EMC® VNX™ Series

Release 7.1

VNX™ Glossary

P/N 300-013-501 Rev 01

EMC Corporation
Corporate Headquarters:
Hopkinton, MA 01748-9103
1-508-435-1000
www.EMC.com

Copyright © 1998 -2012 EMC Corporation. All rights reserved.

Published July 2012

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

For the most up-to-date regulatory document for your product line, go to the Technical Documentation and Advisories section on EMC Powerlink.

For the most up-to-date listing of EMC product names, see EMC Corporation Trademarks on EMC.com.

All other trademarks used herein are the property of their respective owners.

Corporate Headquarters: Hopkinton, MA 01748-9103

Contents

Preface.....5

A.....**7**

B.....**13**

C.....**17**

D.....**23**

E.....**31**

F.....**35**

G.....**39**

H.....**41**

I.....**43**

J.....**47**

K.....**49**

L.....**51**

M.....55

N.....59

O.....65

P.....67

Q.....73

R.....75

S.....81

T.....91

U.....95

V.....99

W.....103

X.....105

Z.....107

Special Character.....109

Preface

As part of an effort to improve and enhance the performance and capabilities of its product line, EMC® periodically releases revisions of its hardware and software. Therefore, some functions described in this VNX™ Glossary may not be supported by all revisions of the software or hardware currently in use. For the most up-to-date information on documentation and product features, refer to your product release notes on the EMC® Powerlink® website.

If a product does not function properly or does not function as described in the VNX Glossary, please contact your EMC Customer Support Representative.

Audience

This document is part of the VNX documentation set, and is intended for use by system administrators during installation and setup of the product.

Organization

This is a glossary of network-attached storage (NAS) terminology used in reference to the VNX product line. Terms specific to a particular product are designated as such in the definition.

Where to get help

EMC support, product, and licensing information can be obtained as follows:

Product information — For documentation, release notes, software updates, or for information about EMC products, licensing, and service, go to the EMC Online Support website (registration required) at http://Support.EMC.com.

Troubleshooting — Go to the EMC Online Support website. After logging in, locate the applicable Support by Product page.

Technical support — For technical support and service requests, go to EMC Customer Service on the EMC Online Support website. After logging in, locate the applicable Support by Product page, and choose either **Live Chat** or **Create a service request**. To open a service request through EMC Online Support, you must have a valid support

agreement. Contact your EMC sales representative for details about obtaining a valid support agreement or with questions about your account.

Note: Do not request a specific support representative unless one has already been assigned to your particular system problem.

Your comments

Your suggestions will help us continue to improve the accuracy, organization, and overall quality of the user publications.

Please send your opinion of this document to:

`techpubcomments@EMC.com`

A

access-based enumeration (ABE)
With ABE enabled, Windows will not display files or folders that the user does not have the rights to access. Only those files or folders that the user has the rights to access are visible, thus increasing folder-level security.

access control entry (ACE)
In a Microsoft Windows environment, an element of an access control list (ACL). This element defines access rights to a file for a user or group.

access control levels
Entries in an access control level table created and recognized only in the Control Station database that define the access level allowed for specified administrative users. These entries are used in conjunction with an access control value associated with certain system objects to define administrative user access to VNX for file.

access control list (ACL)
List of access control entries (ACEs) that provide information about the users and groups allowed access to an object.

access policy
Policy that defines which access control methods (NFS permissions or Windows ACLs or both) are enforced when a user accesses a file on VNX for file in an environment configured to provide multiprotocol access to some file systems. The access policy is set with the server_mount command and also determines which actions a user can perform against a file or directory.

access privileges
Extent to which a user may operate a system resource on a network or file server. In many cases, permission to access a server, view its contents, and modify or create files is limited by the network's system administrator to maintain security.

ACE
See access control entry.

ACL
See access control list.

active/active'
For EMC® Symmetrix® Remote Data Facility (SRDF®) or EMC MirrorView™/Synchronous configurations, a bidirectional configuration with two production sites, each acting as the standby for the other. Each VNX for file has both production and standby Data Movers. If one site fails, the other site takes over and serves the clients of both sites. For SRDF, each Symmetrix system is partitioned into source (production) and remote destination volumes. For MirrorView/S, each VNX for block is configured to have source and destination LUNs and a consistency group.

Active Directory (AD)
Advanced directory service included with Windows operating systems. It stores information about objects on a network and makes this information available to users and network administrators through a protocol such as Lightweight Directory Access Protocol (LDAP).

Active Directory Users and Computers (ADUC)
Administrative tool designed to perform day-to-day Active Directory administration tasks. These tasks include creating, deleting, modifying, moving, and setting permissions on objects stored in the directory. These objects include organizational units, users, contacts, groups, computers, printers, and shared file objects.

active NDMP backup/restore streams
The number of NDMP backup or restore streams that are currently active.

active/passive
For SRDF or MirrorView/S configurations, a unidirectional setup where one VNX for file, with its attached system, serves as the source (production) file server and another VNX for file, with its attached storage, serves as the destination (backup). This configuration provides failover capabilities in the event that the source site is unavailable. An SRDF configuration requires Symmetrix systems as backend storage. A MirrorView/S configuration requires specific VNX for block series systems as backend storage.

active replication session
Replication session that is transferring the delta from source to destination site.

adapter card
Circuit board that provides the physical interface between devices.

adaptive copy disk-pending mode
SRDF mode of operation in which write tasks accumulate in global memory on the local system before being sent to the remote system. This mode allows the primary and secondary volumes to be more than one I/O out of synchronization. The maximum number of I/Os that can be out of sychronization is defined using a maximum skew value.

adaptive copy write-pending mode
SRDF mode of operation in which write tasks accumulate on the primary volume rather than in global memory. A background process destages write tasks to the corresponding destination volumes. Disk mode consumes less global memory, however, transfers are typically slower due to reads coming from disk instead of memory.

Address Resolution Protocol (ARP)
Protocol that translates IP addresses to MAC addresses.

administrative shares
Microsoft term for c$, d$, and so forth that is the automatically shared root level of the file system. Windows maintains default administrative shares that are created for Windows partitions and other system folders. The shares have a dollar sign ($) suffix, are invisible to network browsing, and are only accessible to accounts with administrator, backup operator, or server operator privileges on the particular system.

ADS
See Alternate data stream.

Advanced Encryption Standard (AES)
Advanced Encryption Standard (AES) is a symmetric key encryption standard comprising of three block ciphers. Each cipher has a 128-bit block size, with key sizes of 128, 192, and 256 bits, respectively. AES has replaced DES as the US government's cryptographic standard.

ADUC
See Active Directory Users and Computers.

agent
Software executable that performs specific actions, often in concert with other system software.

alert
In Unisphere™ software, a system event that requires administrative attention. These events may be severe enough to cause a system error or disrupt user access.

Alternate data stream (ADS)
Alternate data stream allows files to be associated with more than one data stream. For example, a file such as text.txt can have an ADS with the name of text.txt:secret (of form filename:streamname) that can only be accessed by knowing the ADS name or by specialized directory browsing programs.

append-only state
State of a file when the data in it cannot be modified, but the file can have new data appended to the end of it. In addition, the file itself cannot be deleted. Once a file in the append-only state has been written to, changing it to the locked state by making it read-only locks it into that state until its retention date has passed.

API
See application programming interface.

application programming interface (API)
Mechanism used to communicate between programs. One program uses the function calls in the API of another program to access its operations.

ARP
See Address Resolution Protocol.

ASCII (American Standard Code for Information Interchange)
7-bit (one byte) character-encoding scheme for representing text and controlling printers and computer communication based on the ordering of the English alphabet. US-ASCII was the most commonly used character encoding on the Internet until it was recently surpassed by UTF-8. ASCII was incorporated into the Unicode character set as the first 128 symbols, so the ASCII characters have the same numeric codes in both sets.

asymmetric cipher
Asymmetric key algorithm is used to generate key pairs for authentication.

See also *public key encryption*.

authentication
Process for verifying the identity of a user trying to access a resource, object, or service, such as a file or a directory.

authorization
Process of granting access permission to a system resource to a user based on their identity. For example, grant a user backup administration privileges.

automated backup and restore
Procedure in which a remote backup server running NDMP-compliant backup software backs up data to a tape library unit (TLU).

See also *local backup* and *remote backup*.

automatic file system extension
Configurable file system feature that automatically extends a file system created or extended with AVM when the high water mark (HWM) is reached.

See also *high water mark*.

Automatic Volume Management (AVM)
Feature of VNX for File that creates and manages volumes automatically without manual volume management by an administrator. AVM organizes volumes into storage pools that can be allocated to file systems.

See also *thin provisioning*.

AV engine
Third-party antivirus software running on a Windows Server that works with the Common AntiVirus Agent (CAVA).

See also *AV server*, *CAVA*, *VC client*, and *virus definition file*.

AVM
See Automatic Volume Management.

AV server
Windows Server configured with the CAVA and a third-party antivirus engine.

See also *AV engine*, *CAVA*, and *VC client*.

AV user

Specific domain user either created or selected as the account configured for the virus checking. Use this account when configuring all of the Windows Servers with CAVA and the AV engine.

B

backplane
Interconnecting device that may or may not have intelligence, but usually has sockets into which circuit boards are plugged.

backup and restore
Technique for ensuring file system integrity and security by backing up to tape or disk a file system or incremental changes to a file system. This data can be restored later.

backup domain controller (BDC)
Windows NT domain controller that has the same database as the primary domain controller (PDC) and may replace the PDC if needed.

bandwidth
Maximum amount of data that can be transmitted through a data channel per unit of time. Usually expressed in megabytes per second.

bandwidth aggregation
See Ethernet channel.

bandwidth schedule
List of time periods (days and hours) and bandwidth values (in KB/s) that control the amount of bandwidth available for a given Data Mover interconnect.

baseline checkpoint
Read-only checkpoint from which a writeable checkpoint is created.

basic input-output system (BIOS)
Essential set of routines stored on a chip. It provides a standard interface between the operating system and vendor-specific hardware.

battery backup unit
VNX for file cabinet component that provides 3 minutes of battery power to the cabinet during a power outage.

BCV
See business continuance volume.

BDC
See backup domain controller.

bitmap
Software register that tracks if a Production File System (PFS) block has changed since the latest checkpoint was created.

See also *Production File System*.

BIOS
See basic input-output system.

blade
See Data Mover.

blockmap
Data structure that maps the older PFS volume block saved to the SavVol block. Each checkpoint has a blockmap and is pageable to the SavVol from the Data Mover memory.

See also *Production File System* and *PFS*.

Blowfish
A public domain symmetric block cipher, used by OpenSSH.

blockmap index file
On-disk representation of a checkpoint's blockmap stored with each checkpoint on the SavVol.

blocks
Units of storage (8 KB each) that comprise a file system.

BoxMonitor
Component of VNX for file Control Station that supports the high-availability feature by monitoring the system hardware components to detect their presence and current state or their absence.

bridge
Device that provides a nonswitching connection between two or more local area networks (LANs).

broadcast
Data frame or packet transmitted to every node on the local network segment.

broadcast domain
Group of entities on the network able to communicate with one another without going through a router.

Browse Master
Microsoft Windows service that gathers and organizes the list of computers and domains displayed in Network Neighborhood. The Browse Master maintains an up-to-date list of network resources and provides this information to other network computers.

browser
Program used to access information over the Internet or an intranet.

b/s
Bits per second (b/s).

B/s
Bytes per second (B/s).

buffer
Storage area used for handling data in transit. Buffers compensate for differences in processing speed between source and destination.

bundle
See Ethernet channel.

business continuance volume (BCV)
Symmetrix volume used as a mirror that attaches to and fully synchronizes with a production (source) volume on the VNX for File. The synchronized BCV is then separated from the source volume and is addressed directly from the host to serve in backup and restore operations, decision support, and application testing.

C

cache
Temporary storage used to retain frequently used data for faster access. For example, a memory cache may be used between a CPU and main memory.

CallHome
VNX for file uses its telephone modem to automatically notify EMC or your service provider when certain problems are detected. Problems that trigger a CallHome include hardware failures, high temperature in the cabinet, and some software errors.

CAVA
See Common AntiVirus Agent.

CAVA Calculator
Tool that estimates the number of CAVAs required to provide a user-defined level of performance in a CAVA pool, based on user information. The tool can be run at any time, even if CAVA is not present.

CAVA sizing tool
Program that monitors all CAVAs in the network, and sizes the network to find the ideal number of AV servers. When you install CAVA on the AV servers, the CAVA sizing tool, cavamon.exe, is also installed.

CDB
See command descriptor block.

Celerra Monitor
Java client/server application that lets an administrator observe the performance of a system attached to VNX for file and the performance of any Data Movers mounted in VNX for file cabinet.

CEPA
See Common Event Publishing Agent.

CEPA API
Mechanism used by consumer applications to register for, receive, and act on events taking place in the CIFS file systems.

Certificate Authority (CA)
Trusted third-party that creates and digitally signs public key certificates.

Certificate Authority Certificate
Digitally signed association between an identity (Certificate Authority) and a public key to be used by the host to verify digital signatures on public key certificates.

CGI
See Common Gateway Interface.

Challenge Handshake Authentication (CHAP)
Access control protocol for secure authentication by using shared passwords called secrets.

channel director
Component in a Symmetrix system that connects the host channels and data storage. It transfers data between the channel and cache.

CHAP
See Challenge Handshake Authentication Protocol.

character encoding
The mapping from a coded character set to a sequence of bits.

character set
Set of characters used by a language (ANSI/ASCII or Unicode). The character set affects file format (how the software stores and transmits data) and string processing (the logic with which text is manipulated).

checkpoint
Point-in-time, logical image of a PFS. A checkpoint is a file system and is also referred to as a checkpoint file system or an EMC SnapSure™ file system.

See also *Production File System.*

checkpoint application
Business application that reads a checkpoint for point-in-time information about a PFS. Checkpoint applications require point-in-time data, but not realtime data.

See also *Production File System*.

checkpoint audit
Process of monitoring the SavVol to determine how much free space remains for capturing checkpoint data. By default, SnapSure automatically audits the SavVol and writes a message to the system log when the SavVol's high water mark (HWM) is reached.

checkpoint refresh
Process of recycling the SavVol space by deleting a PFS checkpoint data and creating a new checkpoint by using the same checkpoint filename, file system identification number, and mount state.

checkpoint restore
Process of restoring a PFS to a point in time by using a checkpoint. As a precaution, SnapSure automatically creates a new checkpoint of the PFS before it performs a restore operation.

See also *Production File System*.

Checkpoint Virtual File System (CVFS)
File system that allows an NFS or a CIFS client read-only access to online snapshots of a file system directory by accessing a virtual .ckpt directory entry. CVFS and SVFS are synonymous terms.

checkpoint window
Length of time a checkpoint is active, beginning when the checkpoint is created and ending when the checkpoint's SavVol is full or the checkpoint is deleted.

CIFS
See Common Internet File System.

CIFS server
Logical server that uses the CIFS protocol to transfer files. A Data Mover can host many instances of a CIFS server. Each instance is referred to as a CIFS server.

CIFS service
CIFS server process that is running on the Data Mover and presents shares on a network as well as on Microsoft Windows-based computers.

CLEAN state
See *not locked state*.

CLI
See command line interface.

client
Front-end device that requests services from a server, often across a network.

clock offset
Difference between the local system time and the time retrieved from the time server.

command descriptor block (CDB)
SCSI term for a fixed block of data transmitted as a single entity. A CDB is a SCSI packet.

command line interface (CLI)
Interface for typing commands through the Control Station to perform tasks that include the management and configuration of the database and Data Movers and the monitoring of statistics for VNX for file cabinet components.

Common AntiVirus Agent (CAVA)
Application developed by EMC that runs on a Windows Server and communicates with a standard antivirus engine to scan CIFS files stored on VNX for file.

See also *AV engine*, *AV server*, and *VC client*.

common base
Internal checkpoint that is common on both replication source and destination site and is used as a base in the next differential data transfer.

Common Event Publishing Agent (CEPA)
EMC-provided agent running on a Windows Server that provides details of events occurring on the Windows Server. It can communicate with VNX for file to display a list of events that occurred.

Common Gateway Interface (CGI)
Standard for interfacing an external application with an information server, such as HTTPS.

Common Internet File System (CIFS)
File-sharing protocol based on the Microsoft Server Message Block (SMB). It allows users to share file systems over the Internet and intranets.

component file system
File system mounted on the nested mount root file system that is part of the nested mount file system.

configured replication session
Replication session that is idle, active, or inactive. A stopped replication session is not a configured session.

ConnectHome
CallHome file delivery system with multitransport and failover support.

connection database
Database of secondary storage connection information that includes the server name, share, and credentials, which are stored on the file and maintained across system reboots.

connectivity
Ability of hardware devices or software to communicate with other hardware or software.

Consistency group
A logical entity that comprises a collection of replication sets grouped together to ensure write order consistency across all the replication sets' primary volumes. Consistency groups are used to configure protection policies, and set RPO and RTO policies according to specific resource allocation and prioritization. They are also used to fail over to, recover production from, and test any replica defined in the group.

Control Station
Hardware and software component of VNX for file that manages the system and provides the user interface to all VNX for file components.

coordinated universal time (UTC)
Formerly Greenwich Mean Time (GMT), UTC is the international time standard.

CRC
See Cyclic Redundancy Check.

CRU
See customer-replaceable unit.

cumulative incremental backup
Backup that copies all data modified since the last full backup. To restore data when cumulative incremental backups are in use, you need only the latest full and cumulative incremental backups.

See also *differential backup*, *differential incremental backup*, *full backup*, and *incremental backup*.

customer-replaceable unit (CRU)
On VNX for block, hardware a customer can add or replace while the disk-array enclosure (DAE) is powered up. Examples of CRUs include power supplies and drive fan packs. These components are also known as field-replaceable units (FRUs).

CVFS
See Checkpoint Virtual File System.

Cyclic Redundancy Check (CRC)
Method used to perform additional error checking on the data sent over a Data Mover interconnect to ensure data integrity and consistency. A CRC is a type of hash function used to produce a checksum, a small fixed number of bits, against a block of data transferred to a remote site. The checksum is used to detect errors after transmission. A CRC is computed and appended before transmission and verified afterwards to confirm that no changes occurred on transit.

D

DACL
See discretionary access control list.

DAD
See Duplicate Address Detection.

DAE2
See disk-array enclosure.

daemon
UNIX process that runs continuously in the background, but does nothing until it is activated by another process or triggered by a particular event.

DAR
See direct access restore.

DART
See data access in real time.

DASD
See direct access storage device.

data access in real time (DART)
On VNX for file, the operating system software that runs on the Data Mover. It is a realtime, multithreaded operating system optimized for file access, while providing service for standard protocols.

data availability
Access to any and all user data by an application.

data element
An attribute in VNX for file derived from a string.

Data Encryption Standard (DES)
Commonly used algorithm for encrypting and decrypting data.

Data Mover
In VNX for file, a cabinet component that is running its own operating system that retrieves data from a storage device and makes it available to a network client. This is also referred to as a blade.

Data Mover Enclosure (DME)
In VNX for file, a shelf that includes an enclosure, one or two Data Movers, management modules, and power and cooling modules.

Data Mover failover
Process started when an active Data Mover fails. The Control Station activates the failing Data Mover's standby replacement, if one is configured. The standby Data Mover takes the identity of the failed Data Mover and continues processing requests. If a Data Mover has multiple standbys, it will fail over only once from production to a standby. If the standby fails, it will not fail over to another standby. Multiple active Data Movers can be associated with a single standby Data Mover.

database management system (DBMS)
Software designed to manage databases. Data Movers use DBMS to create and manage Usermapper and secmap mapping information.

datagram
Unit of data or packet transmitted in a TCP/IP network. A datagram contains source and destination addresses and data.

DBMS
See database management system.

DDAR
See directory DAR.

DDS
See dynamic drive sharing.

deduplication
Process used to compress redundant data, which allows space to be saved on a file system. When multiple files have identical data, the file system stores only one copy of the data and shares that data between the multiple files. Different instances of the file can have different names, security attributes, and timestamps. None of the metadata is affected by deduplication.

default CIFS server
CIFS server created when you add a CIFS server and do not specify any interfaces (with the interfaces= option of the server_cifs -add command). The default CIFS server uses all interfaces not assigned to other CIFS servers on the Data Mover.

delta
For Replication (V2), block changes to the source object, as calculated by comparing the newest, currently marked internal checkpoint (point-in-time snapshot) against the previously replicated internal checkpoint. Replication transfers these changes and applies them immediately to the destination object, then refreshes the latest destination internal checkpoint.

delta set
For SRDF/Asynchronous (SRDF/A), a predetermined cycle of operation used for asynchronous host writes from a source to a destination. Each delta set contains groups of I/Os for processing. The ordering of these I/Os is managed for consistency. For VNX Replicator™, a set contains the block modifications made to the source file system that VNX Replicator uses to update the destination file system (read-only, point-in-time, consistent replica of the source file system). The minimum delta-set size is 128 MB.

demote
To unmount a snapshot from an iSCSI LUN. Upon demotion, the LUN is inaccessible and changes made to the LUN while in a promoted state are lost.

dependent write consistency
For SRDF/A, the maintenance of a consistent point-in-time replica of data between a source and destination through the processing and preservation of all writes to the destination in ordered, numbered delta sets.

DES
See Data Encryption Standard.

destination address
Hostname or IP address of the machine to which data is being sent.

destination VNX for file
Term for the remote (secondary) VNX for file in an SRDF or MirrorView/S configuration. The destination VNX for file is typically the standby side of a disaster recovery configuration. Symmetrix configurations often call the destination VNX for file: the target VNX for file.

device
Two types of devices are physical (port) and virtual.

See also *virtual device*.

device driver
Software component that provides the interface between a hardware device and the operating system.

device prefix
Indication of the type of network controller installed in VNX for file.

DFS
See Microsoft Distributed File System.

DHCP
See dynamic host configuration protocol.

diagnostics
System tests or firmware designed to inspect, detect, and correct failing components. These tests are comprehensive and self-invoking.

differential backup
Backup that copies all data modified since the last full backup. To restore data when differential backups are in use, you need only the latest full backup and the latest differential backups.

See also *cumulative incremental backup*, *differential incremental backup*, *full backup*, and *incremental backup*.

differential copy
The difference between the common base and the object that needs to be copied. Only the delta between the common base and the source object is transferred to the destination.

differential incremental backup
Backup that copies data objects modified since the last full backup or incremental backup. To restore data when differential incremental backups are in use, the newest full backup and all subsequent differential backups are required.

See also *cumulative incremental backup*, *full backup*, and *incremental backup*.

Diffie-Hellman key exchange (DH)
A key exchange algorithm.

digest
iSCSI protocol error-checking method used to verify the integrity of an iSCSI packet header (header digest) or payload data (data digest) by using a checksum.

Digest Access Authentication
Means of verifying that the client and server possess a shared secret (a password).

digital certificate
Electronic ID issued by a certificate authority that establishes a user's credentials. It contains the user's identity (a hostname), a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signatures), and a digital signature from the certificate-issuing authority so that a recipient can verify that the certificate is valid.

Digital Signature Algorithm (DSA)
A digital signature standard.

Digital Signature Standard (DSS)
The original version of DSA.

See also *Digital Signature Algorithm.*

direct access restore (DAR)
Data recovery operation that allows the NDMP client to directly access backed-up data anywhere in a tape set without having to traverse the tape set sequentially.

direct access storage device (DASD)
Peripheral device that is directly addressable, such as a disk or drum. Typically used in a mainframe environment.

director
Component in a Symmetrix system that allows it to transfer data between the host channels and disk drives.

See also *channel director* and *disk director*.

directory database
See SAM.

directory direct access restore (DDAR)
Improved form of DAR that supports directory-level DAR by restoring all the content under the directory.

directory server
Server that stores and organizes information about a computer network's users and network resources, and that allows network administrators to manage users' access to the resources. X.500 is the best-known open directory service. Proprietary directory services include Microsoft's Active Directory.

disaster recovery
Preventive measures using redundant hardware, software, data centers, and other facilities to ensure a business can continue operations during a natural or man-made disaster and if not, to restore business operations as quickly as possible afterward.

discretionary access control list (DACL)
User-specified (as opposed to system- or administrator-specified) functions.

disk-array enclosure (DAE2)
Shelf in VNX for block that includes an enclosure, up to 15 disk modules, one or two Fibre Channel link control cards (LCCs), and one or two power supplies, but does not contain storage processors (SPs).

disk director
Component in the Symmetrix system that interfaces between the cache and the disk drives.

disk drive
Physical disk or logical device in a storage subsystem viewed by the client systems as a physical disk.

disk group
Set of NS600 disk drives from which a disk volume is created. The type of a disk group is specified by its storage profile.

diskmark
On VNX for file, a disk identification number.

disk processor enclosure (DPE2)
Shelf in VNX for block that includes an enclosure, disk modules, storage processors (SPs), Fibre Channel link control cards (LCCs), two power supplies, and fan packs. A DPE supports DAEs in addition to its own disk modules.

disk volume
On a VNX for File, a physical storage unit as exported from the storage system. All other volume types are created from disk volumes.

See also *metavolume*, *slice volume*, *stripe volume*, and *volume*.

DME
See Data Mover Enclosure.

DNFS
Oracle Direct NFS, a new feature in Oracle Database 11g, integrates the NFS client directly with the Oracle software.

DNS
See Domain Name System.

domain
Logical grouping of Microsoft Windows Servers and other computers that share common security and user account information. All resources such as computers and users are domain members and have an account in the domain that uniquely identifies them. The domain administrator creates one user account for each user in the domain, and the users log in to the domain once. Users do not log in to each individual server.

domain controller
Server that authenticates user logins and maintains the security policy and the security account's master database for a Windows domain. Domain controllers manage user access to a network, which includes logging in, authentication, and access to the directory and shared resources.

See also *Windows domain*.

Domain Name System (DNS)
Name resolution software that allows users to locate computers on a UNIX network or TCP/IP network by domain name. The DNS server maintains a database of domain names, hostnames, and their corresponding IP addresses, and services provided by the application servers.

See also *ntxmap*.

DPE2
See disk processor enclosure.

dual-initiator
Symmetrix system feature that automatically creates a backup data path to the disk drives serviced directly by a disk director, should that disk director or the disk management hardware for those devices fail.

dump
Backup format in PAX that traverses a file tree in mixed width-first and depth-first order.

Duplicate Address Detection (DAD)
Means of determining if a new address is unique to the network.

dynamic drive sharing (DDS)
Feature of NDMP-compliant backup software that allows NDMP servers to share tape drives.

dynamic host configuration protocol (DHCP)
Software that automatically assigns temporary IP addresses to client stations logging in to a TCP/IP network. It eliminates having to manually assign permanent IP addresses.

dynamic load balancing
Distributes an I/O workload over all paths that different devices share.

See also *load balancing* and *static load balancing*.

dynamic sparing
Symmetrix system feature that automatically transfers data from a failing disk drive to an available spare disk drive without affecting data availability. This feature supports all nonmirrored devices in the Symmetrix subsystem.

E

EDM
See EMC Data Manager.

EMC ControlCenter
Enterprise management software that allows an administrator to manage Symmetrix systems and other heterogeneous systems in an enterprise network.

EMC Data Manager (EDM)
Combination of software, hardware, and services that provides high-speed, centralized backup and restore systems for enterprise-class data centers, optimized for Symmetrix and Windows database environments.

emergency power-off box (EPO box)
Component in VNX for file cabinet that contains six circuit breakers, one for each power supply.

encoding
Mapping of individual characters in a character set to the specific bits used to represent the data (used in protocol messages and how they are stored on disks).

See also *Unicode* and *UTF-8*.

encryption
Encoding data so it is readable only by specific users. Encrypted data is decoded by using a special algorithm called a decryption key.

enterprise storage
Combination of intelligent systems, software, and services that together enable an enterprise to store, retrieve, manage, protect, and share information from all major computing environments, including UNIX, Windows, and mainframe platforms.

Enterprise Storage Network (ESN)
Combination of intelligent systems, software, and services. These products and services together enable an enterprise to store, retrieve, manage, protect, and share information from all major computing environments, including UNIX, Windows, and mainframe platforms.

EPO box
See emergency power-off box.

ESN
See Enterprise Storage Network.

EtherChannel
See Ethernet channel.

Ethernet
Local area network (LAN) technology that transfers packets ranging from 48 bytes to 9000 bytes. Ethernet uses a media access method that listens before transmitting to minimize packet collisions. Cable media and interface connectors supported on VNX for file include:

Network type	Cable media and interface connectors
10Base2	10 Mb/s, thin-wire coaxial cable with BNC interface (up to 200 m)
10Base5	10 Mb/s, thick-wire coaxial cable (up to 500 m)
10BaseT	10 Mb/s, hub (star) topology with twisted-pair drop cables and RJ-45 interface
10BaseF	10 Mb/s, hub topology with optical fiber drop cables
100BaseTX (Fast Ethernet)	100 Mb/s, two pairs of Category 5 unshielded twisted pair (UTP) cable
1000BaseSX (Gigabit Ethernet)	1 Gb/s, optical fiber cables (up to 550 m)

Ethernet channel
High-availability feature that enables multiple active Ethernet connections to the same switch to appear as a single link with a single MAC address and potentially multiple IP addresses.

EUC (Extended UNIX Code)
Multibyte character encoding system used primarily to represent Japanese, Korean, and Simplified Chinese. The main alternatives to EUC encoding are JIS and more recently Unicode, particularly in the form of UTF-8.

EUI
See extended unique identifier.

event
System-generated message caused by a command, an error, or other condition that may require action by an administrator. Events are typically written to an event log, and may trigger an event notification.

event log
File of system-generated messages based on meeting a condition of a particular severity level. There are separate event logs for the Control Station and for each physical and virtual Data Mover in the system.

event notification
Process by which specified events meeting a severity threshold trigger an action or notification.

See also *notifications*.

exclude file
Related to File Migration Service. Lists files and directories that should not migrate from the source file server. Entries are removed on the Migration File System (MGFS). All other files are migrated in an online state.

expired state
State of a file when its retention date has passed. A file in the expired state can be reverted back to the locked state or deleted from the FLR-enabled file system, but cannot be altered.

export
File system or directory made available to NFS users on the network, or the process of making a file system or directory available to NFS users on the network.

export mask
Masking of an NFS export to give access to only the user-specified hosts.

extended ACL
Container used to store extended attributes. In VNX FileMover system, extended ACLs are used to back up and restore stub files through a CIFS network backup.

extended unique identifier (EUI)
IEEE naming standard supported by the iSCSI protocol. The format of EUI names is eui. followed by an EUI-64 identifier.

Extensible Markup Language (XML)
Standards-based language intended to represent structured information.

extent
Set of adjacent physical blocks.

F

fabric
Fibre Channel topology structured with one or more switching devices that interconnect Fibre Channel N_Ports and route Fibre Channel frames.

facility
Component of VNX for file that monitors the system and generates an event when a certain condition is detected.

failover
Process of immediately routing data to an alternate data path or device to avoid interrupting services in the event of a failure. The impact to service is dependent on the application's ability to handle the change gracefully.

Fail-Safe Network (FSN)
High-availability feature that extends link failover out into the network by providing switch-level redundancy. A FSN appears as a single link with a single MAC address and potentially multiple IP addresses.

fallthrough
Fallthrough occurs when MPFS temporarily employs the NFS or CIFS protocol to provide continuous data availability, reliability, and protection while block I/O path congestion or unavailability is resolved. This fallthrough technology is seamless and transparent to the application being used.

Fast Ethernet
Any Ethernet specification with a speed of 100 Mb/s. Based on the IEEE 802.3u specification.

FAT
See File Allocation Table.

FBI
See Fibre Backend Isolation.

FC4700
See VNX for block.

FC-AL
See Fibre Channel Arbitrated Loop.

FC-SW
See Fibre Channel Switch Fabric.

fiber optics
Communications systems that use optical fiber cables, which are composed of thin glass strands designed for transmitting light.

Fibre Backend Isolation (FBI)
Feature used to help diagnose disk drive problems on VNX for block.

Fibre Channel
Nominally 1 Gb/s data transfer interface technology, although the specification allows data transfer rates from 133 Mb/s up to 4.25 Gb/s. Data can be transmitted and received simultaneously. Common transport protocols, such as Internet Protocol (IP) and Small Computer Systems Interface (SCSI), run over Fibre Channel. Consequently, a single connectivity technology can support high-speed I/O and networking.

Fibre Channel Arbitrated Loop (FC-AL)
Standard for a shared access loop, in which a number of Fibre Channel devices are connected (as opposed to point-to-point transmissions). Requires a port to successfully negotiate to establish a circuit between itself and another port on the loop.

Fibre Channel Class 1 Service
Dedicated, uninterruptible connection designed for time-critical, continuous, dedicated connections.

Fibre Channel Class 2 Service
Connectionless, packet-switched service with guaranteed delivery and confirmed receipt of traffic.

Fibre Channel Class 3 Service
Connectionless service similar to packet-switched systems such as Ethernet in which the path between two devices is not reserved or dedicated. Similar to Class 2, but without delivery guarantee or confirmation mechanism. An American National Standards Institute (ANSI) standard.

Fibre Channel Switch Fabric (FC-SW)
Fibre Channel network standard where nodes are connected to a fabric topology implemented by one or more switches. Each node's N_Port connects to an F_Port on a switch. Pairs of nodes connected to an FC-SW network can communicate concurrently.

field-replaceable unit (FRU)
Component replaced or added by service personnel as a single entity.

See also *CRU*.

File Allocation Table (FAT)
File system used by MS-DOS and other Windows-based operating systems to organize and manage files. The file allocation table (FAT) is a data structure that Windows creates when you format a volume by using the FAT or FAT32 file systems. Windows stores information about each file in the FAT so that it can retrieve the file later.

file-level retention (FLR)
FLR lets you store data on standard rewritable magnetic disks by using NFS or CIFS operations to create a permanent, unalterable set of files and directories.

See also *append-only state*, *expired state*, *locked state*, *not locked state*, and *retention date*.

File Mapping Protocol (FMP)
File system protocol used to exchange file layout information between an application server and VNX for file.

See also *MPFS*.

file server
Computer system that is optimized to serve files to clients. A file server does not run general purpose applications. VNX for file refers to the complete system, which includes several Data Movers and other components. The blocks of data that make up the files served to clients are stored on the system.

file storage object
File created on an UxFS file system that provides the storage space for an iSCSI LUN.

file system
Method of cataloging and managing the files and directories on a system.

file system name
Unique identifier for a file system on VNX for file. There can be only one file system with a particular name across all the Data Movers on the system.

See also *share name*.

file system quota
Configurable file system usage limit on the amount of data or the number of files created on a file system, or the amount of data stored in a directory tree.

File Transfer Protocol (FTP)
High-level protocol for transferring files from one machine to another. Implemented as an application-level program based on the OSI model, FTP uses the TCP protocol.

filter file
File that specifies the types of files to filter and the share on which files are filtered.

filtering for NDMP
Backup feature that allows administrators to specify using environmental variables in the qualified backup vendor's software, which directories and files within a file system to exclude from the backup.

FLARE
Embedded operating system in VNX for block disk arrays.

FLR
See file-level retention.

FLR clock
Non-modifiable, per file system clock used to track the retention date. It is initialized when an FLR-enabled file system is mounted read/write on a Data Mover. It does not advance when a file system is unmounted or mounted read-only.

FLR state
See *locked state*.

FMP
See File Mapping Protocol.

FQDN
See fully qualified domain name.

frame
In communications, a fixed data block transmitted as a single entity. In local area networks (LANs), the terms frame and packet are used synonymously.

See also *packet*.

frame tagging
Information added to a frame so the receiving device can identify the virtual local area network (VLAN) to which it belongs. IEEE 802.3q is a frame-tagging standard.

framework
Set of procedures, rules, and mechanisms for the development of an interface to multiple instances of a type of system facility or component.

FRU
See field-replaceable unit.

FSN
See Fail-Safe Network.

FTP
See File Transfer Protocol.

full backup
Backup that copies a defined set of data, regardless of whether it has changed since the last backup. A full backup is the basis from which incremental backups are taken.

See also *cumulative incremental backup*, *differential incremental backup*, and *incremental backup*.

fully qualified domain name (FQDN)
Full name of a system, which contains the domain name of the organization and its highest subdomain.

gatekeeper
Logical disk used as a buffer between VNX for file and the Symmetrix system for the exchange of management commands and data.

gateway
VNX for file that is capable of connecting to multiple systems, either directly (direct-connected) or through a Fibre Channel switch (fabric-connected).

gateway address
Host or IP address of the gateway machine through which network traffic is routed.

GID
See group identifier.

gigabit (Gb)
10^9 bits, defined as 2 to the 30th power (1,073,741,824) bits. One gigabit is equal to 1,024 megabits.

Gigabit Ethernet
Any Ethernet specification with a speed of 1000 Mb/s. IEEE 802.3z defines Gigabit Ethernet over fiber and cable, which has a physical media standard of 1000Base-X (1000Base-SX short wave, 1000Base-LX long wave) and 1000Base-CX shielded copper cable. IEEE 802.3ab defines Gigabit Ethernet over an unshielded twisted pair (1000Base-T).

gigabyte (GB)
10^9 bytes, defined as 2 to the 30th power (1,073,741,824) bytes. One gigabyte is equal to 1024 megabytes.

global group
In Windows NT, a global group contains only individual user accounts (no groups) from the domain in which it is created. Once created, a global group can be assigned permissions and rights, either in its own domain or in any trusting domain.

globalization (G11N)
The process of internationalizing and localizing software.

GPO
See Group Policy Objects.

graphical user interface (GUI)
Software that uses graphical objects such as pull-down menus and operations such as drag-and-drop to allow the user to enter commands and execute functions.

group identifier (GID)
Numeric identifier assigned to a particular group of users.

Group Policy Objects (GPO)
In Windows operating systems, administrators can use Group Policy to define configuration options for groups of users and computers. Windows Group Policy Objects can control elements such as local, domain, and network security settings.

GUI
See graphical user interface.

H

hard quota
Configurable file system usage limit that, when reached, can cause the system to generate an event or message and immediately deny user requests that would require more disk space, such as creating or saving of files.

See also *quota* and *soft quota*.

hash
Cryptographic hash functions are used in digital signatures for authentication.

HBA
See host bus adapter.

high water mark (HWM)
Trigger point at which the VNX for File performs one or more actions, such as sending a warning message, extending a volume, or updating a file system, as directed by the related feature's software/parameter settings.

home directory
Special directory reserved for a particular user, it contains files and programs for the user. In a Windows environment, the home directory is often specified in a user's profile so that upon login, the home directory is automatically assigned to a network drive.

host
Addressable end node capable of transmitting and receiving data.

host bus adapter (HBA)
Interface card on a Data Mover used to access a storage device, comprising hardware and loaded microcode.

hostname
Name of a computer on a network.

HTML
See Hypertext Markup Language.

HTTP
See Hypertext Transfer Protocol.

HTTPS
See Hypertext Transfer Protocol Secured.

hub
Central connecting device that joins communication lines together in a star configuration.

HWM
See high water mark.

hyper
Hypervolume.

See also *metavolume*.

Hypertext Markup Language (HTML)
Document format used on the World Wide Web.

Hypertext Transfer Protocol (HTTP)
Communications protocol used to connect to servers on the World Wide Web.

Hypertext Transfer Protocol Secured (HTTPS)
HTTP over SSL. All network traffic between the client and server system is encrypted. In addition, there is the option to verify server and client identities. Server identities are typically verified and client identities are not.

Hypertext Transfer Protocol (HTTP)
Communications protocol used to connect to servers on the World Wide Web.

Hypertext Transfer Protocol Secured (HTTPS)
HTTP over SSL. All network traffic between the client and server system is encrypted. In addition, there is the option to verify server and client identities. Server identities are typically verified and client identities are not.

I

I18N
An abbreviation for internationalization (I + 18 letters + N).

See internationalization.

ICMP
See Internet Control Message Protocol.

Identity Management for UNIX (IdMU)
Microsoft software that provides a UNIX environment on Windows, specifically UNIX identity and security services.

idle replication session
Replication session that is configured but is not transferring data from the source site to the destination site.

IdMU
See Identity Management for UNIX.

inactive replication session
Replication session that experiences a fatal error. User must stop or delete the replication session to continue.

include file
Related to File Migration Service. Lists high-priority files on all drives from the source file server that should be migrated before all other files. Files are migrated in an online state. All other files remain in an offline state. Listed entries cannot be a directory.

incremental backup
Term that encompasses both cumulative incremental backups and differential incremental backups. Any backup that copies only data objects modified since the time of some previous backup.

See also *cumulative incremental backup*, *differential incremental backup*, and *full backup*.

initial copy
Full copy of the source data from the source site to the destination site.

initialization
The process of creating the original baseline copy of a source object for the purpose of establishing a replication. The baseline copy is then either transported over the network (the default behavior) or physically by tape or disk from the source site to the destination site.

See also *silvering*.

inode
"On-disk" data structure that holds information about files in a file system. This information identifies the file type as being a file that includes VNX FileMover stub files, a directory, or a symbolic link.

interconnect
Communication path between a given Data Mover pair located on the same VNX for file cabinet or different cabinets.

interface (network)
Named logical element mapped to a physical network connection, or port, on a Data Mover. Each interface assigns an IP address to the port.

internal checkpoint
Read-only, logical point-in-time image of a source object created during replication on the source and destination sides. Internal checkpoints cannot be managed by users. Replicator (V2) internal checkpoints are identified by the prefix root_rep_ckpt.

internationalization (I18N)
The process of generalizing software such that it can be made to handle various languages and locales.

Internet Control Message Protocol (ICMP)
Internet protocol that reports errors and provides control information related to IP-packet processing.

Internet Protocol (IP)
Network layer protocol that is part of the Open Systems Interconnection (OSI) reference model. IP provides logical addressing and service for end-to-end delivery.

Internet Protocol address (IP address)
Address uniquely identifying a device on any TCP/IP network. Each address consists of four octets (32 bits), represented as decimal numbers separated by periods. An address is made up of a network number, an optional subnetwork number, and a host number.

Internet SCSI (iSCSI)
Protocol for sending SCSI packets over TCP/IP networks.

Internet Storage Name Service (iSNS)
Discovery and naming protocol designed to facilitate the automated discovery, management, and configuration of iSCSI and Fibre Channel Protocol (FCP) devices on a TCP/IP network.

I/O device
Addressable input/output unit, such as a disk drive.

IP
See Internet Protocol.

IP address
See Internet Protocol address.

IP interface
Named logical entity representing a physical device (a port) or a virtual device (a combination of physical devices) and used to assign an IP address to the device. There may be multiple IP interfaces associated with a single device.

IP replication service
Service that uses the IP network to transfer the delta sets from the replication SavVol on the source site to the replication SavVol on the destination site.

IQN
See iSCSI qualified name.

iSCSI
See Internet SCSI.

iSCSI host
Computer hosting an iSCSI initiator.

iSCSI initiator
iSCSI endpoint, identified by a unique iSCSI name, which begins an iSCSI session by issuing a command to the other endpoint (the target).

iSCSI LUN
VNX for file iSCSI software feature that processes SCSI commands such as reading from and writing to storage media.

iSCSI qualified name (IQN)
Naming standard supported by the iSCSI protocol. IQN names are globally unique and in the form of iqn, followed by a date and a reversed domain name.

iSCSI session
Relationship between two iSCSI endpoints (the initiator and the target) over a group of TCP connections.

iSCSI target
iSCSI endpoint, identified by a unique iSCSI name, which executes commands issued by the iSCSI initiator.

iSNS
See Internet Storage Name Service.

JIS (Japanese Industrial Standards)

Multibyte character encoding system used to represent Japanese. Includes Shift JIS (SJIS) encoding. The main alternatives to JIS encoding are EUC (used on UNIX systems where the JIS encodings are incompatible with POSIX standards) and more recently Unicode, particularly in the form of UTF-8.

jumbo frames

Changes an Ethernet frame's Maximum Transmission Unit (MTU) from the IEEE 1500 bytes up to 9000 bytes. Jumbo frames should only be used when the packet to/from any combination of Ethernet devices can be handled without any Layer 2 fragmentation or reassembly.

K

Kerberos
Authentication, data integrity, and data privacy encryption mechanism used to encode authentication information. Kerberos coexists with NTLM (Netlogon services) and, using secret-key cryptography, provides authentication for client/server applications.

Kerberos Key Distribution Center (KDC)
Stores and retrieves information about security principals in the Active Directory database. Each domain controller in Windows 2000 or later is a Kerberos KDC that acts as a trusted intermediary between a client and a server.

kernel
Software responsible for interacting most directly with the computer's hardware. The kernel manages memory, controls user access, maintains file systems, handles interrupts and errors, performs input and output services, and allocates computer resources.

kibibytes
Kibibytes comes from kilo binary and stands for 1024 in the ISO International System of Units. Network performance is measured in kibibytes.

kilobit (Kb)
1024 bits.

kilobyte (KB)
1024 bytes.

L

L10N
An abbreviation for localization (L+10 letters+N).

See localization.

LAN
See local area network.

LCC
See link control card.

LDAP
See Lightweight Directory Access Protocol.

LDAP-based directory
Directory servers that support LDAP, including Active Directory with IdMU, or SFU, OpenLDAP, or iPlanet (also known as Sun Java System Directory Server and Sun ONE Directory Server).

Lightweight Directory Access Protocol (LDAP)
Industry-standard information access protocol that runs directly over TCP/IP. It is the primary access protocol for Active Directory and LDAP-based directory servers. LDAP version 3 is defined by a set of Proposed Standard documents in Internet Engineering Task Force (IETF) RFC 2251.

link
Working data connection between systems on a network. Also, a connection between two or more ports.

link aggregation
High-availability feature based on the IEEE 802.3ad Link Aggregation Control Protocol (LACP) standard which allows Ethernet ports with characteristics similar to the same switch to combine into a single virtual device, or link with a single MAC address and potentially multiple IP addresses.

link control card (LCC)
Element of VNX for block shelf that receives and electrically terminates the incoming Fibre Channel signal. It passes the signal between shelves in the cabinet and passes the output signal (through cables) to the next device in the loop.

link-local address
Address that is used for Neighbor Discovery or by applications in an environment where no routers are present.

load balancing
Process of distributing an I/O workload across all paths.

See also *static load balancing* and *dynamic load balancing*.

local area network (LAN)
Minimum of two network nodes communicating through a physical medium over a distance of less than 3 km.

local backup
Procedure that backs up a file system, or incremental changes to a file system from a Data Mover to a locally attached TLU.

See also *automated backup and restore*.

local group
Group that is granted permissions and rights from its own computer to only those resources on its own computer on which the group resides. Computers must be running Windows Server 2000 Professional and member servers.

local hosts file
Text file on a Data Mover that contains a list of IP addresses and their corresponding hostnames.

local mirror
Symmetrix shadow volume that is a complete replica of a production volume within the same storage unit. If the production volume becomes unavailable, I/O continues to use the local mirror transparent to the host.

See also *R1 volume*.

local replication
Replication of a file system on a single VNX for file with the source file system on one Data Mover and the destination file system on another Data Mover.

locale
A set of user preferences for a particular country or region including language (for example, en-US for American English) and associated settings such as the formatting and parsing of dates, times, numbers, and currencies, units of measure, sort-order (collation), and translated names for time zones, languages, and countries.

localization (L10N)
The process of adapting software for a specific culture or language by adding locale-specific components and translating text.

locked state
State of a file when its read/write permission is changed to read-only in a file system enabled for file-level retention. Files committed to the locked (WORM) state cannot be altered or deleted until their retention date has passed.

logical device
One or more physical devices or partitions managed by the storage controller as a single logical entity.

See also *logical volume*.

logical drive
Access point for a logical volume such as C:\ or D:\.

logical unit (LU)
For iSCSI on VNX for file, a logical unit is an iSCSI software feature that processes SCSI commands, such as reading from and writing to storage media. From an iSCSI host perspective, a logical unit appears as a disk drive.

logical unit number (LUN)
Identifying number of a SCSI or iSCSI object that processes SCSI commands. The LUN is the last part of the SCSI address for a SCSI object. The LUN is an ID for the logical unit, but the term is often used to refer to the logical unit itself.

logical volume
Logical devices aggregated and managed at a higher level by a volume manager.

See also *logical device*.

loopback replication
Replication of a file system with the source and destination file systems residing on the same Data Mover.

LU
See logical unit.

LUN
See logical unit number.

LUN mask
Set of access permissions that identify which iSCSI initiator can access specific LUNs on a target.

M

MAC address
See media access control.

MAC layer
Media-specific access control protocol within IEEE 802 specifications.

Management Information Base (MIB)
Hierarchical database maintained by an agent that a network management station can query by using a network management protocol such as the SNMP.

manual local backup
On VNX for file, a procedure in which an operator enters commands manually or by using a script. During the backup operation, a single Data Mover or multiple Data Movers in parallel are backed up fully or incrementally to one or more locally attached tape drives. Each Data Mover requires its own tape drive, attached to one of the Data Mover's SCSI or Fibre Channel ports. Data goes directly to VNX for file's attached tape drive, and does not traverse the network. Also called simple local backup.

maximum concurrent sessions supported
The maximum number of NDMP backup or restore streams that the Data Mover supports. If the system memory is less than 8 GB, only four concurrent streams are allowed. If the system memory is more than 8 GB, you can set the concurrent streams to more than four and up to a maximum of eight.

Maximum Transmission Unit or Maximum Transfer Unit (MTU)
Largest frame size transmitted over the network. Messages longer than the MTU must be divided into smaller frames. The Layer 3 protocol (including IP, IPX) extracts the MTU from the Layer 2 protocol (including Ethernet), fragments the messages into that frame size, and makes them available to the lower layer for transmission.

Mb
Megabit. Approximately 1 million bits.

MB
Megabyte. Approximately 1 million bytes.

media
Plural of medium. Variety of physical devices, such as the disk surface on which data is stored or the physical cable connecting nodes to form a network.

media access control (MAC) address
Data link hardware address every physical device (port) or virtual device needs to connect to a network segment. These addresses are used by network devices to locate the logical devices.

member server
Computer joined to a domain, but not a domain controller of the domain. Member servers participate in a domain, but do not perform domain user-account authentication. For a member server, permissions can be set on resources so that only authorized users can connect to the server and use its resources. Resource permissions can be granted for domain global groups and users as well as local groups and users.

message digest
The representation of text in the form of a single string of digits, created by using a formula called one-way hash function. A message digest is also called as hash value, cryptographic hash, digital fingerprint, cryptographic checksum, hash, hash digest.

metadata
Data that contains structural information, such as access methods, about itself.

metavolume
On a VNX for File, a concatenation of volumes, which can consist of disk, slice, or stripe volumes. Also called a hypervolume or hyper. Every file system must be created on top of a unique metavolume.

See also *disk volume*, *slice volume*, *stripe volume*, and *volume*.

MGFS
See Migration File System.

MIB
See Management Information Base.

Microsoft Distributed File System (DFS)
Windows operating systems service that consists of software residing on network servers and clients that transparently links shared folders located on different file servers into a single namespace.

Microsoft Management Console (MMC)
Extensible common presentation service for management applications included in the Windows operating system.

See also *MMC snap-in*.

Microsoft Windows Services for UNIX (SFU)
Microsoft software that provides a UNIX environment on Windows.

Migration File System (MGFS)
EMC file system type used to perform data migration from either CIFS or NFS to VNX for file.

mirrored pair
Logical volume with all data recorded twice, once on each of two different physical devices.

mirroring
Method by which the system maintains two identical copies of a designated volume on separate disks.

MirrorView Synchronous (MirrorView/S)
Software application that synchronously maintains copies of production images (source LUNs) at a separate location to provide disaster recovery capability. The copied images are continuously updated to be consistent with the source, and provide the ability for a standby VNX for file to take over for a failed VNX for file in the event of a disaster on the production site. Synchronous remote mirrors (source and destination LUNs) remain in synchronization with each other for every I/O. MirrorView/S requires VNX for block backend storage.

MMC
See Microsoft Management Console.

MMC snap-in
Management tool an administrator can add to the interface of a Microsoft Management Console (MMC).

See also *Microsoft Management Console*.

mount
Process of attaching a subdirectory of a remote file system to a mount point on the local machine.

mount point
Local subdirectory to which a mount operation attaches a subdirectory of a remote file system.

MPFS
See Multi-Path File System.

MPFS over iSCSI
Multi-Path File System over iSCSI-based clients. MPFS client running an iSCSI initiator works in conjunction with an IP-SAN switch containing an iSCSI to SAN blade. The IP-SAN blade provides one or more iSCSI targets that transfer data to the storage area network (SAN) systems.

See also *Multi-Path File System (MPFS)*.

MPFS session
Connection between an MPFS client and VNX for file.

MPFS share
Shared resource designated for multiplexed communications by using the MPFS file system.

MSL
See Multiprotocol Support Layer.

MTU
See Maximum Transmission Unit or Maximum Transfer Unit.

multibyte support
Generic term for encoding schemes for characters that may require more than one byte.

multicast
Communication between one sender and multiple receivers. Multicast messages are sent to a defined subset of network addresses.

Multi-Path File System (MPFS)
VNX for file feature that allows heterogeneous servers with MPFS software to concurrently access, directly over Fibre Channel or iSCSI channels, shared data stored on a EMC Symmetrix or VNX for block storage system. MPFS adds a lightweight protocol called File Mapping Protocol (FMP) that controls metadata operations.

Multiprotocol Support Layer (MSL)
On VNX for file, the data access in real time (DART) operating system layer that allows both NFS and CIFS protocols to access a file system.

N

native mode
Normal operating mode of a computer, as opposed to emulation mode.

NBS
See Network Block Service.

NDMP
See Network Data Management Protocol.

NDMP2D
See NDMP Backup-to-Disk.

NDMP Backup-to-Disk (NDMP2D)
Software-based virtual tape library configured on a Data Mover that emulates a real TLU, and allows NDMP backup-to-disk functionality. This feature is sometimes referred to as a virtual tape library unit (VTLU). However, it does not provide true VTLU functionality as found in EMC Disk Library and similar storage products.

NDMP client
Application that controls the NDMP session. The NDMP client runs an NDMP-compliant backup application, such as EMC NetWorker®.

NDMP host
Host system (Data Mover) that executes the NDMP server application. Data is backed up from the NDMP host to either a local tape drive or to a backup device on a remote NDMP host.

NDMP server
NDMP process that runs on an NDMP host, which is a Data Mover in VNX for file environment.

NDMP Volume Backup (NVB)
EMC-specific type of NDMP backup mechanism that backs up data blocks at a volume level, rather than at a file level. NVB reads a set of disk data blocks in an efficient manner compared to the method used for traditional, file-based backups. NVB works only with EMC-qualified vendor backup software. NVB is commonly known as Volume Based Backup (VBB).

NDMS
See Network Data Management Service.

Neighbor Discovery
IPv6 protocol used for address resolution, prefix detection, default router detection and settings, and redirect functions. It uses link-local addresses for communication.

nested export
Export of a component file system. The export has its own specified access controls.

nested mount file system (NMFS)
File system that contains the nested mount root file system and component file systems.

nested mount file system root
File system on which the component file systems are mounted read-only, except for mount points of the component file systems.

NetBIOS
See network basic input/output system.

NetBIOS alias
Alternative NetBIOS name. NetBIOS aliases provide multiple, alternate identities for a given resource.

NetBIOS name
Name recognized by WINS, which maps the name to an IP address.

netgroup
Group of computers on a network administered by using a single name. Netgroups can be defined by using a local text file that provides the list of hosts in a netgroup, or by using NIS or an LDAP-based directory server.

network
Combination of devices, cabling, and software that makes up a communication infrastructure.

network-attached storage (NAS)
Specialized file server that connects to the network. A NAS device, such as VNX for file, contains a specialized operating system and a file system, and processes only I/O requests by supporting popular file sharing protocols such as NFS and CIFS.

network backup
See remote backup.

network basic input/output system (NetBIOS)
Network programming interface and protocol developed for IBM personal computers.

Network Block Service (NBS)
Proprietary client/server protocol of VNX for file that provides a block device (for example, iSCSI device) management functionality over a TCP/IP connection. Supported block device management functions include snapshots and remote replication.

Network Data Management Protocol (NDMP)
Open standard network protocol designed for enterprise-wide backup and recovery of heterogeneous network-attached storage.

Network Data Management Service (NDMS)
Network communication service that uses the Network Data Management Protocol (NDMP) and contains its own backup and retrieval utilities.

network element
SNMP-managed devices such as hosts, gateways, and terminal servers on a network.

network file system (NFS)
Network file system (NFS) is a network file system protocol that allows a user on a client computer to access files over a network as easily as if the network devices were attached to its local disks.

Network Information Service (NIS)
Distributed data lookup service that shares user and system information across a network, including usernames, passwords, home directories, groups, hostnames, IP addresses, and netgroup definitions.

network interface card (NIC)
Circuit board that provides network communication capabilities to and from a computer system.

network lock manager (NLM)
Service that allows clients to lock files or byte ranges.

network management station (NMS)
Systems that execute management applications, such as SNMP commands to monitor and control network elements.

network node
Network connection point.

network portal
Component that listens for and is capable of accepting iSCSI connections within a given iSCSI session. A network portal for an iSCSI initiator is identified by its IP address. A network portal for an iSCSI target is identified by its IP address, listening port, and group tag.

network status monitor (NSM)
Protocol that allows NFS clients and servers to monitor each other's status and be aware of reboots.

Network Time Protocol (NTP)
Protocol used to synchronize the realtime clock in a computer with a network time source.

NFS
See network file system.

NIC
See network interface card.

NIS
See Network Information Services.

NLM
See network lock manager.

NMFS
See nested mount file system.

NMS
See network management station.

NonNumericStat
Class that is derived from the Stat class and represents text-based value. NonNumericStat does not offer summary information unlike NumericStat.

not locked state
Initial state of a file when it is created. A file that is not locked is treated in the same manner as any file in a file system not enabled for file-level retention (FLR). This means it can be renamed, modified, and deleted until the time that the file is locked.

notifications
Actions the Control Station takes in response to particular events. Some possible actions include sending an email message or an SNMP trap. There are two types of notifications: event notifications, which are notifications based on predefined system events such as a temperature being too high, and resource notifications, which are notifications based on user-specified resource usage limits or thresholds.

NSM
See network status monitor.

NT file system (NTFS)

See NTFS.

NTFS
NTFS is the standard file system of Windows NT, including its later versions. NTFS supersedes the FAT file system as the preferred file system for Microsoft Windows. NTFS has several improvements over FAT such as improved support for metadata and the use of advanced data structures to improve performance, reliability, and disk space utilization, plus additional extensions such as security access control lists (ACLs) and file system journaling.

NTP
See Network Time Protocol.

ntxmap
Customized software used to support mapping requirements in a multiprotocol environment.

NumericStat
Class that is derived from the Stat class and represents a numeric statistic. NumericStat also offers summary (min/max/avg) information on the collected statistic.

NVB
See NDMP Volume Backup.

O

on-link
Nodes on the same broadcast domain.

OpenLDAP
Open-source implementation of an LDAP-based directory service.

Open Systems Interconnection (OSI)
International Standards Organization (ISO) standard for worldwide communications that defines a framework for implementing protocols in seven layers.

organizational unit (OU)
Active Directory container object that is used within domains. An organizational unit (OU) is a logical container where users, groups, computers, and other organizational units are placed. The OU can contain objects only from its parent domain. An OU is the smallest scope to which a Group Policy Object can be linked, or over which administrative authority can be delegated.

orphan file
File that exists on secondary storage, but is no longer referenced by a stub file on VNX for file. An orphan file is kept intact on secondary storage. It can be managed by the system administrator.

OSI
See Open Systems Interconnection.

OpenSSH
OpenSSH is a protocol developed by the OpenBSD project. OpenSSH provides encrypted communication over a network by using the SSH protocol.

P

packet
In communications, a fixed block of data transmitted as a single entity. In local area networks (LANs), the terms frame and packet are used synonymously.

See also *frame*.

passthrough
Archiving method option that instructs VNX for file to read the requested data from secondary storage. The data is returned to the client, but is not recalled to primary storage; thus the stub file remains intact.

path
Route to a file or directory on a disk.

pause
On VNX for file, when a SnapSure checkpoint is created, the system pauses the file system before creating the bitmap. The system stops responding to network requests (but does not drop the connection), allows requests in process to complete, and then internally locks the file system. This puts the file system in a consistent state for the creation of the checkpoint bitmap.

PAX
See Portable Archive Interchange.

PBR
See Persistent Block Reservation.

PCI
See Peripheral Component Interconnect.

PCSE
See preconfigured single enclosure.

PDC
See primary domain controller.

PDU
See Protocol Data Unit.

Peripheral Component Interconnect (PCI)
Peripheral bus used to provide a high-speed data path between the CPU and peripheral devices.

Persistent Block Reservation (PBR)
Technique of reserving an adequate number of blocks in a file system to support creation of a logical unit of a specified size. The blocks are reserved for the logical unit whether or not in use.

persona
Means of providing an identity for a Data Mover as either a server or a client through a private key and associated public key certificate. Each persona can maintain up to two sets of keys (current and next) to allow for the generation of new keys and certificates prior to the expiration of the current certificate.

PFS
See Production File System.

PFS application
Business application that accesses a PFS and performs transactions, such as read, write, or delete on the PFS blocks.

See also *Production File System*.

physical volume
Disk drive on the backend system. VNX for file addresses the physical volumes of a system through logical disk volumes.

See also *volume*.

PKI
See public key infrastructure.

playback service
Process of reading the delta sets from the destination SavVol and updating the destination file system.

PLU
See production logical unit.

pNFS
The parallel NFS (pNFS) is part of NFS version 4.1 that allows the clients to access storage device directly and in parallel.

policy
Set of rules used to guide VNX FileMover software about when to back up, archive, or migrate files from one data store to another.

policy and archiving software
Policy and software used to archive data from VNX for file to secondary storage according to customer-defined policies and schedules.

policy engine
External server on which the policy and archiving software runs.

pop-up messages
Feature that warns or informs Microsoft Windows clients (connected to a specific machine name) when certain system events occur. Pop-up messages can be customized to provide specific instructions or contact information.

port
Physical connection point to a network or a number used at the transport layer to track host-to-host virtual circuits.

Port Range
The range of port numbers that is defined by a user to listen for NDMP data connections. It is recommended to use dynamic or private ports (49152-65535) of IANA to set the NDMP port range.

Port Width
The number of ports that are present in a port range. The required minimum port width is 32. However, it is recommended that the port width should be at least 100.

Portable Archive Interchange (PAX)
VNX for file archive protocol that works with standard UNIX tape formats and provides file-level backup and recovery operations.

portal group
Collection of network portals for a given iSCSI target.

portmapper
RPC service that assigns port numbers to applications. On VNX for file, the portmapper allows clients access to the services registered on the Data Mover.

POST
See power on self-test.

power on self-test (POST)
Series of built-in diagnostics performed by the BIOS in a personal computer when it is first started.

PowerPath
EMC host-resident software that integrates multiple path I/O capabilities, automatic load balancing, and path failover functions into one comprehensive package for use on open server platforms connected to Symmetrix or VNX for block.

preconfigured single enclosure (PCSE)
The system preconfigured at the factory with VNX for file and Symmetrix system in one cabinet.

primary Control Station
Provides utilities for managing, configuring, and monitoring of the Data Movers in VNX for file. VNX for file support configurations with dual, redundant Control Stations, a primary and secondary Control Station. Under normal circumstances, after the primary Control Station fails over, you can continue to use the secondary Control Station as the primary.

See also *Control Station*, *secondary Control Station*, and *standby device*.

primary domain controller (PDC)
Windows NT service that manages security for its local domain.

See also *BDC*.

primary group
Group identified on NFS systems by the group identifier (GID) in the fourth column of the password file. This is set through the Windows User Manager in a Microsoft Windows environment.

primary storage
VNX for file that provides clients access to normal files and archived files through the stub files that represent them. The VNX for file contains all the stub files.

primary Usermapper service
Instance of the Usermapper service that assigns user IDs (UIDs) and GIDs to Windows users and groups by asking VNX for file for access to system objects.

principal
Unique name to which the Kerberos Key Distribution Center (KDC) can assign tickets. A principal can be a user, service, or server.

Production File System (PFS)
Production File System on VNX for File. A PFS is built on Symmetrix volumes or VNX for Block LUNs and mounted on a Data Mover in the VNX for File.

production logical unit (PLU)
iSCSI LUN that serves as a primary storage device. A PLU can be configured as a disk drive through an iSCSI initiator.

promote
To mount a snapshot to an iSCSI LUN, so it can be configured as a disk drive through an iSCSI initiator.

protocol
Standard defined between the client and the user that determines how information is transferred and interpreted over a network.

Protocol Data Unit (PDU)
iSCSI term for a fixed block of data transmitted as a single entity. A PDU is an iSCSI packet.

public key infrastructure (PKI)
Means of managing private keys and associated public key certificates for use in public key cryptography. It is a framework which allows the creation of a certificate which is used by SSL.

Q

qualified name
Name of an iSCSI target or initiator in IQN or EUI format.

quota
Limit on the amount of allocated disk space and the number of files (inodes) that a user or group of users can create in a Production File System. Quotas control the amount of disk space or the number of files that a user or group of users can consume or both.

quota policy
Parameter you set to tell the system to calculate disk usage either by blocks or by file size. (Default is by blocks.)

quota tree
Directory or subdirectory to which tree quotas are applied.

R1 volume
SRDF term denoting the source (primary) Symmetrix volume.

See also *local mirror*.

R2 volume
SRDF term denoting the destination (secondary) Symmetrix volume.

See also *remote mirror*.

RAID
See redundant array of independent disks.

RAID 1
RAID method that provides data integrity by mirroring (copying) data onto another disk in the LUN. This RAID type provides the greatest data integrity at the greatest cost in disk space.

RAID 1/0
RAID method that mirrors and stripes, with data being written to two disks simultaneously. Data transfer rates are higher than with RAID 5, but RAID 1/0 uses more disk space for mirroring.

RAID 5
Data is striped across disks in large stripes. Parity information is stored so data can be reconstructed if needed. One disk can fail without data loss. Performance is good for reads, but slow for writes.

RAID 6
Data and parity are striped on a block level across multiple disks. Two sets of parity data are maintained. RAID 6 provides an extremely high fault tolerance, and can sustain two simultaneous drive failures without data loss.

RAID group
A group of disks in the system that takes on a RAID characteristics.

RAID S
EMC proprietary variant of RAID 5.

read hit
Data requested by a read operation in global memory.

read miss
Data requested by a read operation not in global memory.

read-only checkpoint
Read-only, point-in-time, logical image of a PFS.

See also *Production File System*.

realm
In a networked environment, a set of security principals (users, service, and computers) subject to Kerberos authentication, and managed by the same Kerberos authority.

reason code
On VNX for file, a number representing the state of a Data Mover.

recall policy
Attribute that is set per individual file and is in the stub file when a file is archived to secondary storage. VNX for file uses the recall policy to determine the amount of data that is recalled to primary storage to satisfy the client read request.

recovery point objective (RPO)
Describes the acceptable amount of data loss, measured in units of time, for example, 12 minutes, 2 hours, or 1 day. This represents a target that is derived from conditions specified in an SLA, RTO, and relevant analyses. The RPO in conjunction with the recovery time objective (RTO) is the basis on which data protection strategy is developed.

recovery time objective (RTO)
How long a business process can be down before consequences are unacceptable. This represents a target that is derived from conditions specified in an SLA and business impact analysis.

Redundant Array of Independent Disks (RAID)
Method for storing information where the data is stored on multiple disk drives to increase performance and storage capacities and to provide redundancy and fault tolerance.

redundant components
Backup arrays, drives, disks, or power supplies that duplicate functions performed elsewhere.

reduplication
Process to undo the effect of deduplication on a file. If the file was compressed, it will be decompressed. If there are multiple instances of the file data, then a copy of the file data is made so that blocks are not shared between instances of the file. This process consumes additional space in the file system. Therefore, there must be sufficient free space in the file system to hold an additional copy of the original file for this process to complete.

regular iSCSI LUN
iSCSI LUN that uses Persistent Block Reservation (PBR) to ensure that the file system has sufficient space for all data that might be written to the LUN.

remote backup
Remotely initiated procedure that backs up data to a TLU which can be attached to a target server different from the source Data Mover. The configuration determines whether data traverses the network.

See also *automated backup and restore* and *three-way backup*.

remote mirror
For SRDF, a remote mirror is a Symmetrix shadow volume physically located in a remote Symmetrix system. Using the EMC SRDF technology, the remote system is joined to a local system with a local mirror. If the local mirror becomes unavailable, the remote mirror is accessible. For MirrorView/S, a remote mirror is a LUN mirrored on a different VNX for block. Each remote mirror contains a particular source LUN (primary image) and its equivalent destination LUN (secondary image). If the source site system fails, the destination LUN in the mirror can be promoted to take over, thus allowing access to data at a remote location.

See also *R2 volume*.

remote procedure call (RPC)
Programming interface that allows one program to utilize the services of another program in a remote machine.

remote replication
Replication of a file system from one VNX for file to another. The source file system resides on a different system from the destination file system.

remote three-way backup
See heterogeneous three-way backup.

replication
Service that produces a read-only, point-in-time copy of a source file system. The service periodically updates the copy, making it consistent with the source file system.

replication reversal
Process of reversing the direction of replication. The source file system becomes read-only and the destination file system becomes read/write.

replication service
Service that copies modified blocks from a source file system to a replication SavVol prior to transferring the data to the destination file system.

Replication set
A collection of production source volume and the replica volume/s to which it replicates. Every SAN-attached storage volume in the production storage must have a corresponding volume at each copy. Each consistency group contains as many replication sets as there are volumes in the production storage to replicate.

Replicator ConfigVol
Internal information store for replication. Provides a storage vehicle for tracking changes in the source file system.

Replicator failover
Process that changes the destination file system from read-only to read/write and stops the transmission of replicated data. The source file system, if available, becomes read-only.

Replicator SavVol
Volume required by replication, used to store modified data blocks from the source file system.

Request for Comment (RFC)
Name given to Internet standards.

retention date
Date until which a locked file in an FLR-enabled file system will be protected. Users and applications manage a file's retention date by using NFS or CIFS to set the file's last access time to a future date and time. The retention timestamp is compared to the file system's FLR clock to determine whether a file's retention date has passed.

RFC
See Request for Comment.

RIP
See routing information protocol.

router
Device that transfers information between networks and determines the most efficient route for it to follow.

routing information protocol (RIP)
Routing protocol optimized for creating routes within one organization (interior gateway protocol). RIP is a distance vector protocol that uses hop count (max 15) as the metric. RIP-1 does not send the mask in updates. RIP-2 sends the mask in updates.

RPA
Hardware that is used to run the RecoverPoint software, which is responsible for most of the product's intelligence. These intelligent data protection appliances manage all aspects of reliable data replication at all sites.

RPC
See remote procedure call.

RPO
See recovery point objective.

RSA
A public key algorithm, named after inventors Rivest, Shamir, and Adleman. RSA uses public and private keys that are functions of a pair of large prime numbers.

RTO

See recovery time objective.

S

SAM
See Security Access Manager or Security Accounts Manager.

SAN
See storage area network.

SavVol
Standard metavolume to which VNX SnapSure writes checkpoint data. This volume can be smaller than the Production File System upon which the checkpoint is based.

SavVol extend
Process of enlarging the SavVol space to ensure that it does not become full and inactivate one or more checkpoints. By default, and as system resources permit, VNX SnapSure automatically extends the SavVol each time the HWM is reached.

See also *high water mark*.

scrubbing
Process of reading, checking error-correction bits, and writing corrected data back to the source.

SCSI
See small computer system interface.

SCSI adapter
Circuit board in a system that provides the physical interface between the disk director and the disk drives.

SCSI bus
Parallel bus that carries data and control signals from SCSI devices to a SCSI controller.

SCSI CAM
See SCSI common access method.

SCSI common access method (SCSI CAM)
American National Standards Institute (ANSI) standard interface that provides a common language between device drivers and SCSI adapters.

SD
See security descriptor.

secondary Control Station
If the primary Control Station goes offline, the secondary Control Station, if properly configured, automatically takes over all primary Control Station functions and executes any of VNX for file commands you enter. After the primary Control Station is repaired or replaced and the Controls Stations are rebooted, the first Control Station to start is restored as the primary.

See also *Control Station*, *primary Control Station*, and *standby device*.

secmap
See secure mapping.

secondary storage
Storage device that contains original files associated with stub files on the primary storage. This device must be either a CIFS, HTTP, HTTPS, or NFS server. VNX for file can also be secondary storage.

secondary Usermapper service
In a multi-VNX for file environment, an instance of the Usermapper service that forwards requests for user mappings to the primary Usermapper service and returns those mappings to the Data Movers in addition to storing the mappings it processes.

Secure File Transfer Protocol (SFTP)
Also called as SSH File Transfer Protocol, SFTP is a network protocol that provides file transfer and manipulation functionality over any reliable data stream. It is typically used with version two of the SSH protocol to provide secure file transfer.

secure mapping (secmap)
Cache that contains all mappings between SIDs and UID or GIDs used by a Data Mover or Virtual Data Mover (VDM).

secure shell protocol (SSH)
Enables you to execute VNX for file CLI commands through a secure shell directly onto the Control Station. The SSH protocol encrypts the data sent between your computer and the Control Station. Interactive features are not supported by the CLI commands option.

Secure Sockets Layer (SSL)
Security protocol that provides encryption and authentication. It encrypts data and provides message and server authentication. It also supports client authentication if required by the server.

Security Access Manager or Security Accounts Manager (SAM)
Microsoft Windows service that authenticates users to use resources on the network. The SAM database is the location for all security and user account information for a Windows NT domain.

security descriptor (SD)
In a Microsoft Windows environment, information associated with a file that includes the owner and the group SID for the file's access control list (ACL).

security identifier (SID)
Unique identifier that defines a user or group in a Microsoft Windows environment. Each user or group has its own SID.

security mode
Setting that specifies how a Data Mover performs authentication for CIFS users. The security mode is set for each Data Mover not for a file system.

server
Device that handles requests made by clients connected through a network.

Server Message Block (SMB)
Underlying protocol used by the CIFS protocol enhanced for use on the Internet to request file, print, and communication services from a server over the network. The CIFS protocol uses SMB to provide secure file access and transfer to many types of hosts such as LANs, intranets, and the Internet.

service level agreement (SLA)
Contract or agreement that formally defines the level of expected availability, serviceability, performance, operation, or other attributes of service and even penalties in the case of violation of the SLA. An SLA may include acceptable downtime or disaster recovery time. In theory, an SLA is a formal agreement. However, in practice the agreement is often informal in which case it may be called a service level expectation (SLE).

service processor (SP)
Service processor on a Symmetrix system. The device running the Symmetrix monitoring software.

SetStat
Represents a collection of elements each of which contains one or more Stat objects. To retrieve values, clients need to iterate through the elements and then iterate through the list of Stat objects for each element.

SFU

See Microsoft Windows Services for UNIX.

shadow copy
Point-in-time copy created through Microsoft's Volume Shadow Copy Service.

Shadow Copy for Shared Folders (SCSF)
Microsoft Windows feature that provides Windows XP and Windows Server 2003 clients direct access to VNX SnapSure point-in-time images of their files and folders for the purpose of recovering point-in-time data.

share
File system, directory, or service that has been made available to CIFS users on the network. Also, the process of making a file system, directory, or service available to CIFS users on the network.

share name
Name given to a file system, or resource on a file system available from a particular CIFS server to CIFS users. There may be multiple shares with the same name, shared from different CIFS servers.

shelf
On VNX for block, the common functional components in either a disk-array enclosure (DAE) or disk-array processor enclosure (DPE).

SID
See security identifier.

silvering

See initialization.

Simple Mail Transfer Protocol (SMTP)
Standard email protocol on the Internet.

Simple Network Management Protocol (SNMP)
Method used to communicate management information between the network management stations and the agents in the network elements.

Simple Network Time Protocol (SNTP)
Adaptation of the Network Time Protocol (NTP) used to synchronize computer clocks in the Internet.

See also *NTP*.

single enclosure
See PCSE.

skew (time)
Time difference between VNX for file and its network clients.

SLA

See service level agreement.

slewing
Process of gradually correcting the local system time.

slice volume
On VNX for File, a logical piece or specified area of a volume used to create smaller, more manageable units of storage.

See also *disk volume*, *metavolume*, *stripe volume*, and *volume*.

SLU
See snapshot logical unit.

small computer system interface (SCSI)
Standard set of protocols for host computers communicating with attached peripherals.

SMB
See Server Message Block.

SMTP
See Simple Mail Transfer Protocol.

snapshot
Generic term for a point-in-time copy of data.

snapshot logical unit (SLU)
Snapshot promoted to logical unit status and configurable as a disk drive through an iSCSI initiator.

Snapshot Virtual File System (SVFS)
File system that allows an NFS or a CIFS client read-only access to online snapshots of a file system directory by accessing a virtual .ckpt directory entry. SVFS and CVFS are synonymous terms.

SnapSure
On the VNX for file, a feature that provides read-only, point-in-time copies, also known as checkpoints, of a file system.

SnapSure SavVol
The volume to which SnapSure copies original point-in-time data blocks from the Production File System (PFS) before the blocks are altered by a transaction. SnapSure uses the contents of the SavVol and the unchanged PFS blocks to maintain a checkpoint of the PFS.

SNMP
See Simple Network Management Protocol.

SNMP agent
Software module in a managed device, such as VNX for file or Symmetrix system, that maintains local management information and delivers that information to a manager by using SNMP.

SNMP community
Name for the SNMP transaction with a remote system. This is used as a password to control access to the SNMP MIB.

SNMP trap
Asynchronous message sent from an SNMP agent to an SNMP management program. Traps are typically used to report errors. VNX for file can be configured to send SNMP traps when specified events occur.

See also *event notification*.

SNTP
See Simple Network Time Protocol.

soft quota
Configurable file system usage limit that, when reached, can cause the system to generate an event, and send a warning message to Windows clients. The soft quota limit serves as a grace period providing reaction time so that reaching the hard quota can be avoided.

See also *quota* and *hard quota*.

software virtual tape library (SVTL)
See VTLU.

source object
The production data being copied. Also known as the Production File System, production LUN, and primary file system. Replicator source objects are file systems, iSCSI LUNS, and Virtual Data Movers (VDM).

source VNX for file
Term for the local (primary) VNX for File. A source VNX for file is typically the "production" side of a disaster recovery SRDF/S or MirrorView/S configuration.

SP
See storage processor and service processor.

SP A
See storage processor A.

spare disk drive
Disk drive that can take over for a failed disk drive.

SP B
See storage processor B.

SPE
See storage processor enclosure.

SPS
See standby power supply.

SRDF
See Symmetrix Remote Data Facility.

SRDF channel
Method used to move information between the Control Stations of systems joined in an SRDF configuration.

SRDF/Asynchronous (SRDF/A)
SRDF extended-distance replication facility providing a restartable, point-in-time remote replica that lags not far behind the source. Using SRDF/A with VNX for file provides dependent write consistency for host writes from a source VNX for file/Symmetrix DMX™

system pair to a destination VNX for file/Symmetrix DMX system pair through predetermined time cycles (delta sets).

SRDF/Synchronous (SRDF/S)
SRDF complete disaster recovery configuration option that provides synchronized, real-time mirroring of file system data between the source Symmetrix system and one or more remote Symmetrix systems at a limited distance (up to 200 km). SRDF/S can include EMC TimeFinder®/FS NearCopy in the configuration (active/passive; active/active').

SSH
See secure shell protocol.

SSH 1
The SSH protocol, version 1. This protocol went through several revisions, of which 1.3 and 1.5 are the best known. It is considered obsolete today.

SSH-2
The SSH protocol, version 2, as defined by several draft standards documents of the IETF SECSH working group.

SSL
See Secure Sockets Layer.

SSP
See storage service provider.

stand-alone CIFS server
Type of CIFS server that uses local user accounts on the Data Mover and therefore does not require any Windows domain infrastructure. When users log in to a stand-alone server, NTLM is used to authenticate users against the local accounts database.

standard volume (STD)
Active application volume containing a Production File System (production data and programs). An STD volume is a local volume on a Symmetrix system upon which VNX for file builds the Production File System.

See also *business continuance volume*.

standby device
Device held in reserve against a failure of its active partner. When the active device fails, the standby device takes over.

standby power supply (SPS)
Battery system used to provide power to VNX for block during a power failure.

Stat
An abstract representation of all types of statistics values.

StatSummary
An interface that provides summary information (min/max/avg) for NumericStat objects.

static load balancing
Assigns different devices to different physical paths in distributing an I/O workload, so that all paths are used for one or more devices.

See also *load balancing* and *dynamic load balancing*.

STD
See standard volume.

storage area network (SAN)
Network of data storage disks. In large enterprises, a SAN connects multiple servers to a centralized pool of disk storage.

See also *network-attached storage (NAS)*.

storage device
Physical device that can attach to a SCSI device, which connects to the SCSI bus.

storage pool
Groups of available disk volumes organized by AVM that are used to allocate available storage to file systems. They can be created automatically by AVM or manually by the user.

See also *Automatic volume management (AVM)*

storage processor (SP)
Storage processor on VNX for block. On VNX for block, a circuit board with memory modules and control logic that manages the system I/O between the host's Fibre Channel adapter and the disk modules.

Storage processor A (SP A)
Generic term for the first storage processor in VNX for block.

Storage processor B (SP B)
Generic term for the second storage processor in VNX for block.

storage processor enclosure (SPE)
Shelf in VNX for block that includes an enclosure, storage processors (SPs), Fibre Channel link control cards (LCCs), two power supplies, and fan packs.

storage profile
Predefined set of parameters used to configure a disk volume. Every disk volume on VNX for file is associated with a single storage profile. The parameters specify the RAID type of the disk volume, the storage processor associated with the disk group, and other information.

storage service provider (SSP)
Third-party provider that manages the storage facilities for an enterprise.

stripe size
Number of blocks in one stripe of a stripe volume.

stripe volume
Arrangement of volumes that appear as a single volume. Allows for stripe units that cut across the volume and are addressed in an interlaced manner. Stripe volumes make load balancing possible.

See also *disk volume*, *metavolume*, and *slice volume*.

stub file
File that replaces the original file on VNX for file when the file is archived to secondary storage. The stub file contains all the metadata associated with the archived file and the information required by VNX for file to allow it to access the archived data on secondary storage when required.

subnet
Any network that is part of a larger IP network as identified by the IP address and subnet mask.

subnet mask
32-bit address mask used in IP to identify the bits of an IP address used for the subnet address.

Sun Java System Directory Server
Also known as Sun ONE Directory Server and iPlanet. A distributed directory service accessible by using LDAP.

SVFS
See Snapshot Virtual File System.

SVTL
See software virtual tape library.

switch
Network device that selects a path or circuit for sending data between destinations.

switch fabric
Combination of interconnected Fibre Channel switches used throughout a campus or large geographical area, which collectively provide a routing infrastructure.

switchover
Replication operation that snychronizes the destination object with the source, stops the replication with no data loss, and then mounts the destination object read/write and the source object read-only.

symbolic link
File that points to another file or directory.

symmetric cipher
A symmetric cipher is a secret key that can be used for both decryption and encryption. An asymmetric cipher does not have this behavior. Some examples of symmetric ciphers are RC4, 3DES, and AES.

Symmetrix Integrated Cached Disk Array (Symmetrix ICDA)
Storage array that provides centralized, sharable enterprise storage. It helps create an information infrastructure capable of managing large, complex ultra-dynamic storage area network (SAN) environments by consolidating storage from multiple heterogeneous hosts onto a single system.

Symmetrix Remote Data Facility (SRDF)
EMC technology that allows two or more Symmetrix systems to maintain a remote mirror of data in more than one location. The systems can be located within the same facility, in a campus, or hundreds of miles apart using fibre or dedicated high-speed circuits. The SRDF family of replication software offers various levels of high-availability configurations, such as SRDF/Synchronous (SRDF/S) and SRDF/Asynchronous (SRDF/A).

System
Array of physical disk drives and their supporting processors, power supplies, and cables.

system configured concurrent streams
The number of NDMP backup or restore streams that can run concurrently. This number can be modified by using the server_param command.

system-defined storage pool
Predefined AVM storage pools that are set up to help you easily manage both storage volume structures and file system provisioning by using AVM.

T

tagging
See frame tagging.

tape library unit (TLU)
Physical device that contains and manages sets of tape drives and cartridges.

tar
Backup format in PAX that traverses a file tree in depth-first order.

target VNX for File
SRDF term for the remote (secondary) VNX for file. The target VNX for file is typically the "standby" side of a disaster recovery configuration.

TB
See terabyte.

TCP
See Transmission Control Protocol.

TCP Offload Engine (TOE)
TOE network interface card offloads TCP protocol stack processing from the host and helps improve network performance and reduce CPU utilization.

Telnet
Internet standard protocol for remote terminal connection, which allows a user at one site to interact with a remote device or system that expects terminal-mode traffic.

template
Predefined set of parameters used to configure all new disk drives that are added to the system.

terabyte (TB)
2 to the 40th power (1,099,511,627,776) bytes, or approximately 1 trillion bytes.

TFTP
See Trivial File Transfer Protocol.

thread
Sequential flow of control in a computer program. A thread consists of address space, a stack, local variables, and global variables.

three-way backup
NDMP backup that directs data from one Data Mover through a network connection to a remote Data Mover to its attached tape library backup device.

See also *heterogeneous three-way backup* and *remote backup*.

throttle schedule
See bandwidth schedule.

throughput
In computers, a measurement of the work that can be processed within a set time period. In networking, a measurement of the amount of data that can be successfully transferred within a set time period.

TID
See Transfer Identifier.

TimeFinder/FS
Business continuance configuration allowing customers to use Symmetrix business continuance volumes (BCVs) to provide a local or remote point-in-time copy of VNX for file.

time offset
Difference between local system time and time retrieved from a time server.

timeout
Time interval at which the system takes some predetermined action.

time out of sync
Maximum amount of time in minutes (1–1440), or hours that the source object and the destination object in a replication session can be out of synchronization before an update is performed.

time to live (TTL) time stamp
TTL time stamp is used to maintain the consistency of the credential. In case the TTL expires, the credential is rebuilt to take into account any modification that might have occurred.

TLS
See Transport Layer Security.

TLU
See tape library unit.

TOE
See TCP Offload Engine.

Transfer Identifier (TID)
Randomly chosen identifiers used by TFTP and passed to the Datagram layer to be used as ports during the connection. TIDs must be between 0 and 65,535.

Transmission Control Protocol (TCP)
Connection-oriented transport protocol that provides reliable data delivery.

Transport Layer Security (TLS)
Successor protocol to SSL for general communication authentication and encryption over TCP/IP networks. TLS version 1 is nearly identical with SSL version 3.

trap
Asynchronous message sent from an SNMP agent to an SNMP management program. Traps are typically used to report errors.

tree quota
Feature that lets you specify soft and hard quota limits on a directory tree. The usage is computed for all files created in the tree hierarchy.

Triple DES (3DES)
Triple DES is a block cipher developed from the Data Encryption Standard (DES) cipher.

Trivial File Transfer Protocol (TFTP)
Simple, UDP-based protocol to read and write files. TFTP can be used to boot remote clients from a network server, but does not authenticate users or provide access control.

trunk
Set of physical network devices bundled together for high availability. Ethernet channels and link aggregations are trunks.

TTL time stamp
See time to live (TTL) time stamp.

two-way back-up
NDMP backup that directs data from a Data Mover (NDMP server) to the tape library device attached to the Data Mover.

U

U
Unit of measurement for rackmount equipment. One U is 1.75 in. (4.44 cm).

UCS-2 (Universal Character Set-2)
An obsolete character encoding which is a predecessor to UTF-16.

UDP
See User Datagram Protocol.

UFS
See UNIX file system.

UFWD SCSI
See Ultra fast-wide differential SCSI.

UID
See User ID.

Ultra fast-wide differential SCSI (UFWD SCSI)
High-speed channel connection between Data Movers and the system.

See also *Fibre Channel*.

UNC
See universal naming convention.

Unicode
Family of universal character encoding standards used for representation of text for computer processing.

Unicode Consortium
Organization responsible for defining the behavior of and relationships among Unicode characters and for providing technical information to implementors (www.unicode.org).

Unicode or UCS Transformation Format-8 (UTF-8)
Multibyte encoding form, UTF-8, uses an algorithmic mapping scheme to convert every Unicode value to a unique 1- to 4-byte sequence with no embedded null characters.

unified storage
VNX for file that is connected to a captive system that is not shared with any other VNX for files and is not capable of connecting to multiple systems.

uniform resource locator (URL)
Address for a page in the World Wide Web. A URL usually consists of an access protocol, a domain name, and optionally a path to a file or other resource.

Unisphere for Block
Enables you to discover, monitor, provision, and report on VNX for block from your web browser.

Universal Extended File System (UxFS)
High-performance, VNX for File default file system, based on traditional Berkeley UFS, enhanced with 64-bit support, metadata logging for high availability, and several performance enhancements.

universal naming convention (UNC)
Standard for identifying servers, printers, and other resources in a network. Originated in the UNIX community.

UNIX file system (UFS)
Standard UNIX file system.

URL
See uniform resource locator.

User Datagram Protocol (UDP)
Connectionless transport protocol in the TCP/IP stack that allows datagrams to be exchanged without acknowledgements or a delivery guarantee.

user-defined storage pools
User-created storage pools containing volumes that are manually added. User-defined storage pools provide an appropriate option for users who want control over their storage volume structures while still using the automated file system provisioning functionality of AVM to provision file systems from the user-defined storage pools.

user file
Refers to the passwd file that resides on each Data Mover.

User ID (UID)
Numeric identifier that corresponds to a particular user.

Usermapper
Service that automatically maps distinct Windows users and groups to distinct UNIX-style UIDs and GIDs.

Usermapper host
Machine that runs an External Usermapper daemon or service.

UTC
See coordinated universal time.

UTF-8 (8-bit Unicode Transformation Format)
Multibyte encoding form that uses an algorithmic mapping scheme to convert every Unicode value to a unique 1- to 4-byte sequence with no embedded null characters.

See *Unicode* or *UCS Transformation Format-8*.

UTF-16 (16-bit Unicode Transformation Format)
Multibyte encoding form that supports the 16-bit Unicode or "wide" characters used by Windows. UTF-16 is an extension of UCS-2.

UxFS
See Universal Extended File System.

V

variable length subnet mask (VLSM)
Means of specifying different subnet masks for the same network on various subnets. VLSM maximizes the use of IP address space.

VBB
See volume based backup.

VC client
See virus-checking client.

VDM
See Virtual Data Mover.

Virtual Data Mover (VDM)
VNX for file software feature that enables users to administratively separate CIFS servers, replicate CIFS environments, and move CIFS servers from one Data Mover to another.

virtual device
Combination of multiple physical devices defined by a single MAC address.

virtual local area network (VLAN)
Group of devices physically residing on different network segments, but communicating as if they resided on the same network segment. VLANs are configured by management software and are based on logical connections as compared to physical connections for increased administrative flexibility.

Virtual Storage Area Network
SAN that can be broken up into sections allowing traffic to be isolated within the section. See VSAN.

virtual tape library unit (VTLU)
Software-based virtual tape library configured on a Data Mover that emulates a physical TLU. A VTLU allows NDMP to work with disk-based storage.

virtually provisioned iSCSI LUN
iSCSI LUN without reserved space on the file system. Adequate file system space must be available for allocation whenever data is added to the LUN.

virus-checking client (VC client)
Virus-checking agent component of VNX for file software that runs on the Data Mover.

See also *AV engine*, *AV server*, and *CAVA*.

virus definition file
File containing information for a virus protection program that protects a computer from the newest, most destructive viruses. This file is sometimes referred to as a virus signature update file, a virus pattern update file, or a virus identity (IDE) file.

See also *AV engine*, *AV server*, *CAVA*, and *VC client*.

VLAN
See virtual local area network.

VLSM
See variable length subnet mask.

VNX
EMC network-attached storage (NAS) product line.

VNX Event Enabler
Framework that provides the working environment for the CAVA and CEPA facilities.

VNX FileMover
Policy-based system used to determine where files should be physically stored. In most cases, policies are based on file size or last access time (LAT) or both and are used to identify data that can be moved to slower, less-expensive storage.

VNX FileMover API
API that enables integration between VNX for file and policy and archiving software applications to automatically monitor and manage the movement of files between primary and secondary image.

VNX for Block
EMC midrange block system.

volume
On VNX for File, a virtual disk into which a file system, database management system, or other application places data. A volume can be a single disk partition or multiple partitions on one or more physical drives.

See also *disk volume*, *metavolume*, *slice volume*, and *stripe volume*.

volume based backup (VBB)
See NDMP Volume Backup.

Volume Shadow Copy Service (VSS)
Windows service and architecture that coordinate various components to create consistent point-in-time copies of data called shadow copies.

VSAN
See Virtual Storage Area Network.

VSS
See Volume Shadow Copy Service.

VSS provider
Component in the VSS architecture that creates and maintains shadow copies.

VTLU
See virtual tape library unit.

W

WAN
See wide area network.

wide area network (WAN)
Private or public network that covers a wide geographical area.

Windows domain
Microsoft Windows domain controlled and managed by a Microsoft Windows Server by using the Active Directory to manage all system resources and by using the DNS for name resolution.

Windows Internet Naming Service (WINS)
Software service that dynamically maps IP addresses to computer names (NetBIOS names). This allows users to access resources by name instead of requiring them to use IP addresses that are difficult to recognize and remember. WINS servers support clients by running Windows NT 4.0 and earlier versions of Microsoft operating systems.

Windows NT domain
Microsoft Windows domain controlled and managed by a Microsoft Windows NT server by using a SAM database to manage user and group accounts and a NetBIOS namespace. In a Windows NT domain, there is one primary domain controller (PDC) with a read/write copy of the SAM, and possibly several backup domain controllers (BDCs) with read-only copies of the SAM.

See also *domain* and *domain controller*.

WINS
See Windows Internet Naming Service.

writeable snapshot
Read-write, point-in-time, logical image of a PFS created from a read-only (baseline) checkpoint.

See also *Production File System*.

write hit
Existence of room in cache for the data presented by the write operation.

write miss
Failed write operation due to lack of room in cache for the data presented.

X

X.509
Widely used standard for defining digital certificates.

XML
See Extensible Markup Language.

XML API
Interface for remotely managing and monitoring VNX for file. The interface uses XML formatted messages, and is programming language neutral.

Z

zones

Set of devices that can see one another, but cannot see other devices connected to the same connectivity product (such as a switch). In a Fibre Channel switch topology, several devices can be grouped into zones by function or by location.

Special Character

8859-1
Part 1 of ISO/IEC 8859, a standard character encoding of the Latin alphabet less formally referred to as Latin-1. Each character is encoded as a single eight-bit code value.