP share

1. On the primary navigation bar, Choose Shares.
2. On the Shares page, choose Shares.
3. Select the share for which you want to add FTP client access, and then choose Properties.
4. Select the FTP Sharing tab.
5. Select the Log visits check box.
6. Choose OK.

Setting Web HTTP Share Properties

Use this page to specify which HTTP clients are granted access to each share. Access can be granted or denied on the basis of client host name. Access can also be granted or denied on the basis of client groups, where a client group contains one or more client host names.

To allow clients permission to a Web share

1. On the primary navigation bar, choose Shares.
2. On the Shares page, choose Shares.
3. Select the share for which you want to add HTTP client access, and then choose Properties.
4. From the General tab, select the Web (HTTP) check box.
5. Select the HTTP Sharing tab, and then:
 - Select the Read check box to allow read access.

—OR—

 - Select the Write check box to allow write access.

6. Choose OK.

Setting NetWare Share Properties

Use these instructions to specify sharing properties for an existing Novell NetWare Share.



NOTE

If the share does not yet exist, create the share first by following the procedures in Adding A Novell NetWare Share.

To set NetWare sharing properties

1. On the primary navigation bar, choose **Shares**.
2. On the Shares page, choose **Shares**.
3. Select the share for which you want to add NetWare client access, and then choose **Properties** from the Tasks list. The Share Properties of user page appears.
4. Click the **NetWare Sharing** tab. This opens a Terminal Services window.
5. Click **Yes** to clear the warning message.
6. Log into Windows 2000. The Shared Folders dialog box appears.
7. In the Shared Folder pane, locate the share you want to modify.



NOTE

Note that if a share is enabled for more than one protocol, there will be multiple shares with the same name. Be sure to select the share for NetWare as shown in the Type column.

8. Double click the share you want to modify. The *</share name>* Properties dialog box appears.
9. On the **General** tab, set the limit to the number of users.
10. If you want to limit access, select the Share Permissions tab and either remove the **everyone** group or modify its permissions (the default permission levels for **everyone** allows full control of the share). Then add any users or groups for whom you want to grant access.

11. Click **OK** to accept the changes.
12. Exit the Terminal Services session.
13. Click **OK** on the Shared Folders page to complete your changes.

Setting AppleTalk Share Properties

Use these instructions to specify sharing properties for an existing AppleTalk share.



NOTE

Note that if the share does not exist, create the share first by following the procedures in Adding an AppleTalk Share.

Setting AppleTalk Sharing Properties

Use these instructions to specify sharing properties for an existing AppleTalk share.



NOTE

If the share does not yet exist, create the share first by following the procedures in Adding an AppleTalk Share.

1. On the primary navigation bar, choose **Shares**.
2. On the Shares page, choose **Shares**.
3. Check the checkbox of the share for which you want to add AppleTalk client access, and then choose **Properties** from the Tasks list. The Share Properties of *<sharename>* page displays.
4. Click the **AppleTalk Sharing** tab. This opens a Terminal Services window.
5. Click **Yes** to clear the warning message.
6. Log into Windows 2000. The Shared Folders dialog box displays.
7. In the Shared Folder pane, locate the share you want to modify.

**NOTE**

If a share is enabled for more than one protocol, there will be shares with the same name. Be sure to select the share for Macintosh (AppleTalk), as shown in the Type column.

8. Double-click the share you want to modify. The *<sharename>* Properties dialog box displays.
9. On the **General** tab, set the User Limit to specify how many users can access the share at one time.
10. Set the SFM Volume Security **Password** if you want password authentication to limit access to this share.
11. Set the **This volume is read-only** checkbox to prohibit writing to this share.
12. Set or clear the **Guests can use this volume** checkbox to enable or disable guest access to this.

**NOTE**

If you enable the **Guests can use this volume** checkbox, you may also need to enable the Guest user account. If the Guest user account is disabled, there will be no Guest to access your share.

13. To set user and group access rights, select the **Security** tab and either remove the **everyone** group or modify its permissions (the default permission levels for **everyone** allows full access to the share). Then add any users or groups for whom you want to grant access. For detailed Help, use the “?” help button at the top of the dialog box.
14. Click **OK** to accept your changes.
15. Exit the Terminal Services session.
16. Click **OK** on the Shared Folders page to complete your changes.

Related Topics

- Adding a Share
- AppleTalk LAN Connection
- AppleTalk Service Properties
- Modifying Share Properties

- Removing a Share
- Setting AppleTalk Sharing Properties
- Setting FTP Sharing Properties
- Setting NetWare Sharing Properties
- Setting NFS Sharing Properties
- Setting UNIX (NFS) Sharing Properties
- Setting Web Sharing Properties
- Setting Windows (CIFS) Sharing Properties
- Sharing Properties

Managing Sharing Protocols

The **Sharing Protocols** page allows you to enable, disable, stop, or configure relevant network protocols. The **Sharing Protocol** page displays the **Object/Task Selector** with the following columns:

- **Name:** Lists each protocol by name. To enable, disable, or change the properties of a given protocol, select the button next to the protocol you want to modify.
- **Status:** Indicates that the protocol is **Running**, **Stopped**, or **Paused**.
- **Startup Type:** Indicates whether the protocol should start automatically when the server appliance boots, be invoked manually, or be disabled.
- **Description:** Displays a brief description of the protocol.
- **Tasks:** The **Tasks** list is located next to the **Object/Task Selector**. Use the **Name** column of the **Object/Task Selector** to select a protocol. To perform a task, choose the appropriate task from the **Tasks** list.

Enabling Sharing Protocols

Microsoft recommends that you enable only the necessary network protocols. Limiting the number of enabled network protocols will enhance the performance of other network protocols. Additionally, if a problem is encountered with a network or dial-up connection, the system will attempt to establish connectivity by using every network protocol that is installed and enabled. By only enabling the protocols that your system can use, the server appliance can conserve resources and perform better.

To enable a sharing protocol

1. On the primary navigation bar, choose **Shares**.
2. Choose **Sharing Protocols**.

3. Select the protocol you want to enable.
4. In the **Tasks** list, choose **Enable**.

Related Topics

- Configuring Protocol Properties
- Disabling Protocols

Disabling Sharing Protocols

To disable sharing protocols

1. On the primary navigation bar, choose **Shares**.
2. Choose **Sharing Protocols**.
3. Select the protocol you want to disable.
4. In the **Tasks** list, choose **Disable**.

Related Topics

- Configuring Protocol Properties
- Enabling Protocols

Configuring Sharing Protocol Properties

Use the property page of the designated protocol to configure the desired network protocols.

To configure network protocol properties

1. On the primary navigation bar, choose **Shares**.
2. Choose **Sharing Protocols**.
3. Select the protocol you want to configure.
4. In the **Tasks** list, choose **Properties**.

NFS Sharing Protocol

Setting NFS Sharing Protocol

You can use the **NFS Protocol** option to configure the MaxAttach NAS 6000 to act as an NFS server. The **NFS Protocol** allows users to share files in a mixed environment of computers, operating systems, and networks.

You can use the **NFS Protocol** to manage **NFS Client Groups**, **NFS Locking**, and **NFS User and Group mappings**. **NFS Shares**, however, are created from the **Shares** section of the Web UI.

From the **NFS Client Group** page, you can create, delete, or edit NFS client groups.

To configure the NFS protocol

1. On the primary navigation bar, choose **Shares**.
2. Choose **Sharing Protocols**.
3. Select **NFS Protocol**, and then choose **Properties**.
4. Select the NFS configuration task you want.

Adding NFS Client Groups

To add an NFS client group

1. On the primary navigation bar, choose **Shares**.
2. Choose **Sharing Protocols**.
3. Select **NFS Protocol**, and then choose **Properties**.
4. Choose **Client Groups**.
5. In the **Tasks** list, choose **New**.
6. On the **New NFS Client Group** page, type the group name you want to add in the **Group name** box.
7. In the **Client name or IP address** box, type the computer name or IP address you want to add to the group.

8. Choose **Add**.
9. Choose **OK**.

Related Topics

- Editing NFS Client Groups
- Setting AppleTalk Sharing Properties

Editing NFS Client Groups

To add members to an NFS client group

1. On the primary navigation bar, choose **Shares**.
2. Choose **Sharing Protocols**.
3. Select **NFS Protocol**, and then choose **Properties**.
4. Choose **Client Groups**.
5. Select the group you want to edit.
6. In the **Tasks** list, choose **Edit**.
7. On the **Edit NFS Client Group** page, type the IP address or computer name of the member to add to the group.
8. Choose **Add**.
9. Choose **OK**.

To remove members to an NFS client group

1. On the primary navigation bar, choose **Shares**.
2. Choose **Sharing Protocols**.
3. Select **NFS Protocol**, and then choose **Properties**.
4. Choose **Client Groups**.
5. Select the group you want to edit.
6. In the **Tasks** list, choose **Edit**.

7. On the **Edit NFS Client Group** page, select the IP address or computer name of the member to remove from the group.
8. Choose **Remove**.
9. Choose **OK**.

Related Topics

- Adding NFS Client Groups
- Removing NFS Client Groups

Removing NFS Client Groups

To remove an NFS client group

1. On the primary navigation bar, choose **Shares**.
2. Choose **Sharing Protocols**.
3. Select **NFS Protocol**, and then choose **Properties**.
4. Choose **Client Groups**.
5. Select the NFS Client Group(s) you want to remove.
6. In the **Tasks** list, choose **Delete**.
7. On the **Delete NFS Client Group** page, choose **OK**.

Related Topics

- Adding NFS Client Groups
- Editing NFS Client Groups

Setting NFS Locks

NFS locks allow a process to have exclusive access to all or part of a file. File locking is implemented both on the server appliance and the client. When a file is locked, the buffer cache is not used for that file, and each write request is immediately sent to the server.

After a system failure, when the server appliance is restarted, the server appliance attempts to restore the file lock status to the previous condition. If the client fails, the server appliance releases the file lock. However, after the client restarts it has a short period of time to reclaim the file lock.

To manage NFS locks

1. On the primary navigation bar, choose **Shares**.
2. Choose **Sharing Protocols**.
3. Select **NFS Protocol**, and then choose **Properties**.
4. Choose **Locks**.
5. Optional: In the **Current locks** list, select the client whose locks you want to release.
6. Optional: In the **Wait period** box, type the number of seconds after restarting that the server appliance waits to re-establish a file lock with a client.
7. Choose **OK**.

Related Topics

- NFS Client Groups
- Managing NFS Locks
- User and Group Mappings
- Shares

NFS Protocol with User and Group Mappings

Setting NFS User and Group Mappings

To provide security for server appliance files accessed from a UNIX environment, the NFS protocol requires the system administrator to map UNIX user or group accounts to their twin accounts on the server appliance. Users then have equivalent access rights under UNIX as they have under Microsoft Windows. Alternatively, Web sites with less stringent security needs can bypass the mapping procedure and treat all UNIX users as anonymous users.

User And Group Mappings lets you create maps between Windows and UNIX user and group accounts even though the user and group names in both environments may not be identical. Perhaps most important, **User and Group Mappings** lets you maintain a single mapping database for the entire enterprise.

You can use simple maps, which map Windows and UNIX accounts with identical names. You can also create advanced maps to associate Windows and UNIX accounts with different names, which you can use in conjunction with simple maps. Furthermore, with **User and Group Mappings**, you can obtain UNIX user, password, and group information from one or more network information protocol (NIS) servers, or from imported password and group files.

To map NFS users and groups

1. On the primary navigation bar, choose **Shares**.
2. Choose **Sharing Protocols**.
3. Select **NFS Protocol**, and then choose **Properties**.
4. Choose **User and Group Mappings**.

To configure for using an NFS server

1. On the **General** tab, select the **Use NIS server** button.
2. In the **NIS domain** box, type the name of the domain from which the UNIX user and group information is obtained.
3. Optionally: in the **NIS server (optional)** box, type the name of the server you want to map.
4. To specify the length of time the server appliance waits to refresh the user and group information, type the time in the **Hours** and **Minutes** boxes.
5. Choose **OK**.

To configure for using password and group files

1. Select the **Use password and group files** button.
2. In the **Password file** box, type the name of the password file to use.

3. This is a *passwd* format file from a UNIX system containing all the UNIX user accounts that could be mapped.
4. In the **Group file** box, type the name of the group file you want to use.
5. Choose **OK**.

Related Topics

- Enabling Simple Maps
- Configuring Explicit User Maps
- Configuring Explicit Group Maps

Enabling Simple NFS Maps

If enabled, simple maps create automatic mappings between UNIX users and Microsoft Windows users that share the same user name. In a simple user map, users in a Windows domain are implicitly mapped one-to-one to UNIX users on the basis of user name. When the Windows domain and the UNIX *passwd* and group files or NIS domain are identified, the simple maps function maps users who have the same name in the Windows and UNIX or NIS domain. If no match exists for a user name in either place, that user is not mapped.



NOTE

To access this page you must have typed a valid NIS server name on the **General** tab.

To enable simple NFS maps

1. On the primary navigation bar, choose **Shares**.
2. Choose **Sharing Protocols**.
3. Select **NFS Protocol**, and then choose **Properties**.
4. Choose **User and Group Mappings**.
5. Select the **Simple Maps** tab.
6. Select the **Enable simple maps** check box.
7. On the **Windows domain** list, select the server appliance name, or the domain to which the server appliance belongs.

8. If you select the server appliance name, the local users and groups will be mapped.
9. Choose **OK**.

Related Topics

- Related Topics
- Configuring User and Group Mappings
- Configuring Explicit User Maps
- Configuring Explicit Group Maps

Configuring Explicit User NFS Maps

User and Group mapping lets you create inter-platform and cross-platform maps among Microsoft Windows and UNIX user and group accounts, even when the user and group names in both environments are not identical.

User and Group mapping also lets you set up one-to-one inter-platform and cross-platform mappings among Windows and UNIX users and groups. For example, a Windows user name could be mapped to a UNIX user name, or a UNIX group could be mapped to one or more Windows user accounts. Explicit user maps can also be used when the same person has different user names on Windows and UNIX accounts. Using the **Explicit User Maps** option lets you maintain a single mapping database for the entire enterprise.

To create explicit user NFS maps

1. On the primary navigation bar, choose **Shares**.
2. Choose **Sharing Protocols**.
3. Select **NFS Protocol**, and then choose **Properties**.
4. Choose **User and Group Mappings**.
5. Fill out the **General** tab, making sure you have either supplied a NIS Domain or PCNFS *passwd* and group files.



NOTE

For more information on filling out the General tab, see Configuring User and Group Mappings.

6. Select the **Explicit User Mapping** tab.
7. Optionally: Enter the name of the NIS server to map to in the NIS domain field.
8. Choose the **List UNIX Users** button to populate the **Unix users** box.
9. Select a user from each group, and then choose **Add**.

The mapped users will appear in the **Explicitly mapped users** box. If you wish to map to a DOMAIN user, you must enter the DOMAIN\user name, select a UNIX user, and then the add button next to the DOMAIN\user entry box

**NOTE**

You can map users from one Windows domain to more than one UNIX domain, but cannot map a UNIX user to multiple Windows users.

To set one of the NFS mappings as primary for a given user

1. Select the mapping from the **Explicitly mapped users** list.
2. Choose **Set primary**.
3. Choose **OK**.

To delete explicit user maps

1. Follow steps 1–4 in the **To create explicit user maps** procedure to navigate to the **Explicit User Maps** page.
2. In the **Explicitly mapped users** list, select the user mapping you want to delete.
3. Choose **Remove**.
4. Choose **OK**.

Related Topics

- Configuring User and Group Mappings
- Enabling Simple Maps
- Configuring Explicit Group Maps

Configuring Explicit Group Maps

User and Group mapping lets you create inter-platform and cross-platform maps among Microsoft Windows and UNIX user and group accounts even when the user and group names in both environments are not identical.

User and Group mapping also lets you set up one-to-one mappings between Windows users and UNIX users and groups. For example, a Windows user name could be mapped to a UNIX user name, or a UNIX group could be mapped to one or more Windows user accounts. Explicit maps can also be used when the same person has different user names on Windows and UNIX accounts. Using the **Explicit Group Maps** option lets you maintain a single mapping database for the entire enterprise.

To create explicit group maps

1. On the primary navigation bar, choose **Shares**.
2. Choose **Sharing Protocols**.
3. Select **NFS Protocol**, and then choose **Properties**.
4. Choose **User and Group Mappings**.
5. Fill out the **General** tab, making sure you have either supplied a NIS Domain or PCNFS *passwd* and group files.
 - For more information on filling out the General tab, see Configuring User and Group Mappings.
6. Select the **Explicit Group Maps** tab.
7. Optionally: Enter the name of the NIS server to map to in the NIS domain field.
8. To populate the **UNIX groups** list, choose the **List UNIX Groups** button.
9. Select a group from each group, and then choose **Add**.
10. The mapped groups will appear in the **Explicitly mapped groups** box. If you wish to map to a DOMAIN group, you must enter the DOMAIN\group name, select a UNIX group, and then the add button next to the DOMAIN\group entry box



NOTE

You can map groups from one Windows domain to more than one UNIX domain, but not the reverse.

To set one of the mappings as the primary maps for a given group

1. Select the mapping from the **Explicitly mapped groups** list.
2. Choose **Set Primary**.
3. Choose **OK**.

To delete explicit group maps

1. Follow steps 1–4 from the **To create explicit group maps** procedure to navigate to the **Explicit Group Maps** page.
2. In the **Explicitly mapped groups** list, select the group mapping you want to delete.
3. Choose **Remove**.
4. Choose **OK**.

Related Topics

- Configuring User and Group Mappings
- Enabling Simple Maps
- Configuring Explicit User Maps

FTP Sharing Protocol

Setting FTP Sharing Protocol

File Transfer Protocol (FTP) is used to copy files between two computers on the Internet. Both computers must support their respective FTP roles: one must be an FTP client and the other an FTP server.

You can configure your server appliance to act as an FTP server. Client computers can then access the server appliance with Windows® Explorer or an FTP command line program, such as ftp.exe, by typing the URL in the address bar in the format *ftp://sitename/*.

The File Transfer Protocol (FTP) is integrated with the Windows security model. Users connecting using FTP are authenticated based on the user accounts on the Windows Powered server appliance. They receive access based on those user profiles. Keep in mind,

however, that the FTP server relies on the ability to send user passwords over the network without data encryption. As a result, a user with physical access to the network could examine user passwords during the FTP validation process.

FTP supports all Microsoft Windows FTP client commands, when a server appliance is running FTP, other computers using the FTP utility can connect to the server and transfer files. On the other hand, non-Microsoft versions of FTP clients might contain commands that are not supported by the FTP server protocol.

Enabling FTP Logging

You can log incoming FTP connections to the FTP log by enabling **FTP Logging**. By default, FTP logs are stored by in %windir%\system32\logfiles\msftpsvc1.

Administrators can access these files from their workstation by either accessing an administrative share—for example, \\appliance\name\admin\$\winnt\system32—or by creating a new share for this folder.

To enable FTP logging

1. On the primary navigation bar, choose **Shares**.
2. Choose **Sharing Protocols**.
3. Select **FTP Protocol**, and then choose **Properties**.
4. Select the **Logging** tab.
5. Select the **Enable logging** check box, and then choose **OK**.

Related Topics

- For more information about FTP anonymous access, see FTP Anonymous Access. For more information about adding FTP messages, see Adding

Enabling FTP Anonymous Access

To enable FTP Anonymous

1. On the primary navigation bar, choose **Shares**.
2. Choose **Sharing Protocols**.

3. Select **FTP Protocol**, and then choose **Properties**.
4. Select the **Anonymous Access** tab.
5. Select the **Enable Anonymous Access** check box, and then choose **OK**.

Disabling FTP Anonymous Access

To disable FTP anonymous

1. On the primary navigation bar, choose **Shares**.
2. Choose **Sharing Protocols**.
3. Select **FTP Protocol**, and then choose **Properties**.
4. Select the **Anonymous Access** tab.
5. Clear the **Enable Anonymous Access** check box, and then choose **OK**.

Adding Custom FTP Messages

You can create customized welcome and exit messages that are sent to users when they connect or disconnect from the server appliance.

To add custom messages

1. On the primary navigation bar, choose **Shares**.
2. Choose **Sharing Protocols**.
3. Select **FTP Protocol**, and then choose **Properties**.
4. Select the **Messages** tab.
5. In the **Welcome message** box, type the message that will greet users when they connect to the server appliance.
6. In the **Exit message** box, type the message that will appear when users disconnect from the server appliance.
7. Choose **OK**.

Related Topics

- FTP Anonymous Access
- Adding a Share
- Removing a Share
- Modifying Share Properties
- Setting Windows (CIFS) Sharing Properties
- Setting NFS Sharing Properties
- Setting FTP Sharing Properties
- Setting Web Sharing Properties
- Setting NetWare Sharing Properties
- Setting AppleTalk Sharing Properties

Web HTTP Sharing Protocol

Setting Web HTTP Sharing Protocol

The HTTP is the Internet protocol used by World Wide Web browsers and servers to exchange information. The protocol defines what actions Web servers and browsers should take in response to various commands, thus making it possible for a user to use a client program to enter a URL, or choose a hyperlink, and retrieve text, graphics, sound, and other digital information from a Web server. All URLs of files on Web servers begin with *http://*.

The hypertext transfer protocol (HTTP) is a communications protocol designed to transfer hypertext documents between computers over the Web. HTTP defines what actions Web servers and browsers should take in response to various commands.

The commands used by the Web are defined in HTTP.

To specify the location of a resource, HTTP uses Uniform Resource Locators (URLs). URLs follow a naming convention that uniquely identifies the location of a computer, directory, or file on the Internet. The URL also specifies the Internet protocol—FTP, HTTP, for example—needed to retrieve the resource. If you know the URL of a resource, you can provide the URL, or you can link to it from a document you want to make available to Web users.

The HTTP protocol supports anonymous access, as well as basic and Windows authentication.

To configure Web (HTTP) sharing properties

1. On the primary navigation bar, choose **Shares**.
2. Choose **Sharing Protocols**.
3. Select **HTTP Protocol**, and then choose **Properties**.
4. Choose to allow all IP address to access data shares on the server appliance, or select a single IP address from the list.
5. Type the port number that can be used to access data shares on the appliance. The default port number is 80.

Related Topics

- For more information about HTTP, see Web (HTTP).
For more information about HTTP share properties, see Web (HTTP) Sharing.
- Adding a Share
- Removing a Share
- Modifying Share Properties
- Setting Windows (CIFS) Sharing Properties
- Setting NFS Sharing Properties
- Setting FTP Sharing Properties
- Setting Web Sharing Properties
- Setting NetWare Sharing Properties
- Setting AppleTalk Sharing Properties

NetWare Sharing Protocol

Setting NetWare Sharing Protocol

You can use the NetWare sharing protocol to share volumes on your server appliance powered by Microsoft® Windows® with NetWare clients.

Related Topics

- Setting Windows (CIFS) Sharing Properties
- Setting NFS Sharing Properties

- Setting FTP Sharing Properties
- Setting Web Sharing Properties
- Setting NetWare Sharing Properties
- Setting AppleTalk Sharing Properties

AppleTalk Sharing Protocol

Setting AppleTalk Sharing Protocol

Microsoft Windows 2000 Server AppleTalk network integration allows you to share files and printers among your server appliance and any Apple Macintosh clients that are connected to your network.

With AppleTalk network integration, Macintosh computers need only the Macintosh OS software to function as clients; no additional software is required.

AppleTalk network integration simplifies administration by maintaining just one set of user accounts instead of separate user accounts, for example, one on the Macintosh server and another on the computer running Windows 2000 Server.

Related Topics

- Enabling Protocols
- Setting NFS Sharing Properties
- Setting FTP Sharing Properties
- Setting NetWare Sharing Properties
- Setting AppleTalk Sharing Properties

Chapter #9 - O/S 2.0 - Users and Groups

Chapter Outline

- Manage Local Users
 - Adding a User Account
 - Enabling the Guest Account
 - Removing a User Account
 - Setting a User Password
 - Modifying User Properties
- Manage Local Groups
 - Adding a Group Account
 - Removing a Group Account
 - Modifying Group Properties

Users and Groups

From this page you can create, edit, and delete local users and groups on the server appliance. You can also change the members of each group. If the server appliance is a member of a domain, you will not want to create any users on the server appliance itself. The primary purpose of this page is to add one or more domain members to the local group.

You may also want to use domain user and group accounts to control access to resources on the server appliance. You may also want to use domain management tools to manage domain users and domain groups.

Related Topics

- Manage Local Users
- Manage Local Groups

Manage Local Users

A local user or group account is an account that exists on the server appliance itself and grants users or groups access to its resources. The server appliance can also be configured to grant access to domain users and groups. Domain users and groups are those that exist in a Microsoft® Windows NT® 4 or Microsoft® Active Directory™ domain. You can add local users, domain users, and domain groups to local groups.

Users and groups are important in Microsoft Windows® Powered security because you can assign permissions to limit the ability of users and groups to perform certain actions. A permission is a rule associated with an object, usually a file, folder, or share, that regulates which users, and in what manner those users can access the object. Any local or domain user who is a member of the local administrator group on the server appliance has administrative privileges on the server appliance. Likewise, any user who is a member of a group that has been assigned to the administrator group on the local computer has administrative privileges for that computer. For example, you could assign the TeamLeads groups, consisting of Tom, Mary, Hazel, and Jim to the administrative group on the server appliance. Each of the TeamLeads group members would then have administrative privileges on the server appliance.

Related Topics

- Adding a User Account
- Removing a User Account
- Setting a User Password
- Modifying User Properties

Adding a User Account

When you add a user account, you should include a user name, the user's full name, a brief description of the account, and an account password.

Keep in mind that user names must be unique, and must not duplicate the name of any existing group.

Other limitations exist on user names:

- A user name cannot be identical to any other user or group name on the computer being administered.
- A user name can contain up to 20 uppercase or lowercase characters except for the following: " / \ [] : ; | = , + ? < > .
- Additionally, a user name cannot consist solely of periods (.) or spaces.

In the Password and Confirm password boxes, you can type a password containing up to 127 characters.

**NOTE**

If you are using Microsoft® Windows® 2000 on a network that also has computers using Microsoft Windows 95 or Microsoft Windows 98, consider using passwords that contain fewer than 14 characters. Windows 95 and Windows 98 support passwords that contain up to 14 characters. If your password is longer, you may not be able to log on to your network from those computers.

The only new users you should add to the administrators group are those that will be solely performing administrative tasks.

To add a user account

1. From the primary navigation bar, choose Users.
2. From the Users page, choose Local Users.
3. In the Tasks list, choose New.
4. Type the information for the new user account.
5. The Home Directory field specifies a new directory which will be created, and to which the user will have exclusive access permission. The directory name is the same as user name defined above, and will be located in the path specified.
6. Choose OK.

Related Topics

- Removing a User Account
- Setting a User Password
- Modifying User Properties

Enabling the Guest Account

By default, the guest account is disabled. For workgroups that have Windows 95 and Windows 98 client computers, enabling the guest account is the quickest way to provide access to resources on a server appliance. By enabling the guest account, however, any user connected to the network will have access to resources on the appliance. An alternative is to create a user account for every user on the network.

To enable the guest account

1. On the primary navigation bar, choose Users.
2. Choose Local Users.
3. In the Name column, select Guest.
4. In the Tasks list, choose Properties.
5. On the General tab, clear the Disable this user account check box.
6. Choose OK.

Removing a User Account

With the exception of the last remaining account and your personal account, you can remove all user accounts that you have created on the Microsoft Windows Powered appliance. In addition, you can remove multiple user accounts at once. However, if you remove the only user account on the server appliance, security is disabled.

When removing user accounts, keep the following guidelines in mind:

- Built-in users cannot be deleted.
- A deleted user cannot be recovered.

If you delete a user account and then create another user account with the same user name, you must set new permissions for the new user; the new user will not inherit the permissions that were granted to the old user.

To remove user accounts

1. On the primary navigation bar, choose Users.
2. Choose Local Users.
3. Select the user account(s) you want to remove.
4. In the Tasks list, choose Delete.
5. Verify you want to delete the indicated user account(s), and then choose OK.

Related Topics

- Adding a User Account

- Setting a User Password
- Modifying User Properties

Setting a User Password

This allows you to change the user's password for their account, usually in cases where they have lost or forgotten it.

To set the user password

1. From the primary navigation bar, choose Users.
2. Choose Local Users.
3. Select the user account for which you want to change the password.
4. In the Tasks List, choose Set a Password.
5. Type the new password, and then confirm it in the boxes provided.
6. The new password must conform to any password complexity rules in effect for the domain to which the server appliance belongs.
7. Choose OK.

Related Topics

- Adding a User Account
- Removing a User Account
- Modifying User Properties

Modifying User Properties

User properties include the user name, full name, and description. From the user's Properties page, you can also enable or disable a user account. Furthermore, you can also change the properties of several user accounts at once by selecting all the accounts you wish to modify before opening the Properties page.

To access user properties

1. On the primary navigation bar, choose Users.
2. Choose Local Users.

3. Select the user account(s) you want to modify.
4. In the Tasks list, choose Properties.
5. Change the user properties you want.
 - The Home Directory field specifies a new directory which will be created, and to which the user will have exclusive access permission.
 - The directory name is the same as user name defined above, and will be located in the path specified.
6. Choose OK.

Related Topics

- Adding a User Account
- Removing a User Account
- Setting a User Password

Manage Local Groups

A local user or group account is an account that exists on the server appliance itself and grants users or groups access to its resources. The server appliance can also be configured to grant access to domain users and groups. Domain users and groups are those that exist in a Microsoft® Windows NT® 4 or Microsoft® Active Directory™ domain. You can add local users, domain users, and domain groups to local groups.

Users and groups are important in Microsoft Windows Powered security because you can limit the ability of users and groups to perform certain actions by assigning them permissions. A permission is a rule associated with an object, usually a file, folder, or share, that regulates which users can access the object and in what manner. Any local or domain user who is a member of the local administrator group on the server appliance has administrative privileges for the server appliance.

Likewise, any member of a group that has been assigned to the administrator group on the local computer has administrative privileges for that computer.

For example, you could assign the TeamLeads group, consisting of Tom, Mary, Hazel, and Jim to the administrative group on the server appliance. Each of these TeamLeads group members would then have administrative privileges on the server appliance.

Related Topics

- Adding a Group Account
- Removing a Group Account
- Modifying Group Properties

Adding a Group Account

To add a group account

1. On the primary navigation bar, choose Users.
2. Choose Local Groups.
3. In the Tasks list, choose New.
4. On the General tab, type the name and description of the group you want to add.
5. On the Members tab:

- To add members to the group, select a user or group to add from the Add user or group box, and then choose Add.

**NOTE**

Note Only local users are displayed in the list. To enter a domain user account, type the domain and user name (<domain\user name>)

- To remove members from the group, select a member or group from the Members box, and then choose Remove.

6. Choose OK.

Related Topics

- Removing a Group Account.
- Modifying Group Properties.

Removing a Group Account

You can remove any group account that you have created. A group account that has been removed, however, cannot be re-created. Notably, you can remove several group accounts at once by selecting all the group account prior to launching the Delete task.

To remove a user account

1. From the primary navigation bar, choose Users.
2. Choose Local Groups.
3. Select the group account(s) you wish to remove.
4. In the Tasks list, choose Delete.
5. Verify that the group identified is the group account you want to delete, and then choose OK.

Related Topics

- For more information about adding a group account, see Adding a Group Account.

- For more information about modifying group properties, see Modifying Group Properties.

Modifying Group Properties

The Group Properties page displays the General tab and the Members tab. Use the General tab to set or modify the group name and description. Use the Members tab to add or remove users and groups.

To set or modify a group name or description

1. On the primary navigation bar, choose Users.
2. Choose Local Groups.
3. Select the group account you want to modify.
4. In the Tasks list, Choose Properties.
5. On the General tab, type a name and description of the desired group.
6. Choose OK.

To set or modify group membership

1. On the primary navigation bar, choose Users.
2. Choose Local Groups.
3. Select the group account you want to modify.
4. In the Task list, choose Properties, and then select the Members tab.

To add a new member:

1. In the Add user or group box, select a local user or group from the list, and then
2. Choose the Add button.

—OR—

1. Type the domain and group name (<domain\group name>) of a domain group, or a domain user account (<domain\user name>) and then

2. Choose Add.

**NOTE**

If you are adding Domain\Group, however, you must also enter credentials that will allow for the addition from that domain.

To remove a member

1. Select a user name from the Members list, and then
2. Choose Remove.
3. Choose OK.

Related Topics

- Adding a Group Account.
- Removing a Group Account.

Chapter #10 - O/S 2.0 - Maintenance

Chapter Outline

- Updating software
- Setting date and time
- Shutdown
- Logs
 - Managing application logs
 - Managing FTP logs
 - Managing NFS logs
 - System log
 - Security log
 - Managing Web HTTP shares logs
 - Managing web administration logs
 - Clear log files
 - downloading log files
 - Modifying log properties
 - View log entry details
- Backup
- Terminal services
- Alert email
- Language
- Add/remove programs
- Computer management
- System recovery option
- Session timeout
- Re-image system drive

Software Update

Use this page to apply software updates to your server appliance.

To update the software

1. From the primary navigation bar, choose Maintenance.
2. Choose Software Update.
3. Follow the Software Update Wizard prompts

Setting Date and Time

Using the Date/Time page, you can set the date, time, and time zone used by the server appliance.

To set the date, time, and time zone

1. On the primary navigation bar, choose Maintenance.
2. Choose Date/Time.
3. Type the date and time in the format defined by the default language selected in your browser.
4. Select the appropriate time zone from the list.
5. You can also automatically adjust the server appliance for daylight saving changes, which is recommended.
6. Choose OK.

Shutting Down the System

Use this page to shut down, restart, or to schedule a shutdown or restart of the server appliance.

To shut down or restart the system

1. On the primary navigation bar, choose Maintenance.
2. Choose Shutdown.
3. Choose the task you want to perform.
4. Choose OK to confirm your decision.
5. If you have chosen to restart the server appliance, the Restarting page will display.

**NOTE**

The Restarting page checks periodically to determine whether the appliance is back online. If the Restarting page detects that the appliance is online, it automatically returns to the default page.

To schedule a shutdown or restart

1. From the primary navigation bar, choose Maintenance.
2. Choose Shutdown.
3. Choose Scheduled Shutdown.
4. Choose the scheduled shutdown settings you want.
5. Choose OK.

**NOTE**

To cancel a currently-scheduled event, select the No scheduled shutdown or restart button.

Add or Remove Programs

The MaxAttach provides Web user interface access to the Windows 2000 Add/Remove Programs applet in the Control Panel. You can use this applet to install or remove a program or driver.

**NOTE**

Do not remove or change any system software that was provided with the server by Maxtor unless directed to do so by Maxtor Customer Support.

To remove a program

1. Using Internet Explorer, log in to the MaxAttach NAS 6000 as administrator.
2. Click Maintenance.
3. Select Add/Remove Programs. This opens a terminal services session.
4. Log in to Windows 2000. The Add/Remove Programs dialog box displays.
5. Select the program you want to remove from the list. Note: do not remove system programs provided by Maxtor unless directed to do so by Maxtor Customer Support.
6. Click the Change/Remove button for the chosen program.
7. The Add/Remove applet removes the program. Follow the on screen instructions to complete your task.

To add a program or driver

1. From Internet Explorer, log in to your MaxAttach NAS 6000 as administrator.
2. Create a share on a convenient drive. This share will hold your new software (when creating the share, check to see if there is enough disk space to hold the contents of the new software). For convenience, you can map this share to a drive on your client machine.
3. On your client machine, insert the new program's CD or floppy into the appropriate drive.
4. Copy the contents of the CD or floppy to the share you created on the MaxAttach.
5. Using Internet Explorer, log in to the MaxAttach as administrator.
6. Click Maintenance on the main menu bar.
7. Select Terminal Services. This starts a terminal services session.
8. Log in to Windows 2000.

9. Navigate to the share that has the new software.
10. Run the new program's Setup (or do whatever is required to install the new program).
11. When the installation program is finished, you can remove the share that you created, as it is no longer needed.

Automatic System Backup Schedule

By default, automatic system backup is scheduled for once each week, beginning at 2:00 AM on Saturdays. The backup copy can be used to recover from a boot failover. To change this schedule or to disable automatic system backup, see Automatic System Backup Schedule.

Changing the Automatic Backup Schedule

To change the automatic backup schedule

1. Log in to the Maxtor MaxAttach NAS 6000 as administrator.
2. Click Maintenance on the main menu bar.
3. Select Terminal Services. A terminal services session starts.
4. Log in to Windows 2000.
5. On the Windows Start menu, select Settings > Control Panel. The control panel displays.
6. Double-click the Scheduled Tasks icon. This opens the scheduler.
7. Right-click BackupMaxAttach6000.bat and select Properties.
8. On the Schedule tab, enter the new schedule parameters
9. Click OK.

Disabling the Automatic Backup Schedule

To disable the automatic backup schedule

1. Log in to the MaxAttach NAS 6000 as administrator.

2. Click Maintenance on the main menu bar.
3. Select Terminal Services. A terminal services session starts.
4. Log in to Windows 2000.
5. On the Windows Start menu, select Settings > Control Panel. The control panel displays.
6. Double-click the Scheduled Tasks icon. This opens the scheduler.
7. Right-click BackupMaxAttach6000.bat and select Properties.
8. On the Schedule tab, clear the Enabled (scheduled task runs at specified time) checkbox.
9. Click OK.

Manual Back Up

You can back up the MaxAttach NAS 6000 system before its scheduled time, for example, if you are about to make changes to the system and want to make a backup before you begin.

To immediately back up the system

1. Log in to the MaxAttach NAS 6000 as administrator.
2. Click Maintenance on the main menu bar.
3. Select Terminal Services. A terminal services session starts.
4. Log in to Windows 2000.
5. On the Windows Start menu, select Run.
6. Type the following in the Run field: D:\backupmaxattach6000. The backup program runs, displaying various dialog boxes and messages. No user intervention is required.
7. When the program completes, exit from terminal services.

Re-Image System Drive

The Re-Image System Drive page lets you copy a backup image of the operating system to the boot drive, restoring the operating system and other system software to an earlier state.



WARNING

Using this feature will overwrite the current operating system and will erase all current configuration information. Use this feature with care!

In the Select an image to write to the system (boot) drive section, select an option by clicking its radio button:

- Original factory-shipped image – select this option to restore the system software from a copy of the original system that was shipped from the factory. Note that all changes made since the system was first put into service will be lost.
- Most recently saved system image – select this option to restore the system software from its most recent backup copy. In the default configuration, the backup copy of the system on drive D: is automatically refreshed from the C: drive once per week. Note that this copy may be up to one week old and may not reflect recent changes.
- Click OK to write the selected image to the system (boot) drive.

Set Session Timeout

The session timeout feature is designed to prevent unauthorized access to the server if the administrator leaves his or her computer unattended while logged on to the MaxAttach. When the timeout interval expires, the user is automatically logged out.



NOTE

This feature requires Internet Explorer 5.5 or later on the client computer.

You can set the timeout interval to a longer interval to prevent unwanted time-outs while you are performing server maintenance or configuration, or a shorter interval to improve security.

Maxtor recommends that you keep the interval as short as practical to enhance system security. If you set a long time interval temporarily, remember to return it to a low value to restore its protective function. The default timeout is 10 minutes.

To set the session timeout interval

1. Using Internet Explorer, log in to the MaxAttach as administrator.
2. Click Maintenance.
3. Select Session Timeout. This opens the Session Timeout page.
4. In the Session Timeout Interval field, type the number of minutes you want to the system to wait before it automatically logs out. The timeout range is from 1 minute to 1440 minutes (one day). If you want to deactivate the timer, enter 0.
5. Click OK.

Setting Alert E-Mail

Your server appliance can be configured to generate an automatic e-mail notification when an alert is raised. You can choose to be notified when any type of alert is raised or only for specific alert types, such as informational, warning, or critical alerts.

This feature uses the SMTP service in the server appliance to send e-mail. In a normal Internet environment, you do not need to configure an SMTP gateway. However, to send e-mail to Microsoft® Exchange Server or Lotus Notes, you need to provide the name of the specific SMTP gateway. You must put the SMTP gateway server name, or IP address, in the SMTP server field in the Web user interface (UI). Contact your Microsoft Exchange administrator for the server name of the SMTP gateway.

To set the alert e-mail feature

1. From the primary navigation bar, choose Maintenance.
 2. Choose Alert E-Mail.
 3. Select the Disable sending alert e-mail button.
- OR -
1. Select the Enable sending alert e-mail button, and then select the check boxes for the circumstances under which you want alert e-mail to be sent.
 2. In the To box, type the system administrator's e-mail address.

- You may have alert e-mail sent to multiple addresses, simply type the addresses into the To box, separated by a comma.
3. In the With box, type the SMTP gateway name or IP address of the SMTP server.
 4. To test the settings, choose Test.
 - After clicking the Test button, test e-mail will be sent.
 - If the SMTP service is not installed on your computer, or there is no network cable, you will receive the error message “Test e-mail cannot be sent out.”
 - If you do not receive the test e-mail at all, even though the message “Test e-mail has been sent out. Please check administrator’s mailbox” has been displayed in the Web UI, the error has most likely been caused by the SMTP server.
 - To clear this error, reset the SMTP server name.
 5. Choose OK.

Backing up and Restoring the O/S

From this page you can choose to back up or restore the operating system (O/S).

To back up or restore the OS

1. On the primary navigation bar, choose Maintenance.
2. Choose Backup.
3. Logon to Terminal Services Advanced Client. The backup application will start automatically.
4. When you are finished, close the application by clicking the X in the upper right hand corner. This will log you off from the Terminal Services Advanced Client.



NOTE

It may take a few moments for the session to log off when closing the application.

Terminal Services Client

Terminal Services Client is the tool used to back up and restore the server appliance operating system. It supports only two concurrent connections. Additionally, if you navigate to another page during an open session, the client will be disconnected but the session will be preserved. This can prevent other users from accessing a Terminal Services session.

With the 32-bit Terminal Services Client you can access a server running Terminal Services and do any of the following:

- Connect to Terminal Services.
- Check the Terminal Services Client number.
- Use short cut keys
- Cut and paste from the Terminal Services Client window into an application running locally.
- Print to your local printer from applications running on the Terminal server.
- Cut and paste from the Terminal Services Client window into an application running locally.
- Print to your local printer from applications running on the Terminal server.
- Disconnect without ending a session.
- Disconnect and end a session.



NOTE

Once connected to Terminal Services, additional help is available on the server. Click Start and then click Help. In the table of contents, click Client Services and then click Terminal Services.

To connect to Terminal Services

1. Click Start, point to Programs, point to Terminal Services Client, and click Terminal Services Client.
2. In Server, type a Terminal server name or TCP\IP address or select a server from the list of Available servers.
3. In Screen area, select the screen resolution for the Terminal server window.
4. If you are connecting using a modem or a slow network, click Use data compression.
5. If you would like to have commonly used bitmaps stored on your local hard drive,

select Cache bitmaps to disk.

6. Click Connect.
7. The Log On to Windows dialog box will appear within the Terminal Services Client window.
8. Type your user name, password, and domain (if required).



NOTE

If you previously disconnected from a Terminal server without ending the session, the Terminal Services Client reconnects to that session (if the connection is configured for the re-connection of disconnected sessions).

To check the Terminal Services Client version

1. Click Start, point to Programs, point to Terminal Services Client, and click Terminal Services Client.
2. Click About.

To use shortcut keys

The following shortcut keys are available from a Terminal Services Client:

- **CTRL+ALT+END:** Opens the Windows Security dialog box.
- **ALT+PAGE UP:** Switches between programs from left to right.
- **ALT+PAGE DOWN:** Switches between programs from right to left.
- **ALT+INSERT:** Cycles through the programs in the order they were started.
- **ALT+HOME:** Displays the Start menu.
- **CTRL+ALT+BREAK:** Switches the client between a window (if applicable) and a full screen.
- **ALT+DELETE:** Displays the window's pop-up menu.
- **CTRL+ALT+Minus (-):** The minus symbol on the numeric keypad places a snapshot of the active window, within the client, on the Terminal server clipboard (provides the same functionality as pressing ALT+PrintScrn on a local computer.)
- **CTRL+ALT+Plus (+):** The plus symbol on the numeric keypad places a snapshot of the entire client window area on the Terminal server clipboard (provides the same functionality as pressing PrintScrn on a local computer.)

Using the Clipboard During Terminal Server Sessions

Using Terminal Services provides seamless clipboard sharing, making clipboard contents available to applications locally on a user computer and within a Terminal Services session.

The shared clipboard synchronizes its contents with the local clipboard and can be viewed using the Windows Clipbook Viewer (clipbrd.exe). You can copy and paste text or graphics from a document within the client window, and paste it into a document on your local machine. You cannot, however, copy and paste files and folders.

When you cut or copy information from an application, it is moved to the Clipboard and remains there until you clear the Clipboard or until you cut or copy another piece of information. The Clipboard window in ClipBook Viewer shows the contents of the Clipboard. You can paste the information from the Clipboard into any document as often as you like. However, the information is only stored on the Clipboard temporarily.

Local Printing During Terminal Server Sessions

Terminal Services provides printer redirection which routes printing jobs from the Terminal server to a printer attached to your local computer. There are 2 ways to provide access to local printers: automatic and manual printer redirection. Use manual redirection when your local printer requires a driver that is not available on Windows 2000 Server.

Automatic Printer Redirection

Printer redirection is automatic when the local printer uses a driver that is installed on the Windows 2000 server. When you log on to a session on the Terminal server, any local printers attached to LPT, COM and USB ports that are installed on the client computer are automatically detected and a local queue is created on the server. The client computer printer settings for the default printer and some properties (such as printing on both sides of the page) are used by the server.

When a client disconnects or ends the session, the printer queue is deleted and any incomplete or pending print jobs are lost. Information about the clients local printers and settings are saved on the client computer. On subsequent logons, the printer queue is created using the information stored on the client computer.

If a printer driver is not found on the server, an event is logged and the client printer is not created. To make the printer available, the driver must be manually installed on the server.

Manual Printer Redirection

Printers attached to LPT and COM ports on the clients local computer can be manually redirected, although manual redirection of printers connected through USB ports is not supported.

To manually redirect a client printer, contact your administrator and provide the name of your computer (or IP address for a Windows-based Terminal). The client must be connected to the Terminal server during manual redirection.

After the initial manual redirection, printers will be automatically redirected during subsequent logons.



NOTE

Redirected printers are available for use with applications running on the server. Redirected printers appear in the Printers folder in Control Panel and are named in this format: Client Printer Name/Client Computer Name/Session Number.



NOTE

When you disconnect or log off from a session, the printer queue is deleted and incomplete or pending print jobs are lost.

To Close the Client

You have the option of disconnecting with or without ending the session.

Disconnecting without ending the session reconnects to this session the next time you connect to this Terminal server (if the connection is configured for the re-connection of disconnected sessions). Logging off ends the session and the next time you log on, a new session will be started.

To disconnect without ending a session

1. In the Terminal Services Client window, click Start and then click Shut Down.
 - The Shut Down Windows dialog box appears.
 - The dialog box asks you “What do you want the computer to do?”
2. Select Disconnect.

**NOTE**

The Terminal Services Client reconnects to this session the next time you connect to this server (if the connection is configured for the re-connection of disconnected sessions).

To log off and end a session

1. In the Terminal Services Client window, click Start and then click Shut Down.
 - The Shut Down Windows dialog box appears.
 - The dialog box asks you “What do you want the computer to do?”
2. Select Log Off.

Logs

A log file is a file that stores messages, or event logs generated by an application, service, or Microsoft® Windows®. These messages are used to track the operations performed in the server appliance.

You can use the Logs feature to view, clear, download, and configure the following types of event logs provided by the system:

- Managing Application Logs
- Managing FTP Logs
- Managing NFS Logs
- Managing Security Logs
- Managing System Logs
- Managing Web (HTTP) Shares Logs
- Managing Web Administration Logs
- Clearing Log Files
- Downloading Log Files
- Modifying Log Properties
- Viewing Log Details

Managing Application Logs

The application log contains events logged by applications or programs. For example, a word-processing program might record a file error in the application log. The events that are recorded are dependent upon the application.

To manage application logs

1. On the primary navigation bar, choose **Maintenance**.
2. Choose **Logs**.
3. Choose **Application Log**.

Related Topics

- Clearing Log Files
- Downloading Log Files
- Modifying Log Properties
- Viewing Log Details

Managing FTP Logs

The FTP log contains events logged by the FTP server.

To manage FTP logs

1. On the primary navigation bar, choose **Maintenance**.
2. Choose **Logs**.
3. Choose **FTP Log**.

Related Topics

- Clearing Log Files
- Downloading Log Files
- Modifying Log Properties
- Viewing Log Details

Managing NFS Logs

The NFS log contains events logged by the NFS server.

To manage NFS logs

1. On the primary navigation bar, choose **Maintenance**.
2. Choose **Logs**.
3. Choose **NFS Log**.

Related Topics

- Clearing Log Files
- Downloading Log Files
- Modifying Log Properties
- Viewing Log Details

System Log

The system log contains events logged by the Microsoft® Windows® 2000 system components. For example, the failure of a driver or other system component to load during startup is recorded in the system log.

To manage system logs

1. On the primary navigation bar, choose **Maintenance**.
2. Choose **Logs**.
3. Choose **System Log**.

Related Topics

- Clearing Log Files
- Downloading Log Files
- Modifying Log Properties
- Viewing Log Details

Security Log

The security log can record security events such as valid and invalid logon attempts as well as events related to resource use such as creating, opening, or deleting files. An administrator can specify what events are recorded in the security log.

To manage security logs

1. On the primary navigation bar, choose **Maintenance**.
2. Choose **Logs**.
3. Choose **Security Log**.

Related Topics

- Clearing Log Files
- Downloading Log Files
- Modifying Log Properties
- Viewing Log Details

Managing Web HTTP Shares Logs

The Web HTTP shares log contains events logged by the Web server related to accessing HTTP shares.

To manage Web (HTTP) shares logs

1. On the primary navigation bar, choose **Maintenance**.
2. Choose **Logs**.
3. Choose **Web (HTTP) Shares Log**.

Related Topics

- Clearing Log Files
- Downloading Log Files
- Modifying Log Properties
- Viewing Log Details

Managing Web Administration Logs

The Web administration log contains events logged by the Web server related to accessing the administration Web site.

To manage Web administration logs

1. On the primary navigation bar, choose **Maintenance**.
2. Choose **Logs**.
3. Choose **Web Administration Log**.

Related Topics

- Clearing Log Files
- Downloading Log Files
- Modifying Log Properties
- Viewing Log Details

Clear Log Files

From this page you can clear specific log files. When you clear application, NFS, security, or system logs, all log content is cleared, however, when you clear FTP, Web administration, or Web (HTTP) shares logs, you may select the specific log files you want to clear.

To clear application, NFS, security, or system logs

1. On the primary navigation bar, choose **Maintenance**.
2. Choose **Logs**.
3. Select the type of log you want to clear.
4. Select **Clear Log**.
5. Choose **OK**.

To clear FTP, Web administration, or Web (HTTP) shares logs

1. On the primary navigation bar, choose **Maintenance**.
2. Choose **Logs**.
3. Select the type of log you want to clear.

4. Select one or more log files to clear.
5. Choose **Clear Log**.
6. Choose **OK**.

Related Topics

- Downloading Log Files
- Modifying Log Properties
- Viewing Log Details

Download Log Files

From this page you can download specific log files to your server appliance.

To download application, security or system logs

1. On the primary navigation bar, choose **Maintenance**.
2. Choose **Logs**.
3. Choose the type of log you wish to download.
4. Choose **Download**.
5. Select **Save this file to disk**
6. Click **OK** to download the file.

To download NFS logs

1. On the primary navigation bar, choose **Maintenance**.
2. Choose **Logs**.
3. Choose **NFS Logs**.
4. Choose **Download**.
5. Select **Save this file to disk**.
6. Choose **OK**.

To download FTP, Web administration, or Web (HTTP) shares logs

1. On the primary navigation bar, choose **Maintenance**.
2. Choose **Logs**.
3. Select the log to download.
4. Select the log file to download.
5. Choose **Download**.
6. Select **Save this file to disk**.
7. Choose **OK**.

Related Topics

- Clearing Log Files
- Modifying Log Properties
- Viewing Log Details

Modify Log Properties

You can configure the properties for application, system, and security logs. From this page you can specify the maximum log size and determine how the system will handle log entries when the maximum capacity of the server appliance is reached.

To modify the properties of a log file

1. On the primary navigation bar, choose **Maintenance**.
2. Choose **Logs**.
3. Choose the **Application**, **System**, or **Security** log you wish to configure.
4. Select the log you want to configure.
5. Choose **Properties**.
6. In the **Maximum log size** box, type the maximum size of the log, in kilobytes.
7. Select the button that best represents how you want to handle log entries once the

maximum log size is reached.

Related Topics

- Clearing Log Files
- Downloading Log Files
- Viewing Log Details

View Log Entry Details

You can view the log entry details for application, system, and security logs. From this page you can view the date, time, source, event identifier, description, and data of specific log files.

To view the details of a log file

1. On the primary navigation bar, choose **Maintenance**.
2. Choose **Logs**.
3. Choose the type of log you wish to view.
4. Select the log entry you want to view.
5. Choose **Details**.
6. Choose **Up** and **Down** to scroll through the log files.
7. Choose **Back** to return to the Object/Task Selector for the specific log type you've chosen.

Related Topics

- Clearing Log Files
- Downloading Log Files
- Modifying Log Properties

Global Array Manager Overview

The Global Array Manager (GAM) is a utility that administrators can use to monitor, maintain, and configure the MaxAttach RAID subsystem.

Administrators can use the GAM to:

- Run routine system tests (e.g.: drive consistency check, patrol reads, device health monitoring)
- View drive statistics and logs (e.g.: disk and controller information, controller log file, NVRAM error tables)
- Monitor real-time disk array read/write statistics
- Configure or initialize the MaxAttach RAID arrays
- Replace a failed drive



WARNING

The Global Array Manager is a powerful utility that must be used properly to prevent data loss. The utility provides many cautions and warnings. Read these carefully before acting.

To start the Global Array Manager:

1. Using Internet Explorer, log in to the MaxAttach as administrator.
2. Click Disks on the main menu bar.
3. Select RAID Configuration. This starts a terminal services session.
4. Log in to Windows 2000. The GAM displays.
5. To log in to the GAM for the first time, use gamroot as the username. Leave the password field blank.

The Global Array Manager has its own help system. Click the Help icon to find out more about GAM features.

Chapter #11 - Appendix - Disk Array RAID Concepts

Chapter Outline

- Introduction to RAID
 - RAID basic comparison
 - RAID benefits
 - RAID limitations
 - RAID verses performance
- Primary RAID concepts
 - Striping
 - Fault tolerance
 - Array
 - Mirroring
 - Hot Standby
 - Hot Swappable
 - Spanning
 - Parity checking
- RAID array type definitions
 - RAID 0
 - RAID 1
 - RAID 0+1
 - RAID 5
 - JBOD
- RAID Array comparisons: performance, data capacity, access speed.
- Considerations for creating different types of arrays:
 - RAID 0
 - RAID 1
 - RAID 0+1
 - RAID 5
 - JBOD

- Managing RAID Arrays with Mylex RAID Controller and GAM
 - RAID Controller
 - SCSI Bus
 - GAM Server
 - GAM Client
 - Typical operations: create new arrays, add drives to new, add drives to existing, free up drives from existing, create hot spare, reconfigure last in array, reconfigure middle array

Introduction

Your Maxtor MaxAttach NAS 6000 Base unit comes configured with a set of standard RAID 5 disk arrays that are ready to go after physical installation. If you want to configure the system into other available configurations to suite your unique local needs, you should have a understanding of disk array concepts including RAID or Redundant Arrays of Independent Disks which forms the key methodology in the MaxAttach NAS 6000 system.

RAID - Redundant Array of Independent Disks

RAID Introduction and Overview

RAID is an acronym for Redundant Array of Independent Disks which was developed to optimize groups of hard disk drives to provide various combinations of:

- greater storage capacity than a single physical disk,
- better fault tolerance and data recovery capabilities in the event of a disk failure, and
- faster transfer of the data to and from the disks.

A RAID array is a collection of drives which collectively act as a single storage system, which can tolerate the failure of a drive without losing data, and which can operate independently of each other.

Each level is a different way to spread data across multiple drives--a compromise between cost and speed. Understanding these levels is important, because each level is optimized for a different use.

The common RAID specifications are numbered from 0 to 5, although only RAID 0, RAID 1, and RAID 5 are in current common use with current high performance disk technology.

The user data arrays in the Maxtor MaxAttach NAS 6000 Base Unit are factory configured as RAID 5 arrays, or although RAID 0 or RAID 1 arrays may be used along with another common disk drive configuration method called JBOD (Just a Bunch of Disks).

Key RAID Technical Methods

These key technical methods are used in varying combinations in most RAID/JBOD configurations and will help you understand how a disk array works and why you want one type as opposed to another type for your application.

Hardware RAID and Software RAID

RAID is also divided by the way it is implemented. In the MaxAttach, the disk arrays are implemented as “Hardware RAID” and controlled by a RAID Controller card located in the system Base Unit. In some systems, software drivers are used to control RAID's or “Software RAID.”

In hardware RAID, an array of disk drives is controlled by a RAID controller which administers the data I/O to the disks based on the type of RAID configuration. Using today's disk drives, RAID controllers use combinations of striping, spanning, mirroring and parity checking techniques to obtain an optimum balance of increased disk size, improved data safety, and increased read/write I/O performance.

Striping

Striping is the underlying concept behind most RAID levels. A stripe is a contiguous sequence of data blocks that is written to one or more disk drives. A stripe may be as short as a single data block, or may consist of thousands. The RAID controllers split up their component disk partitions into stripes; the different RAID levels differ in how they organize the stripes, and what data they put in them. The interplay between the size of the stripes, the typical size of files in the file system, and their location on the disk is what determines the overall performance of the RAID subsystem. The effect is to allow larger data volumes than those provided by a single physical disk. Striping is also called Spanning.

Mirroring

Mirroring is creating an exact copy of data from one drive or array on a second drive or array. The entire read/write procedure is done in parallel. Mirroring is the highest level of fault tolerance with 100% of the data backed up as it is created and written. Mirroring is also the most expansive fault tolerance technique where 50% of your disk space is spent on providing fault tolerance,

Parity Checking

Parity checking is creating a parity check sum for the writes to drives in an array, and then writing the parity information to a dedicated parity drive (called dedicated parity) or writing the parity information as the next striped data block to the next drive in the array.separate data block (called distributed parity). The parity check sum allows the system to recover missing data in the event of the failure of a single member of RAID array.

By combining these techniques in various combinations, different system capabilities are provided to met a users unique local needs.

RAID and JBOD Types

The common RAID types are as follows and all area available to most user data drives on the NAS 6000:

- RAID 0 - Striping
- RAID 1 - Mirroring
- RAID 0+1 - Mirrored sets of Striped Disks
- RAID 5 - Striped Disks with Parity Check
- JBOD - An additional non-RAID option for single disk control, also called Just a Bunch Of Disks

RAID 0 Striping

Description

RAID 0 is a performance oriented striped data mapping technique across two or more drives.

Uniformly sized blocks of storage are assigned in regular sequence to all of an array's disks. The controller divides incoming data into as many chunks as there are drives and then writes that data across independent disks. The writing technique is called “striping.” Since all disk write heads work independently, RAID 0 provides the fastest performance RAID configuration.

Fault Tolerance Cost

RAID 0 arrays have no fault tolerance characteristics beyond that provided by each individual disk. As such, there is no utilization space cost. 100% of the drive capacity is available for user data.

Performance

RAID 0 provides high I/O performance at low inherent cost as no additional disks are required and the entire array disk space is used for user data. Fault Tolerance Provided

Application Focus

RAID 0 is often used in managing transient data that has to be processed quickly and then deleted.

The extremely high data throughput rates are especially valuable for applications using large files.

Array Size

The array can be from 2 to 16 drives.

RAID 1 Mirroring

Description

In RAID 1 mirroring, the RAID controller totally duplicates the data writes on two drives at once, providing 100% data redundancy. If one drive fails, the second drive carries on as before with reads and writes until a replacement drive can be added for a data restore. RAID 1 has been used longer than any other form of RAID.

Depending on the system, either the drives, or the drives and their controllers are duplicated.

Fault Tolerance Cost

RAID 1 is fully fault tolerance but carries a 50% disk space cost to implement.

Performance

RAID 1 arrays may use parallel access for high transfer rate when reading. More commonly, RAID 1 array disks operate independently and improve performance for read-intensive applications, but at relatively high inherent cost. If one drive drops offline, read/write performance is the same until the rebuild process starts. During restores, performance can be degraded as the drive controller rebuilds the replacement disk drive.

Application Focus

RAID 1 practical use is usually limited to applications where fault tolerance is required, regardless of cost. This is used primarily in high reliability systems where constant availability is required.

Array Size

RAID 1 array disks are always in pairs. Two disk arrays can be mirrored using a common technique, described below, called RAID 0 + 1 where a striped array of multiple disks is then mirrored. This technique is used in the MaxAttach NAS 6000 O/S images on drive C:\ and D:\.

RAID 0 +1 Mirrored Sets of Striped Drives

Description

RAID 0+1 is a dual level array that utilizes multiple RAID 1 mirrored sets into a single array. Two arrays of striped disks are created. The controller then creates a mirror of the striped array. This technique is used in the MaxAttach NAS 6000 O/S images on drives C:\ and D:\. The resultant array is 100% fault tolerant with an two exact images. The failure of one image usually causes the system to automatically failover to the remaining image.

Fault Tolerance Cost

The fault cost, like RAID 1 is 50% of total available disk space.

Performance

Each drive in the array is duplicated or mirrored. This eliminates the overhead and delay of parity. A RAID 0 + 1 array offers high data transfer advantages of striped arrays and increased data accessibility or reads.

Performance is better than RAID 3, striping with dedicated parity, and RAID 5, striping with distributed parity.

System performance during a drive rebuild is also better than that of parity based arrays, since data does not need to be regenerated from parity information, but copied from the other mirrored drive.

Application Focus

High performance applications where absolute data availability is a must.

Array Size

A minimum of three disks is required to implement RAID 0 + 1, although in practical terms, most RAID 0 + 1 arrays start at four disks. The maximum number of disks is 16.

RAID 5 Multiple Disk Striping with Distributed Parity

Description

RAID 5 is the default user data disk array configuration used in the NAS 6000 in arrays of six disks and is probably the most popular RAID technique in the world. The factory configured user drives in the Base Unit are configured as six disk RAID 5 arrays. RAID 5 in six disk arrays is also the recommend user configuration for Expansion Units.

This level is commonly referred to as striping with distributed parity. No single disk is devoted to parity. The controller strips blocks of data across all drives in the array and then the last data block is written as a parity check of the current write.

On a single drive failure, the parity and remaining data can be used to recreate the missing drive data set. During the time of a drive failure, the array is in a “critical” state, where the data is still safe and array operation continues. However, the failure of any additional drive will cause the loss of all array data.

When a failed drive is replaced either manually or by a hot standby drive, the array rebuild process starts, ultimately fully restoring the fault tolerant nature of the array. In the Maxtor MaxAttach NAS 6000, a Hot Spare drive can be optionally configured that will automatically take over for any failed drive.

A replacement disk or disks can be added to the array so that the system can carry on with user access and full I/O operations even while the rebuild process takes place. The system uses the parity information to recalculate the missing data elements. There is some degradation of service during an online rebuild.

Fault Tolerance Cost

The fault tolerance cost is a function of the number of drives in the array where the equivalent of one array drive's disk space is used for parity.

In RAID 0, there is no fault tolerance, and hence, no fault tolerance cost.

In RAID1, there is fault tolerance as 50% of the drives are used for data backup.

In RAID 5, the cost is approximately the equivalent of one drive per array. In a four drive array, the cost is 25%. In a six disk array, the cost is 17%. In a ten disk array, the cost is 10%.

Performance

Each of the drives is used to store the parity bit, greatly reducing any impact on performance. This can speed small writes in multiprocessing systems. By distributing parity across all of the array's member disks, RAID 5 reduces but does not eliminate the write bottleneck. The performance for reads tends to be lower than for other RAID options. The result is asymmetrical performance, with reads substantially outperforming writes. Although arrays can be from three to 16 drives in size, longer arrays require longer write times.

Array Size

RAID 5 can use a minimum of 3 drives and can be as large as 16 drives. In practical terms, the optimum combination of performance and fault tolerance is usually at six drive. Larger arrays are slower but with lower fault tolerance cost. Smaller arrays faster but are more expensive. RAID-5 is currently viewed as the most appropriate implementation of RAID or large systems.

JBOD Just a Bunch of Disks Single Disk Control

Description

JBOD is not a RAID methodology, but simply single drive control. The controller treats each drive as a standalone disk and provides a high-performance cache. The limitations of JBOD are volume size limited to physical disk size, decreased performance because striping is not present for performance enhancements, and there is no recovery from a disk drive failure.

Fault Tolerance Cost

There is no fault tolerance with JBOD and hence no associated cost.

Performance

The benefits are speed and discrete volume availability. The cache reduces the amount of time the computer waits for a disk to get to the right place to read or write data. The individual disk drive volumes allows for increased data security and permits easy removal of sensitive confidential material to secure physical storage.

Array Size

JBOD is a single disk at the physical disk level. File server O/S can group single JBOD drives into larger multi-drive volumes, but without any striping nor with any fault tolerance.

RAID Benefits Comparison

The tables below summarize and compare the general benefits and functions of each type of RAID configuration.

Table #1 - RAID Comparison			
RAID Level	Description	I/O Advantage	Fault Tolerance
RAID 0	Disk Striping	YES - Fastest	No
RAID 1	Mirroring	NO	YES
RAID 2	Striping with ECC (hamming) - Synchronous-	NO	YES
RAID 3	Striping with dedicated parity and synchronized disks	YES	YES
RAID 4	Striping with dedicated parity and non synchronized disks	YES	YES

Table #1 - RAID Comparison

RAID Level	Description	I/O Advantage	Fault Tolerance
RAID 5	Striping and parity distributed across ALL disks	YES	YES
Volume Set	No Striping No Parity	NO	NO

RAID Functional Comparison

The table below summarizes the strengths and limitations of each RAID and JOBD configuration.

Table #2 - RAID Level Comparison

RAID Level	Description	Data Reliability	Data Transfer and I/O Request Rate	Application Strength	Cost
RAID 1	All data copied onto 2 separate disks	Very high. Can withstand selective multiple disk failures	Data transfer rate is higher than single disk for reads, but does not offer load balancing. Twice that of a single disk for reads. Slightly slower than single disk for writes	General	Very high. Requires twice as many disks for redundancy
RAID 2	Data striped across multiple disks with parity on multiple disks	Very high. Can withstand selective multiple disk failures	High if error correcting codes are computed by hardware Similar to twice that of a single disk	General	High. Requires multiple disks for redundancy
RAID 3	Data striped across all data disks with dedicated parity disk	Much higher than single disk. Can withstand single disk failure	Highest of all types listed here for reading and writing Faster than a single disk, owing to parallel disk accesses	Video, prepress, medical imaging, and other large file applications	Low. Requires only one disk for redundancy
RAID 4	Data striped across some data disks with dedicated parity disk	Much higher than single disk. Can withstand single disk failure	High compared to single disk for reads but significantly lower than single disk for writes*.	Predominantly read-oriented with few writes	Low.
RAID 5	Data and parity striped across multiple disks	Much higher than single disk. Can withstand single disk failure	High compared to single disk for read but generally lower than single disk for writes* Transaction processing with high read to write ratio.	Low. Requires only one disk for redundancy	

*Write operations are slow in these cases because the controller must read parity information from a disk and recompute parity information for the disk before it writes information to the disk array

RAID Fault Tolerance Characteristics

Table #3 - RAID Level Availability & Fault Tolerance Characteristics	
RAID Level	Availability & Fault Tolerance Characteristics
0	No fault tolerance. Data is striped across a set of multiple disks. If a disk in the set ceases to function, all data contained on the set of disks is lost. (If fault tolerance is needed, this configuration is not recommended). Excellent for all types of I/O activity.
00	Spanned RAID 0
1	Mirrored fault tolerance. Data is written to one disk, and then the same data is written to another disk. If either disks fails, the other one in the pair is automatically used to store and retrieve the data. Excellent for write-intensive applications
10	Spanned RAID 1
3	Striped fault tolerance with dedicated drive parity. Data and parity are striped across a set of multiple (at least three) drives. If any of the drives fail, the data (or parity) information from the failed drive is computed from the information from the remaining drives.
30	Spanned RAID 3
5	Striped fault tolerance. Data and parity are striped across a set of multiple (at least three) drives. If any of the drives fail, the data (or parity) information from the failed drive is computed from the information from the remaining drives. Excellent for sequential or random reads and sequential writes
50	Spanned RAID 5
0+1	Mirrored and striped fault tolerance. Data and parity information is striped across multiple drives and written to a mirrored set of drives. This arrangement can survive multiple drive failures and continue to operate.
0+1+0	Spanned RAID 0+1
JBOD	Just a Bunch of Disks. JBOD offers no redundancy and is not recommended for applications requiring fault tolerance.

RAID and Obtaining Maximum Performance

To see the advantages of the RAID levels as they apply to performance, see the table below.

Table #4 - RAID Level Access Profile Characteristics	
RAID Level	Access Profile Characteristics
0	Excellent for all types of I/O activity.
1	Excellent for write-intensive applications.
3	Good for sequential or random reads and sequential writes.
5	Excellent for sequential or random reads and sequential writes.
0+1	Excellent for write-intensive applications.
JBOD	Mimics normal, individual disk performance characteristics.

Maxtor MaxAttach NAS 6000 RAID Operations and the GAM

Within the MaxAttach NAS 6000, the disk arrays are controlled by the Mylex Disk Array Controller card mounted in the Base Unit. Administrators control the functions and configuration of the disk arrays using the Global Array Manager (GAM) Server/Client application.

The GAM provides several features that can provide added fault tolerant to NAS 6000 systems that are described below.

Normal Array Status

During normal operations, all drives in the array are healthy and functions. From the perspective of the user and the O/S, all the drive members of the array represent a single local drive or volume.

Critical Array Status

A drive array is in a “critical state” whenever one and only one of its member drives have failed. This only applies to RAID types where a drive failure can be tolerated; typically RAID 1, RAID 3, RAID 5, and RAID 0+1. While the array is critical, it continues to work, but the failure of any second drive in the array will result in the loss of all array data.

Hot Swap Drives

The term “Hot Swap” refers to the common practice of either inserting or removing disk drives in an operating bus. In the MaxAttach NAS 6000, this specifically refers to the ability to remove defective or failing drive from the system, insert new unformatted drives, and then have the system rebuild and repair the array while maintaining normal system operation and user access to their data.

In practical terms, this means that drives can be removed whenever they are quiescent, or not involved in the write operation. For best results and to eliminate the possibility of losing data, use the GAM to make the disk off line so that the amber Disk Status LED lights. With the disk unavailable, all read/writes are canceled and the disk can be safely exchanged.



WARNING

READ/WRITE I/O OPERATIONS: When ever the disk green LED is blinking, the disk is undergoing some sort of I/O operation. Never remove a disk drive during an I/O operation or data loss will occur.

After the failed drive has been exchanged for a new drive, the administrator must use the GAM to rebuild the affected array and incorporate the new drive. Once initiated by the administrator, the rebuild process will proceed in the background with some load on system performance. A full rebuild of a six disk array takes between five and seven hours.

Hot Spare Drives

Hot Spare Drives (also called Hot Standby Drives) are one or more drives that are not assigned to any RAID array nor being used as a JBOD disk. These are available in reserve to take over in case of the failure of any array drive. Controlled by the Mylex RAID Controller card, a hot spare drive is powered-on but idle during normal array operation. If a failure occurs on a disk in a fault-tolerant RAID array, the hot spare drive takes over for the failed drive and the array rebuild process begins as described above.

After completing an automatic rebuild cycle, the array continues to function in a fully fault-tolerant mode. The rebuild cycle for a six disk RAID 5 array takes between five and seven hours. After the rebuild cycle completes, the array is returned to full fault tolerance and normal I/O operations. the array can now safely suffer a second drive failure and continue to function before any disks are replaced.

Comparison of Terms

A variety of terms are used to define disks and volumes. One problem exists in that Microsoft, Mylex, and common terminology use slightly differing definitions of these terms. The table below summarizes the various terms with additional discussion below.

Table #5 - Comparison of Disk and Array Terms

Microso ft Term	Term Definition	Mylex Term
Folder	File collection on a volume	
Partition	Partition: Basic, Simple, Dynamic When you format a hard drive, you can assign the number of partitions you want on a physical hard disk. The computer will recognize each partition as a separate drive, and they will show up as different drives under most operating systems; a logical drive.	
Volume	The name given to a disk partition, or group of partitions, that is available to network users as a single designated drive. A drive may cover several volumes and a volume may span several physical drives under some operating systems.	
Physical Drive	A hardware RAID controller's presentation of a disk to the O/S. Identified as standard drive letters: C:\, D:\, E:\, etc.	Logical Drive
	A list of physical drives that store one or more logical drives. An array must contain at least one logical drive although multiple logical drives can be made from within one array. Array types are RAID 0, RAID 1, RAID 0+1, RAID 5, and JBOD.	Array of disks
	The physical disk drives inserted into the MaxAttach NAS 6000 Base or Expansion Unit drive bays. Each drive is identified by its SCSI Channel and LUN ID. (e.g. drive 0:03 is drive LUN 03 on SCSI channel 0.)	Physical Drive - SCSI Address
	There are 12 drives per shelf and 36 drives in a fully configured system. Physical naming convention labels the Base Unit as BU; the first Expansion Unit as EU1, and the second Expansion Unit as EU2. Drives are identified as 1 to 12 from left to right when viewed from the front.	Physical Drive - Equipment Shelf and Physical Position

Volume Set

- A volume set is an additional storage type, not included in the RAID specifications but supported by Windows NT is a VOLUME SET.
- A volume set simply allows the logical drive to be extended to an additional physical drive.
- It offers no additional performance or fault tolerance and is in fact quite dangerous since the failure of one of the members of the volume will destroy the entire volume.

Logical (System) Drives

After all physical drive groups are defined and arranged, one or more logical drives must be created. Logical drives are the drives presented to the operating system.

A logical drive's capacity may encompass any portion of a drive group (up to the total capacity of that Drive Group), or the capacity of more than one drive group. Up to 8 (below PCI firmware version 2.6, and all External Controller firmware) or 32 (PCI firmware version 2.6 and above) logical drives may be created. The following illustration shows a RAID 0+1 configuration with three mirrored logical drives created in a drive group containing three disk drives.

System Drives

Each System Drive has a defined RAID Level (0, 1, 5, 0+1, etc.) based on the number of drives in the Drive Group from which it is created. If a Drive Group has enough drives to support several different RAID levels, the System Drive can be assigned any available levels. However, a System Drive may have only one RAID level.

Chapter #12 - Appendix - SNMP

Chapter Outline

- Overview of MaxAttach NAS 6000 SNMP capabilities
- SNMP Alerts
- Overview
- Management System
- Agent
- Management Information Base
- Specifications
- MIB File Locations
- Windows 2000 Server SNMP MIB
- Maxtor MaxAttach NAS 6000 SNMP MIB
- Maxtor MaxAttach NAS 6000 SNMP MIB Tree
- Maxtor MaxAttach NAS 6000 SNMP MIB Variables
- MaxAttach SNMP Traps

Overview

MaxAttach NAS 6000 and SNMP (Simple Network Management Protocol) monitors and traps report alert conditions, which are then accessible at an SNMP management system.

MaxAttach SNMP Alert Overview

MaxAttach SNMP service provides SNMP agents that can participate in remote, centralized management via SNMP management consoles.

Using SNMP requires two components: an SNMP management system and an SNMP Agent.

SNMP Management System

The SNMP management system, also called the *management console*, sends information and update requests to an SNMP agent across the network. Any computer running SNMP management software is an SNMP management system. The management software application does not need to run on the same host as the SNMP agent.

The SNMP management system requests information from a managed computer, such as the amount of hard disk space available or the number of active sessions. The SNMP management system can also initiate a change to the configuration of an SNMP agent. However, this is rare because most clients have read-only access.

SNMP Agent

MaxAttach and Windows 2000 as SNMP Agents

Any computer running SNMP agent software is an *SNMP agent*. As such, the Maxtor MaxAttach NAS 6000 thus also functions as an SNMP agent. The SNMP agent responds to SNMP management system requests for information. The Windows 2000 SNMP service, which is also an SNMP agent, responds to information requests from one or more management systems. The SNMP service can be configured to specify which statistics are tracked and which management systems are authorized to request information.

Respond Only To Queries

In general, SNMP agents do not originate messages, but only respond to queries. The exception is the *trap message*. The agent originates a trap message when an alarm-triggering event occurs, such as a system reboot or illegal access. By monitoring trap events, managers can provide enhanced system security.

SNMP Community

Management hosts and agents belong to an SNMP *community*, which is a collection of hosts grouped together for administrative purposes. Defining communities provides security by allowing only management systems and agents within the same community to communicate.

Management Information Base

SNMP agents collect information in a database called a *Management Information Base*, or MIB. Microsoft has defined database structures for its servers in which its SNMP services collect a wide variety of information. In addition, MaxAttach NAS units have an additional set of unique MIB variables developed specifically for the MaxAttach NAS system. The MaxAttach NAS SNMP services support variables from both the Microsoft server MIBs and its own MIB.

For a list of supported variables, see the MaxAttach SNMP Specification section below.

Configuring SNMP Service

To configure the SNMP service

1. On the primary menu bar, select **Network Setup**.
2. Select the **SNMP Service Configuration** option.
3. Follow the prompts and re-enter your User name and Password.
4. Double-click **SNMP Service** in the list of services.
5. Edit values as needed on the **Agent**, **Traps**, and **Security** tabs. Do not alter values on the other tabs.
6. For information on specific fields in the tabs, right-click a field to view “What's This?” help (or select a field and press F1).
7. Click **OK**.
8. Close the Services window.

MaxAttach SNMP Specifications

The SNMP agent support for the Maxtor MaxAttach NAS 6000 consists of various SNMP extension agents provided by the Windows 2000 Server and by the MaxAttach SNMP extension agent. Taken together, they provide the necessary management information and event traps for remote network management. The collection of management information and event traps is called the *management information base* or MIB.

MIB File Locations and Types

All of the SNMP MIB extension agent files are stored on the MaxAttach in the **C:/Winnt/System32** directory. A system's SNMP MIBs come from two sources:

- Windows 2000 Server SNMP extension agents
- MaxAttach NAS 6000 MIB

Windows 2000 Server SNMP MIBs

The Microsoft Windows 2000 Server supports the following SNMP MIBs:

- **mib_ii.mib:** The standard MIB 2 which provides the NAS server's general system and network information:
- **hostmib.mib:** The standard host resources MIB which provides information on the NAS server's storage and devices.
- **msft.mib, inetsrv.mib, ftp.mib, http.mib:** The Microsoft-defined FTP and HTTP MIBs which provide FTP and HTTP server statistics.

MIB Specifications

MaxAttach NAS 6000 SNMP MIB

- The MaxAttach NAS 6000 MIB is **mxtr6000.mib**.

MaxAttach NAS 6000 Series MIB Variables

The MaxAttach SNMP agent supports the following unique MaxAttach system information:

- **SysProdName:** NAS system product name
- **SysProdVersion:** NAS system product version
- **SysManufacturer:** NAS system manufacturer's name
- **SysComputerName:** NAS system computer name
- **sysCPUName:** NAS system processor name
- **sysBIOSVersion:** NAS system BIOS version
- **sysUptime:** The time (in hundredths of a second) since the NAS system was last brought on line
- **sysDate:** NAS System local time in display format as follows: year/month/day hour:minutes:seconds:milliseconds
- **sysPhysMemLoad:** The approximate percentage of physical memory in use in the NAS system
- **SysTotalPhysMem:** The amount of total physical main memory in Kbytes contained in the NAS system
- **SysFreePhysMem:** The amount of available physical main memory in Kbytes contained in the NAS system
- **SysTotalVirtualMem:** The amount of total virtual memory in Kbytes contained in the NAS system
- **SysFreeVirtualMem:** The amount of available virtual memory in Kbytes contained in the NAS system

MaxAttach NAS 6000 Series MIB Tree

The following table is the MIB tree for the MaxAttach NAS 6000 Series servers. The map starts with **1.3.6.1.4.1**, followed by the Maxtor Enterprise ID, **4693**. Under the MaxAttach NAS 6000 Series servers there is currently a single product, MaxAttach NAS 6000. The following table defines the system's information, objects, and trap definitions.



NOTE

All the defined objects have **Read-Only** access. This is indicated by the **R** in the MIB description.

4693	Maxtor Enterprise ID				
	6	NAS 6000 Series			
		1	NAS 6000 (OID = 1.3.6.1.4.1.4693.6.1)		
			10	System Information	
				1	R - sysProdName
				2	R - sysProdVersion
				3	R - sysManufacturer
				4	R - sysComputerName
				5	R - sysCPUName
				6	R - sysBIOSVersion
				7	R - sysUPtime
				8	R - SysDate
				9	R - SysPhysMemLoad
				10	R - SysTotalPhysMem
				11	R - sysFreePhysMem
				12	R - sysTotalVirtualMem
				13	R - sysFreeVirtualMem
			901	R - errorEventLogSummary	
			902	R - errorEventLogString	

MaxAttach SNMP Traps

The MaxAttach supports all of the standard Microsoft Windows 2000 events, and a number of these events pertinent to the functioning of the MaxAttach are sent as SNMP traps. The following event categories are supported as SNMP traps:

- Disk Events (ATAPI, Disk, DiskPerf, Dmboot, Dmio, LDM)
- Power (UPS)

In addition, the MaxAttach also provides traps for its internal environmental monitoring unit (EMU).

Table #1 - Environmental Monitoring Unit Traps		
Trap	Event ID	Description
Trap	Event ID	Description
Power Supply Status	2110 Information 2310 Error	Present, Over temp, AC fail, DC fail
Fan Status	2120 Information 2320 Error	Fan running, Fan Stalled
Disk Drive Present Status	2130 Information 2330 Error	Present, Not Present
Temperature Status	2150 Information 2350 Error	Temperature Levels 1, 2, or 3, where 3 is hottest
Disk Backplane Voltage Status	2160 Information 2360 Error	Voltages Nominal (+/- 5%), Out of tolerance
Intrusion Status	2180 Information 2380 Error	Intrusion Detected

Chapter #13 - Appendix - Disk Drive Error Codes

Mylex Disk Drive Failure Error Codes

These error codes indicate the cause of the drive failure:

Table #1 - Disk Device Error Codes (Sheet 1 of 3)	
Error Code	Error Code Cause
00 – NoCause	No error code or drive not DEAD
01 – WrtRecov01	Write recovery failed
02 – WrtRecov02	Write recovery failed
03 – WrtRecov03	Write recovery failed
04 – WrtRecov04	Write recovery failed
05 – WrtRecov05	Write recovery failed
06 – WrtRecov06	Write recovery failed
07 – WrtRecov07	Write recovery failed
08 – WrtRecov08	Write recovery failed
09 – WrtRecov09	Write recovery failed
0A – WrtRecov10	Write recovery failed
0B – WrtRecov11	Write recovery failed
0C – WrtRecov12	Write recovery failed
0D – WrtRecov13	Write recovery failed
0E – WrtRecov14	Write recovery failed
0F – WrtRecov15	Write recovery failed
10 – WrtRecov16	Write recovery failed

Table #1 - Disk Device Error Codes (Sheet 2 of 3)

Error Code	Error Code Cause
11 – WrtRecov17	Write recovery failed
12 – WrtRecov18	Write recovery failed
13 – WrtRecov19	Write recovery failed
20 – StartDev01	New drive state is DEAD
21 – StartDev02	Standby rebuild bit set
22 – StartDev03	State is DEAD
23 – StartDev04	Failed
30 – BusReset01	Bus reset did not clear (dead channel)
31 – BusReset02	Bus reset did not clear
40 – MaxConsecBusy	Max consecutive busy status count exceeded
41 – DoubleCc	Check condition status on request sense command
42 – MaxSelTimeout	Max consecutive selection timeout count exceeded
43 – CcDeferred	Check condition with sense data deferred error
44 – MaxPerr	Max consecutive/accumulated parity error count exceeded
45 – MaxResCnflct	Max consecutive reservation conflict status count exceeded
46 – MaxCcUatten	Max consecutive unit attention count exceeded
47 – MaxCmdTmout	Max accumulated command timeout count exceeded
50 – DevStatus01	New state is DEAD
51 – DevStatus02	Start device failed
60 – Restart01	Failed restart
61 – Restart02	Failed restart
62 – Restart03	Failed restart
63 – NewCfgFail	Failed to start after writing new configuration
70 – ScanSelTmo	Bus scan: selection timeout
71 – ScanMaxCc	Bus scan: max check conditions exceeded
72 – DevInsertFail	Device insertion: failed to spin device
73 – DevInsertOffl	Device insertion: system drive went offline
74 – UncfigDev01	Unconfigured device failed inquiry

Table #1 - Disk Device Error Codes (Sheet 3 of 3)

Error Code	Error Code Cause
75 – UncfigDev02	Unconfigured device found
76 – UncfigDev03	Unconfigured device found
77 – BadCodId01	Device COD ID does not match selected COD ID
78 – BadCodId02	Device COD ID does not match selected COD ID
79 – DevRoamDead	Drive roaming: dead device moved
7A – DevRoamFail	Drive roaming: failed
7B – DevRoamRplcd	Drive roaming: replaced drive
7C – ScanInqFail	Bus scan: inquiry failed
80 – RbldOffline	System drive went offline during rebuild start
81 – RbldTooSmall	Drive too small for rebuilding
82 – RbldFailed	Rebuild failed and drive not already marked DEAD
83 – RbldTerminated	Rebuild terminated, move rebuilding drive to DEAD
84 – RbldOffline02	System drive went offline during rebuild start
A0 – NoSpareTrack	Drive reported 04/32/00 sense - no spares available

Chapter #14 - Appendix - Disk Array Error Codes

Error Codes Overview

A full list of Error Codes, descriptions, and severity levels can be obtained by opening and reading the EVENTDEF.TXT file inside the folder C:\GAM on the Base Unit.

This information is also available in below in **Table #1 - Mylex Error Codes**. The table displays error descriptions and related messages from the Mylex RAID Controller Card.

Mylex Severity Levels

The Severity Levels are defined by default as follows:

- Critical (0)
- Serious (1)
- Error (2)
- Warning (3)
- Informational (4)

O/S Error Processing

The O/S processes the Mylex Errors based on instructions located in the **SupportedEvents.Inf** file. This file instructs the system when to turn on and off the amber Drive Status LED.

Listing of SupportedEvents.Inf

In its default factory setting, the SupportedEvents.Inf listing is as follows:

```
[Version]
Signature="$Windows NT$"
Provider="Maxtor"
[ONEVENT]
ONEVENT=10,12,33,34,35,36,37,38,39,40,41,42,43,44,45,46,47,48,49,50,54,57
[OFFEVENT]
OFFEVENT=1,2
```

Instructions to Turn Amber Disk Status LEDs Off

The **SupportedEvents.Inf** file instructs the system to turn the amber Disk Status LED **OFF** whenever the following events occur. The information in parenthesis stands for *Gam_event number, User_event number, Priority level, and Severity level*.

- A hard disk has been placed online (1, 1, 4, Information)
- A hard disk added as hot spare (2, 2, 4, Information)

Instructions to Turn Amber Disk Status LEDs On

The **SupportedEvents.Inf** file instructs the system to turn the amber Disk Status LEDs **ON** whenever the described event occurs. The information in parenthesis stands for *Gam_event number, User_event number, Priority level, and Severity level*.

- Rebuild stopped with error. New device failed. (10, 10, 2, Error)
- A hard disk has failed. (12, 12, 1, Serious)
- A hard disk failed because write recovery failed. (33, 33, 1, Serious)
- A hard disk failed because SCSI bus reset failed. (34, 34, 1, Serious)
- A hard disk failed because double check condition occurred. (35, 35, 1, Serious)
- A hard disk failed because device is missing. (36, 36, 1, Serious)
- A hard disk failed because of gross error on SCSI processor. (37, 37, 1, Serious)
- A hard disk failed because of bad tag from the device. (38, 38, 1, Serious)
- A hard disk failed because command to the device timed out. (9, 39, 1, Serious)
- A hard disk failed because of the system reset. (40, 40, 1, Serious)
- A hard disk failed because of busy status or parity error. (41, 41, 1, Serious)
- A hard disk set to failed state by host. (42, 42, 1, Serious)
- A hard disk failed because access to the device met with a selection time out. (43, 43, 1, Serious)
- A hard disk failed because of a sequence error in the SCSI bus phase handling. (44, 44, 1, Serious)
- A hard disk failed because device returned an unknown status. (45, 45, 1, Serious)

- A hard disk failed because device is not ready. (46, 46, 1, Serious)
- A hard disk failed because device was not found on start up. (47, 47, 1, Serious)
- A hard disk failed because write operation of the 'Configuration On Disk' failed. (48, 48, 1, Serious)
- A hard disk failed because write operation of 'Bad Data Table' failed. (49, 49, 1, Serious)
- Physical device status changed to offline. (50, 50, 3, Warning)
- Physical device failed to start. (54, 54, 3, Warning)
- Physical drive missing on startup. (57, 57, 1, Serious)

Viewing and Changing Error Codes

You can view Error Codes individually, and change Error Codes using the Event Editor.

To change an error code description

1. Select Administration > Settings and then select the Event Editor Tab.
2. In the Event ID Field, select the event number.
3. In the User Event ID Field, enter the ID number.
4. In the Severity Field, select the severity level.
5. Use the check boxes to configure your error event at to:
 - Alarm Sound
 - Pager Notification
 - Email Notification
 - Fax Notification
 - Launch Application.
6. If required, in the Event Message Text Field, edit the message.
7. If you make a mistake, click on the Default All button to reset the message to the default settings.
8. To commit your changes, click on the OK button.

Error Codes - EVENTDEF.TXT

The Mylex RAID Controller Error Codes are used to generate the error messages related to the RAID Controller and its attached disk drives.

Mylex Error Codes Table

Table #1 - Mylex Error Codes (Sheet 1 of 8)				
Gam_ev ent Number	User_ev ent Number	Priority Number	Severity Level	Description
1	1	4	Information	A hard disk has been placed online.
2	2	4	Information	A hard disk added as hot spare.
3	3	3	Warning	Hard disk error found.
4	4	3	Warning	Hard disk PFA condition found, this disk may fail soon.
5	5	4	Information	An automatic rebuild has started.
6	6	4	Information	A rebuild has started.
7	7	4	Information	Rebuild is over.
8	8	4	Information	Rebuild is cancelled.
9	9	2	Error	Rebuild stopped with error.
10	10	2	Error	Rebuild stopped with error. New device failed.
11	11	2	Error	Rebuild stopped because logical drive failed.
12	12	1	Serious	A hard disk has failed.
13	13	4	Information	A new hard disk has been found.
14	14	4	Information	A hard disk has been removed.
15	15	4	Information	A previously configured disk is now available.
16	16	4	Information	Expand Capacity Started.
17	17	4	Information	Expand Capacity Completed.
18	18	2	Error	Expand Capacity Stopped with error.
19	19	4	Information	SCSI command timeout on hard device.
20	20	4	Information	SCSI command abort on hard disk.

Table #1 - Mylex Error Codes (Sheet 2 of 8)

Gam_ev ent Number	User_ev ent Number	Priority Number	Severity Level	Description
21	21	4	Information	SCSI command retried on hard disk.
22	22	3	Warning	Parity error found.
23	23	3	Warning	Soft error found.
24	24	3	Warning	Misc error found.
25	25	4	Information	SCSI device reset.
26	26	4	Information	Active spare found.-
27	27	4	Information	Warm spare found.-
28	28	4	Information	Request Sense Data available.
29	29	4	Information	Initialization started.
30	30	4	Information	Initialization completed.
31	31	3	Warning	Initialization failed.
32	32	4	Information	Initialization canceled.
33	33	1	Serious	A hard disk failed because write recovery failed.
34	34	1	Serious	A hard disk failed because SCSI bus reset failed.
35	35	1	Serious	A hard disk failed because double check condition occurred.
36	36	1	Serious	A hard disk failed because device is missing.
37	37	1	Serious	A hard disk failed because of gross error on SCSI processor.
38	38	1	Serious	A hard disk failed because of bad tag from the device.
39	39	1	Serious	A hard disk failed because command to the device timed out.
40	40	1	Serious	A hard disk failed because of the system reset.
41	41	1	Serious	A hard disk failed because of busy status or parity error.
42	42	1	Serious	A hard disk set to failed state by host.
43	43	1	Serious	A hard disk failed because access to the device met with a selection time out.
44	44	1	Serious	A hard disk failed because of a sequence error in the SCSI bus phase handling.
45	45	1	Serious	A hard disk failed because device returned an unknown status.
46	46	1	Serious	A hard disk failed because device is not ready.

Table #1 - Mylex Error Codes (Sheet 3 of 8)

Gam_ev ent Number	User_ev ent Number	Priority Number	Severity Level	Description
47	47	1	Serious	A hard disk failed because device was not found on start up.
48	48	1	Serious	A hard disk failed because write operation of the 'Configuration On Disk' failed.
49	49	1	Serious	A hard disk failed because write operation of 'Bad Data Table' failed.
50	50	3	Warning	Physical device status changed to offline.
51	51	3	Warning	Physical device status changed to Hot Spare.
52	52	3	Warning	Physical device status changed to rebuild.
53	53	3	Warning	Physical device ID did not match.
54	54	3	Warning	Physical device failed to start.
55	55	3	Warning	Physical device negotiated different offset than config.
56	56	3	Warning	Physical device negotiated different bus width than config.
57	57	1	Serious	Physical drive missing on startup.
58	58	3	Warning	Rebuild startup failed due to lower disk capacity.
59	59	3	Warning	Physical drive is switching from a channel to the other channel.
60	60	2	Error	Temporary-Dead physical drive is automatically made online.
61	61	4	Information	A standby rebuild has started.
96	96	1	Serious	Device Loop Id Conflict (Soft Addressing) Detected.
128	128	4	Information	Consistency check is started.
129	129	4	Information	Consistency check is finished.
130	130	4	Information	Consistency check is cancelled.
131	131	2	Error	Consistency check on logical drive error.
132	132	2	Error	Consistency check on logical drive failed.
133	133	4	Information	Consistency check failed due to physical device failure.
134	134	1	Serious	Logical drive has been made offline.
135	135	2	Error	Logical drive is critical.
136	136	4	Information	Logical drive has been placed online.
137	137	4	Information	An automatic rebuild has started on logical drive.

Table #1 - Mylex Error Codes (Sheet 4 of 8)

Gam_ev ent Number	User_ev ent Number	Priority Number	Severity Level	Description
138	138	4	Information	A rebuild has started on logical drive.
139	139	4	Information	Rebuild on logical drive is over.
140	140	4	Information	Rebuild on logical drive is cancelled.
141	141	2	Error	Rebuild stopped with error.
142	142	2	Error	Rebuild stopped with error. New device failed.
143	143	2	Error	Rebuild stopped because logical drive failed.
144	144	4	Information	Logical drive initialization started.
145	145	4	Information	Logical drive initialization done.
146	146	4	Information	Logical drive initialization cancelled.
147	147	2	Error	Logical drive initialization failed.
148	148	4	Information	A logical drive has been found.
149	149	4	Information	A logical drive has been deleted.
150	150	4	Information	Expand Capacity Started.
151	151	4	Information	Expand Capacity Completed.
152	152	2	Error	Expand Capacity stopped with error.
153	153	4	Information	Bad Blocks found.
154	154	4	Information	System drive size changed.
155	155	4	Information	System drive type changed.
156	156	1	Serious	Bad data blocks found. Possible data loss.
157	157	3	Warning	System drive LUN mapping has been written to config.
158	158	1	Serious	Attempt to read data from block that is marked in Bad Data Table
159	159	2	Error	Data for Disk Block has been lost due to Logical Drive problem
160	160	2	Error	Temporary-Offline RAID5/RAID3 array is available to the user again with the possibility of data loss in the array.
161	161	2	Error	Temporary-Offline RAID0+1/RAID1/RAID0/JBOD array is available to the user again.
162	162	4	Information	An standby rebuild has started on logical drive.

Table #1 - Mylex Error Codes (Sheet 5 of 8)

Gam_ev ent Number	User_ev ent Number	Priority Number	Severity Level	Description
256	256	1	Serious	Fan failure.
257	257	4	Information	Fan has been restored.
258	258	1	Serious	Fan failure.
259	259	4	Information	Storage cabinet fan is not present.
272	272	1	Serious	Power supply failure.
273	273	4	Information	Power supply has been restored.
274	274	1	Serious	Power supply failure.
275	275	4	Information	Storage cabinet power supply is not present.
288	288	1	Serious	Over temperature. Temperature is above 70 degrees Celsius.
289	289	3	Warning	Temperature is above 50 degrees Celsius.
290	290	4	Information	Normal temperature has been restored.
291	291	1	Serious	Over temperature.
292	292	4	Information	Storage cabinet temperature sensor is not present.
304	304	1	Serious	Storage Works enclosure reported failure state.
305	305	3	Warning	Storage Works enclosure reported critical state.
306	306	4	Information	Storage Works enclosure reported normal state.
307	307	4	Information	Uninterruptable Power Supply Disabled.
308	308	4	Information	Uninterruptable Power Supply AC Failed.
309	309	3	Warning	Uninterruptable Power Supply Battery Low.
310	310	1	Serious	Uninterruptable Power Supply Failed.
311	311	4	Information	Uninterruptable Power Supply Normal.
320	320	1	Serious	Fan failure.
321	321	4	Information	Fan has been restored.
322	322	4	Information	Fan is not present.
323	323	1	Serious	Power supply failure.
324	324	4	Information	Power supply has been restored.

Table #1 - Mylex Error Codes (Sheet 6 of 8)

Gam_ev ent Number	User_ev ent Number	Priority Number	Severity Level	Description
325	325	4	Information	Power supply is not present.
326	326	1	Serious	Temperature is over safe limit. Failure imminent.
327	327	3	Warning	Temperature is above working limit.
328	328	4	Information	Normal temperature has been restored.
329	329	4	Information	Temperature sensor is not present.
330	330	3	Warning	Enclosure access critical.
331	331	4	Information	Enclosure access has been restored.
332	332	1	Serious	Enclosure access is offline.
333	333	1	Serious	Enclosure Soft Addressing Detected.
334	334	4	Information	Enclosure services ready
384	384	4	Information	Array management server software started successfully.
385	385	2	Error	Write back error.
386	386	3	Warning	Internal log structures getting full, PLEASE SHUTDOWN AND RESET THE SYSTEM IN THE NEAR FUTURE.
388	388	0	Critical	Controller is dead. System is disconnecting from this controller.
389	389	3	Warning	Controller has been reset.
390	390	4	Information	Controller is found.
391	391	0	Critical	Controller is gone. System is disconnecting from this controller.
392	392	4	Information	BBU Present.
393	393	3	Warning	BBU Power Low.
394	394	4	Information	BBU Power OK.
395	395	0	Critical	Controller is gone. System is disconnecting from this controller.
396	396	4	Information	Controller powered on
397	397	4	Information	Controller is online.
398	398	0	Critical	Controller is gone. System is disconnecting from this controller.
399	399	3	Warning	Controller's partner is gone, controller is in failover mode now.
400	400	4	Information	BBU reconditioning is started.

Table #1 - Mylex Error Codes (Sheet 7 of 8)

Gam_ev ent Number	User_ev ent Number	Priority Number	Severity Level	Description
401	401	4	Information	BBU reconditioning is finished.
402	402	4	Information	BBU reconditioning is canceled.
403	403	1	Serious	Installation aborted.
404	404	1	Serious	Controller firmware mismatch.
405	405	3	Warning	BBU removed.
406	406	1	Serious	WARM BOOT failed.
411	411	3	Warning	Controller entered Conservative Cache Mode.
412	412	3	Warning	Controller entered Normal Cache Mode.
413	413	3	Warning	Controller Device Start Complete.
414	414	3	Warning	Soft ECC error Corrected.
415	415	3	Warning	Hard ECC error Corrected.
416	416	1	Serious	BBU Recondition Needed.
417	417	3	Warning	Controller's Partner Has Been Removed.
418	418	2	Error	BBU out of service.
419	419	3	Warning	Updated partner's status.
420	420	3	Warning	Relinquished partner.
421	421	3	Warning	Inserted Partner.
422	422	3	Warning	Dual Controllers Enabled.
423	423	3	Warning	Killed Partner.
424	424	3	Warning	Dual Controllers entered Nexus.
425	425	1	Serious	Controller Boot ROM Image needs to be reloaded.
426	426	0	Critical	Controller is using default non-unique world-wide name.
512	512	4	Information	System started.-
513	513	4	Information	Size table full.-
514	514	4	Information	User logged in.-
515	515	4	Information	User logged out.-

Table #1 - Mylex Error Codes (Sheet 8 of 8)

Gam_ev ent Number	User_ev ent Number	Priority Number	Severity Level	Description
516	516	4	Information	Server alive.
517	517	1	Serious	Lost connection to server, or server is down.
518	518	4	Information	Automatic reboot count has changed.
640	640	3	Warning	Channel Failed.
641	641	3	Warning	Channel Online.
642	642	1	Serious	Back End SCSI Bus Dead.
643	643	4	Information	Back End SCSI Bus Alive.
644	644	1	Serious	Back End Fibre Dead.
645	645	4	Information	Back End Fibre Alive.
700	700	3	Warning	Event Log Empty.
701	701	3	Warning	Event Log Entries Lost.
702	702	3	Warning	Request Sense
703	703	3	Warning	Set Real Time Clock.
800	800	3	Warning	New Configuration Received.
801	801	3	Warning	Configuration Cleared.
802	802	3	Warning	Configuration Invalid.
803	803	3	Warning	Configuration On Disk Access Error.
804	804	3	Warning	Configuration On Disk Converted.
805	805	3	Warning	Configuration On Disk Import Failed.
806	806	4	Information	A Debug Dump exists on this system.
807	807	4	Information	A Debug Dump exists on this system.
896	896	1	Serious	Internal Controller is in the hung state.
897	897	1	Serious	Internal Controller has encountered a Firmware breakpoint.
912	912	1	Serious	Internal Controller has encountered i960 processor specific error.
928	928	1	Serious	Internal Controller has encountered Strong-ARM processor specific error
4294967 295	0	Critical	Unknown	