

Storage Networking Industry Association (SNIA)

SNIA is the globally recognized and trusted authority for storage leadership, standards, and technology expertise. Leading the storage industry by developing and promoting vendor-neutral architectures, standards and educational services that facilitate the efficient management, movement and security of information.

The SNIA Dictionary, 18th Edition

The SNIA Dictionary contains terms and definitions related to storage and other information technologies, and is the storage networking industry's most comprehensive effort to arrive at a common body of terminology for the technologies it represents. The terms go through a rigorous technical review and approval process by the SNIA Technical Council to assure their accuracy. The SNIA Technical Council is a group of technical experts elected by the members of SNIA to guide SNIA's technical efforts. Their extensive individual technical backgrounds cover all aspects of storage.

The reader should recognize that in this rapidly evolving field, new terminology is constantly being introduced, and common usage is shifting. SNIA regards this dictionary as a living document, to be updated as necessary to reflect a consensus on common usage, and encourages readers to treat it in that spirit. Suggestions for improvement are welcomed at any time and may be sent to dictionary@snia.org. SNIA owns the rights to all submitted comments and suggestions.

Proposals for new terms or definitions, or modifications to existing ones, should be submitted on the form located at:
<http://www.snia.org/education/dictionary/submittal>

Periodically SNIA regional groups translate the SNIA dictionary into local languages. There are versions of the dictionary in Japanese, Portuguese, and Chinese. If you would like to lead a translation project, SNIA would be interested to help support this effort. Please contact dictionary@snia.org.

Terms of Use

The SNIA hereby grants permission for individuals to use this glossary for personal use only, and for corporations and other business entities to use this glossary for internal use only (including internal copying, distribution, and display), provided that:

Any definition reproduced must be reproduced in its entirety with no alteration, and, any document, printed or electronic, in which material from this glossary (or any portion hereof) is reproduced must acknowledge the SNIA copyright on that material, and must credit the SNIA for granting permission for its reuse.

Other than as explicitly provided above, you may not make any commercial use of this glossary, sell any or all of this glossary, or distribute this glossary to third parties. All rights not explicitly granted above are expressly reserved to SNIA. In particular, the provisions above do not grant the rights to make any commercial use of this glossary, sell any or all of this dictionary, or distribute this dictionary to third parties.

Permission to use this glossary for purposes other than those enumerated above may be requested by e-mailing dictionary@snia.org; please include the identity of the requesting individual and/or company and a brief description of the purpose, nature, and scope of the requested use.

Copyright © 2004 - 2017 Storage Networking Industry Association, All Rights Reserved. Last updated July 28, 2017.

Definition Format

The format for definitions has changed as of the last half of 2008. Terms are now defined as much as possible using the substitution principle, which states that a term's definition should be substitutable for the term itself in a sentence.

In the case that more text is required or deemed helpful, it is contained in one or more separate paragraphs after the definition itself. This text is informative in nature, and while intended to be accurate, is not technically part of the definition itself.

Deprecated Synonyms

In many cases, as technology develops, companies are forced to invent new terminology to describe innovations in their products. As the technology matures and vendors attempt to compete and compare their products with others, one or two terms become the most widely used, yet a number of other terms may remain in some use which are basically synonyms for the widely used terms. This causes confusion in the marketplace. To encourage crispness and uniformity in product descriptions, this dictionary lists synonyms of this type as "Deprecated synonym for xxxx," where xxxx is the term determined to have become canonical in the industry. This is to indicate both the meaning of xxxx and guide the reader toward use of the more canonical term.

In cases where a synonym is not deprecated, the SNIA does not endorse the use of one synonym over another.

Definitions Taken from Standards Documents

The SNIA has a strong interest in keeping definitions harmonized across various industry groups and national and international standards bodies. Towards this end, some definitions, especially those pertaining to Fibre Channel and SCSI terms and technologies, have been quoted from the appropriate version of the INCITS standard. In all such cases, the INCITS standard is authoritative. The SNIA Dictionary may include terms defined in the the following standards and draft standards:

INCITS 302-1998, SCSI Parallel Interface - 2 (SPI-2)

INCITS 367-2003, SCSI Parallel Interface - 5 (SPI-5)

INCITS 405-2005, SCSI Block Commands - 2 (SBC-2)

INCITS 431-2007, Serial Attached SCSI - 2.1 (SAS-2.1)

INCITS 447-2008, SCSI Architecture Model - 4 (SAM-4)

INCITS 448-2008, SCSI Enclosure Services - 2 (SES-2)

INCITS 461-2010, Fibre Channel - Switch Fabric-5 (FC-SW-5)

INCITS 462-2010, Fibre Channel - Backbone-5 (FC-BB-5)

INCITS 466-2011, Fibre Channel - Single-Byte Command Code Sets - 4 (FC-SB-4)

INCITS 467-2011, SCSI Stream Commands - 3 (SSC-3)

INCITS 470-2011, Fibre Channel - Framing and Signaling - 3 (FC-FS-3)

INCITS 475-2011, Fibre Channel - Inter-Fabric Routing (FC-IFR)

INCITS 476-2011, SAS Protocol Layer (SPL)
INCITS 476/AM1-2012, SAS Protocol Layer Amendment #1 (SPL-AM1)
INCITS 477-2011, Fibre Channel – Link Service - 2 (FC-LS-2)
INCITS 478/AM1-2014, Serial Attach SCSI - 2.1 Amendment #1
(SAS-2.1-AM1)
INCITS 479-2011, Fibre Channel - Physical Interface - 5 (FC-PI-5)
INCITS 481-2012, Fibre Channel Protocol for SCSI - 4 (FCP-4)
INCITS 484-2012, SCSI Media Changer Commands - 3 (SMC-3)
INCITS 497-2013, Automation/Drive Interface – Commands - 3
(ADC-3)
INCITS 505-2013, SAS Protocol Layer - 2 (SPL-2)
INCITS 509-2014, Fibre Channel - Backbone - 6 (FC-BB-6)
INCITS 514-2014, SCSI Block Commands - 3 (SBC-3)
INCITS 516-2014, SCSI Stream Commands - 4 (SSC-4)
INCITS 519-2014, Serial Attached SCSI - 3 (SAS-3)
INCITS 556-201x, Fibre Channel NVMe (FC-NVMe)

The SNIA wishes to thank ANSI and INCITS for their cooperation in this matter.

Copies of INCITS standards may be purchased at ANSI's online store at <http://webstore.ansi.org>.

Context Hierarchy

Most of the terms in this dictionary have meaning primarily in specific sub-contexts of storage networking, such as SCSI or File Systems. The following categories are used to declare the context in which a given definition in this dictionary is held to be valid. No attempt has been made to date to rigorously define these categories, so they remain a guide to understanding, not a formal system.

- General
 - Hardware
 - Network
 - SCSI
 - iSCSI
 - Fibre Channel
 - NVMe
 - Infiniband
 - Data Communication
 - Computer System
 - Storage System
 - Operating System
 - Windows
 - Services
 - Cloud
 - Management
 - Data Management
 - Backup
 - Data Recovery
 - Data Security
 - Database
 - File System
 - Long Term Retention
 - Capacity Optimization
 - Storage Management
 - Energy
 - Standards
 - Legal

The context hierarchy is a work in progress. In part, we are constrained by practice in previous editions of the dictionary. In the above hierarchy representation, context labels indented beneath other context labels represent specializations of the higher-order label concept. Below is an example of how context is indicated:

context example

[Context] The context is called out in square brackets at the beginning of each definition, as in this example.

Authors

The following SNIA volunteers contributed to this version of the SNIA Dictionary:

Carlos Pratt, Chair of Dictionary Team
Mark Carlson, Toshiba
John Crandall, Brocade
Fred Knight, NetApp
Bill Martin, Samsung
Peter Murray, Virtual Instruments
Tom Talpey, Microsoft
David Thiel

Past contributors include:

David Black, EMC Corporation
Roger Cummings, Symantec
Don Deel, NetApp
Eric Hibbard, HDS
Leah Schoeb, Intel
Steve Wilson, Brocade
Alan G. Yoder

Thanks also to the many unsung contributors who have submitted suggestions through the online submission portal.

Numbers

3DES

[Data Security] Acronym for [Triple DES](#).

This algorithm is obsolete.

64B/66B

[Data Communication] An algorithm for encoding data for transmission in which each 64-bit data word is converted to a 66-bit [transmission character](#).

Each transmission character is prefixed with either binary "01" or binary "10". This, combined with scrambling, gives the signal desirable engineering properties, yet incurs a much lower overhead than the traditional 8b/10b encoding.

8B/10B encoding

[Data Communication] An algorithm for [encoding](#) data for transmission in which each eight-bit [data byte](#) is converted to a 10-bit [transmission character](#).

8B/10B encoding is used in transmitting data on [Fibre Channel](#), [ESCON](#), [Gigabit Ethernet](#), and [Serial Attached SCSI](#). It supports continuous transmission with a balanced number of ones and zeros in the code stream and detects single bit transmission errors.

A

AAA

[Data Security] Acronym for [Authentication](#), [Authorization](#), and Accounting.

access

[Data Security] The opportunity to make use of an [information system](#) resource.

access control

[File System] [Data Security] The granting or withholding of a service or access to a resource to a requestor based on the [identity](#) of the [principal](#) for which the requestor is acting.

Access Control Entry (ACE)

[File System] [Data Security] A single entry in an [Access Control List](#), which either denies or grants access to a given resource by one [principal](#) (a user or a group of users and/or groups).

Access Control List (ACL)

[File System] [Data Security] A persistent list, commonly composed of [Access Control](#) Entries (ACEs), that enumerates the rights of principals (users and groups of users and/or groups) to access resources.

access fairness

[Fibre Channel] A process by which [nodes](#) are provided access to a [Fibre Channel arbitrated loop](#) independently of other nodes' activity.

access method

1. [Operating System] The means used to access a physical transmission [medium](#) in order to transmit data.
2. [Operating System] In IBM Corporation's OS/390 operating system and its precursors, a file organization method, such as sequential, random, indexed, etc., and the operating system software used to implement it.

access path

[Storage System] The combination of adapters, addresses and routes through a switching fabric used by a computer to communicate with a [storage device](#).

Some configurations support multiple access paths to a single device. See [multi-path I/O](#).

account

[Data Security] An established relationship between a [principal](#) and a computer, network or service.

accountability

1. [Data Security] The property enabling principals' actions to be attributed to them in such a way that there is little possibility for denying responsibility for those actions.
2. [Data Security] The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity.

This supports non-repudiation, deterrence, fault isolation, [intrusion detection](#) and prevention, and after-action recovery and legal action. [NIST SP 800-27]

ACE

[File System] [Data Security] Acronym for [Access Control Entry](#).

ACL

[File System] [Data Security] Acronym for [Access Control List](#).

ACS

[Data Recovery] Acronym for [Automated Cartridge System](#).

active

1. [Fibre Channel] The state of a [Fibre Channel Sequence Initiator](#) between the start of transmission of the first [data frame](#) of a sequence and the completion of transmission of the last data frame in the sequence.
2. [Fibre Channel] The state of a Fibre Channel [Sequence Recipient](#) between the start of reception of the first data frame of a sequence and the completion of reception of the last data frame in the sequence.

active-active (components, controllers)

[Storage System] Synonym for [dual active components](#) or controllers.

Active archive

[Long term retention] A [long-term data retention](#) system that allows online access to retained file and object data.

active component

[Storage System] A system component that requires electrical power to operate, such as a [power supply](#), fan, or [controller](#).

active data

[Data Management] Data that is immediately accessible to an application without the need to stage it in from a lower tier of storage.

See [near-online data](#).

Active Directory (AD)

[Windows] A Microsoft technology for the central and hierarchical administration of large groups of computers, users and groups.

active-passive (components, controllers)

[Storage System] Synonym for [hot standby](#) components or controllers.

active power

[Energy] The power consumption of a system when powered on and under normal workload.

AD

[Windows] Acronym for [Active Directory](#).

adapter

[General] A hardware device—typically an add-in card or specialized component on a [system board](#)—that converts the timing and [protocol](#) of one bus or interface to another, to enable a computer system's processing hardware to access peripheral devices.

A [Fibre Channel Host Bus Adapter](#) and an [Ethernet Network Interface Card](#) are both kinds of adapters.

adaptive array

[Storage System] A [disk array](#) that is capable of changing its virtual-to-physical location [mapping](#) algorithm—e.g., from mirrored to [parity RAID](#)—while the array is operating.

ADC

1. [Hardware] Acronym for [Analog Digital Converter](#).
2. [SCSI] Acronym for the [INCITS T10](#) Automation/[Drive](#) Interface – Commands standards family.

address

1. [Computer System] A fixed length bit pattern that uniquely identifies a [block](#) of data stored on a disk or tape.
2. [Computer System] A fixed-length bit pattern that uniquely identifies a location (bit, byte, word, etc.) in a computer memory.

3. [SCSI] An identifier whose value uniquely identifies a [SCSI port](#) connected to a [SCSI interconnect](#) for purposes of communication.
4. [Network] A bit pattern that uniquely identifies a device on a network.

address identifier

[Fibre Channel] A 24-bit value used to identify the source ([S_ID](#)) or destination ([D_ID](#)) of a [frame](#), as specified in the [FC-FS-2](#) standard.

The FC-SW-4 standard includes a table of special address identifier values and their meanings. See [S_ID](#), [D_ID](#), [FC-FS-2](#), [FC-SW-4](#).

address resolution

[Network] The process of determining a [MAC](#) address, given a more abstract [LAN](#) or [WAN](#) address.

Address Resolution Protocol (ARP)

1. [Network] Any [protocol](#) used to obtain a [mapping](#) from a higher layer address to a lower layer address; when abbreviated as [ARP](#), the [Ethernet Address Resolution](#) Protocol (see 2) is most often meant.
2. [Network] The protocol used by an [IP](#) networking layer to map IP addresses to lower level hardware (i.e., [MAC](#)) addresses.

addressing

[Computer System] An algorithm by which areas of fixed disk, removable cartridge [media](#), or computer system main memory are uniquely identified.

See [block addressing](#), [C-H-S addressing](#), [explicit addressing](#), [implicit addressing](#).

administration host

[Storage System] A computer that manages one or more storage subsystems (e.g., filers, [disk array](#) subsystems, tape subsystems, etc.).

administrator

[Storage System] [Data Security] A person charged with the installation, [configuration](#), and management of a computer system, network, [storage subsystem](#), database, or application.

Advanced Encryption Standard (AES)

[Data Security] A [cryptographic algorithm](#) designated by [NIST](#) as a replacement for [DES](#).

Advanced Technology Attachment (ATA)

[Storage System] A standard designed to connect hard and removable disk drives.

ATA is also the official name for [Integrated Drive Electronics \(IDE\)](#).

adverse inference

[Legal] Inference that destroyed or missing evidence (data) would have been harmful to a party who failed to provide it.

AES

[Data Security] Acronym for [Advanced Encryption Standard](#).

AFA

[Storage System] Acronym for [All Flash Array](#).

agent

[General] A program that performs one or more services (such as gathering information from the Internet), acting for or as a [principal](#).

aggregation

[Network] [Storage System] A process related to consolidation, consisting of combining multiple similar and related objects or operations into a single one.

AH

[Data Security] Acronym for [Authentication Header](#).

AISL

[Fibre Channel] Acronym for [Augmented ISL](#).

AISL Set

[Fibre Channel] A set of AISLs that connect the controlling switches that are part of a distributed switch.

AIT

[Storage System] Acronym for Advanced Intelligent Tape.

algorithmic mapping

[Computer System] Use of an algorithm to translate from one data [addressing domain](#) to another.

If a [volume](#) is algorithmically mapped, the physical location of a [block](#) of data may be calculated from its virtual volume address using known characteristics of the volume (e.g., [stripe depth](#) and number of [member](#) disks). See [dynamic mapping](#), [tabular mapping](#).

alias

[General] An alternate name for an entity, sometimes used to create names that are more easily human readable.

alias address identifier

[Fibre Channel] One or more address identifiers that may be recognized by an [N_Port](#) in addition to its N_Port Identifier, used to form groups of N_Ports so that frames may be addressed to a group rather than to individual N_Ports.

See [multicast group](#).

AL_PA

[Fibre Channel] Acronym for [Arbitrated Loop Physical Address](#).

all flash array

[Storage System] A synonym for *all solid state* [array](#).

all solid state array

[Storage System] A storage subsystem where all persistence is performed by [solid state storage](#).

alternate client restore

[Data Recovery] The process of restoring files to a different [client](#) than the one from which they were backed up.

alternate path restore

[Data Recovery] The process of restoring files to a different [directory](#) than the one from which they were backed up.

always on

1. [General] The state of always having power applied (systems) or of being continually active (communication links).
2. [Fibre Channel] A state of an [operational](#) link of always being powered on and continually transmitting either data frames, idles or fill words, in contrast to bursty transmissions and listening for a quiet line in earlier 10 and 100 [Mbit/sec Ethernet](#).

American National Standards Institute (ANSI)

[Standards] A body that coordinates the development and use of voluntary consensus standards in the United States and represents the needs and views of U.S. stakeholders in international standardization forums around the globe.

ANSI accredits both standards certification organizations and standards development organizations. The IEEE Standards Association (which standardizes [Ethernet](#) and many other technologies) and [INCITS](#) (which standardizes [SCSI](#), [Fibre Channel](#), MPEG, and many other technologies) are two of over 100 ANSI accredited standards organizations.

Analog Digital Converter (ADC)

[Hardware] A device that converts a continuously valued (analog) input to a discretely valued (digital) output.

ANSI

[Standards] Acronym for [American National Standards Institute](#).

ANSI T10

[Standards] The standards development committee accredited by [INCITS](#) to develop [SCSI](#) standards for communication between host devices (initiators) and [storage device](#) controllers (targets).

The full name of this committee is the INCITS SCSI Storage Interfaces Technical Committee (INCITS TC T10).

ANSI T11

[Standards] The standards development committee accredited by [INCITS](#) to develop standards related to [Fibre Channel](#), related [serial](#) storage interfaces, and certain storage management interfaces.

The full name of this committee is the INCITS Fibre Channel Interfaces (T11) Technical Committee (INCITS TC T11).

API

[General] Acronym for [Application Programming Interface](#).

A_PORT

[Fibre Channel] A type of port used to communicate within a Fibre Channel distributed switch.

A_PORT Switch Link (ASL)

[Fibre Channel] A link connecting one A_Port to another A_Port.

appliance

[General] An [intelligent device](#) programmed to perform a single well-defined function, such as providing file, web, network or print services.

Appliances differ from general purpose computers in that their software is normally customized for the function they perform, pre-loaded by the vendor, and not alterable by the user. See [filer](#).

application

[Storage System] A [client](#) of a storage system.

Applications range from desktop productivity applications to enterprise-wide federated applications spanning multiple databases and file systems.

application I/O request

application read request

application write request

[Storage System] I/O requests made by storage clients, as distinguished from I/O requests made by a [storage subsystem](#)'s own [control software](#).

Application Programming Interface (API)

[General] An interface used by an application program to request services.

The term *API* is usually used to denote interfaces between applications and the software components that comprise the [operating environment](#) (e.g., operating system, [file system](#), [volume manager](#), device drivers, etc.).

Application Response Measurement

[Standards] An Open Group technical standard, being advanced in both The Open Group and the [Distributed Management Task Force](#), which defines function calls for transaction monitoring.

Application Specific Integrated Circuit (ASIC)

[Computer System] An integrated [circuit](#) designed for a particular application, such as interfacing to a [SCSI interconnect](#).

arbitrated loop

1. [Fibre Channel] A [Fibre Channel interconnect topology](#) in which each port is connected to the next, forming a loop. At any instant, only one port in a [Fibre Channel Arbitrated Loop](#) can transmit data. Before transmitting data, a port in a Fibre Channel Arbitrated Loop must participate with all other ports in the loop in an [arbitration](#) to gain the right to transmit

data. The arbitration logic is distributed among all of a loop's ports.

2. [Fibre Channel] The version of the [Fibre Channel protocol](#) used with the arbitrated loop physical topology.

Arbitrated Loop Physical Address (AL_PA)

[Fibre Channel] An 8-bit value used to identify a participating device in an [Arbitrated Loop](#).

arbitration

[General] Any process by which a user of a shared resource—such as a port connected to a shared bus—negotiates with other users for the (usually temporary) right to use the resource (in the given example, by transmitting data on the bus).

archive

1. [Data Management] A collection of data objects, perhaps with associated [metadata](#), in a storage system whose primary purpose is the [long-term preservation](#) and retention of that data.
2. [Data Management] Synonym for [data ingestion](#).
3. An organization of people and systems that have accepted the responsibility to protect, retain, and preserve information and data and make it available for a Designated Community.
(Source: ISO 14721)

ARM

1. [General] Acronym for [Application Response Measurement](#).
2. [Computer System] A common microprocessor architecture, as well as the name of the company that created the architecture.

ARP

[Network] Acronym for [Address Resolution Protocol](#).

array

[Storage System] A [storage array](#), i.e., a [disk array](#) or tape array.

array configuration

1. [Storage System] Assignment of the disks and operating parameters for a [disk array](#) by setting parameters such as [stripe depth](#), [RAID](#) model, [cache](#) allowance, [spare](#) disk assignments, etc. See [configuration](#), [physical configuration](#).
2. [Storage System] The arrangement of disks and operating parameters that results from such an assignment.

ASIC

[Computer System] Acronym for [Application Specific Integrated Circuit](#).

ASL

[Fibre Channel] Acronym for [A Port Switch Link](#).

assigned capacity

[Storage System] The amount of space on a system or data container which has been allotted to be written by an end user or application.

On [thin provisioning](#) systems, an assigned capacity number represents a promise that that amount of space will be provided on demand; [usable capacity](#) is allocated as the container is written. On fully provisioned systems, usable capacity must be committed at the same time the container is allocated. See [thin provisioning](#).

Association ID

[Fibre Channel] A value that uniquely identifies an NVMeoFC association.

assurance

[Data Security] A process for demonstrating that the security goals and objectives for an IT product or system are met on a continuing basis.

assurance level

[Data Security] The measure of confidence that the security features, practices, procedures, and architecture of an

[information system](#) accurately mediate and enforce the security [policy](#).

asymmetric cryptography

[Data Security] A [Cryptography](#) that uses an asymmetric [cryptosystem](#).

asymmetric cryptosystem

[Data Security] A [cryptographic algorithm](#) in which different keys are used to encrypt and decrypt a single message or [block](#) of stored information.

One of the keys is kept secret and referred to as a [private key](#); the other key can be freely disclosed and is called a [public key](#).

asymmetric encryption

[Data Security] Synonym for [public key cryptography](#).

asymmetric virtualization

[Computer System] Synonym for [out-of-band virtualization](#).

Out-of-band virtualization is the preferred term.

asynchronous I/O operation

[Storage System] An [I/O operation](#) whose [initiator](#) does not await its completion before proceeding with other work, enabling an initiator to have multiple concurrent I/O operations in progress.

asynchronous I/O request

[Storage System] A request to perform an [asynchronous I/O operation](#).

asynchronous mirroring

[Storage System] Deprecated synonym for [asynchronous replication](#).

asynchronous replication

[Storage System] A replication technique in which data must be committed to storage at only the primary site and not the secondary site before the write is acknowledged to the host.

Data is then forwarded to the secondary site as the network capabilities permit.

Asynchronous Transfer Mode (ATM)

[Network] A [connection](#)-oriented data communications technology based on switching 53 byte fixed-length units of data called *cells*.

[ATM](#) transmission rates are multiples of 51.840 Mbits per second. Each cell is dynamically routed. In the United States, a public communications service called [SONET](#) uses ATM at transmission rates of 155, 622, 2048, and 9196 Mbits per second. These are called OC-3, OC-12, OC-48, and OC-192 respectively. A similar service called [SDH](#) is offered in Europe. ATM is also used as a [LAN](#) infrastructure, sometimes with different transmission rates and coding methods than are offered with SONET and SDH.

ATA

[Storage System] Acronym for [Advanced Technology Attachment](#).

ATM

[Network] Acronym for [Asynchronous Transfer Mode](#).

atomic operation

[General] An operation that, from an external perspective, occurs either in its entirety or not at all.

For example, database management systems that implement the concept of *business transactions* treat each business transaction as an atomic operation on the database. This means that either all of the database updates that comprise a transaction are performed or none of them are performed; it is never the case that some of them are performed and others not. [RAID](#) arrays must implement atomic write operations to properly reproduce single-disk semantics from the perspective of their clients.

attack

[Data Security] Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself. [CNSSI-4009]

attenuation

[Network] The power loss between an optical or electrical [transmitter](#) and a [receiver](#), expressed in units of decibels (dB).

audit

[General] Independent review and examination of records and activities to assess the adequacy of controls, to ensure [compliance](#) with established policies and [operational](#) procedures, and to recommend necessary changes in controls, policies, or procedures.

audit log

[Data Security] Synonym for [audit trail](#).

audit trail

[Network] [Data Security] A chronological record of system activities that enables the [reconstruction](#) and examination of a [sequence](#) of events and/or changes in a system such as an [information system](#), a communications system or any transfer of sensitive material and/or information.

Augmented ISL (AISL)

[Fibre Channel] An E_Port to E_Port link used by the FC-SW redundancy protocol.

authentic

1. [General] Being genuine, or accurate in representation of facts.
2. [Legal] For evidence, being found by a jury (or trier of fact) to be what it purports to be and thus being worthy of [trust](#), reliance, or belief.

authentication

1. [Data Security] The act of verifying the [identity](#) claimed by a party to an interaction.
2. [Legal] The act of meeting the threshold level for admissibility, but not necessarily of [authenticity](#), of evidence (e.g., [ESI](#)).

authentication header

[Data Security] A component of [IPsec](#), standardized by the [IETF](#), that permits the specification of various [authentication](#) mechanisms designed to provide connectionless [integrity](#), data origin authentication, and an [optional](#) anti-replay service.

authenticity

1. [Data Management] Synonym for [data integrity](#).
2. [Data Security] The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. [NIST SP 800-53]
3. [Legal] The property, condition, or quality of being worthy of [trust](#), reliance, or belief because the proponent (offeror) has shown enough corroborating evidence to a jury (or trier of fact) to warrant such.

authorization

1. [Network] The process of determining—for example via [access control](#)—that a requestor is allowed to receive a service or perform an operation.
2. [Data Security] The limiting of usage of [information system](#) resources to authorized users, programs, processes or other systems, formally described as controlling usage by subjects of objects.

Automated Cartridge System

[Data Recovery] Synonym for tape cartridge handling [robot](#).

automated storage tiering

[Storage System] Automatic movement of data between storage tiers based on [policy](#).

The tiers may be within a single storage system or may span storage systems, including a [cloud storage](#) tier.

automatic backup

[Data Recovery] A [backup](#) triggered by an event (e.g., a schedule point, or a threshold reached) rather than by human action.

automatic failover

[Storage System] [Failover](#) that occurs without human intervention.

automatic swap

[Computer System] The [substitution](#) of a [replacement unit](#) (RU) in a system for a defective one, where the substitution is performed by the system itself while it continues to perform its normal function (possibly at a reduced rate of performance).

Automatic swaps are functional rather than physical substitutions, and do not require human intervention. Ultimately, however, defective components must be replaced in a physical hot, warm, or cold swap operation. See [cold swap](#), [hot swap](#), [warm swap](#), [hot spare](#).

automatic switchover

[Storage System] Deprecated synonym for [automatic failover](#).

autonomic storage management

[Storage System] The ability of a storage system to self-regulate attributes such as capacity, performance, and [resiliency](#) based on application demands, without any administrative intervention.

auto-swap

[Computer System] Abbreviation for [automatic swap](#).

See [cold swap](#), [hot swap](#), [warm swap](#).

auto-tiering

[Storage System] Synonym for [automated storage tiering](#).

availability

1. [General] The amount of time that a system is available during those time periods when it is expected to be available, often measured as a percentage of an elapsed year.
For example, 99.95% availability equates to 4.38 hours of downtime in a year ($0.0005 * 365 * 24 = 4.38$) for a system that is expected to be available all the time. See [data availability](#), [high availability](#).
2. [General] The property of being accessible and usable upon demand by an authorized entity.
[ISO/IEC 27000]

available capacity

[Data Management] [Storage System] Synonym for [free space](#).

B

B_Port

[Fibre Channel] The "[Bridge](#)" port within a bridge device used to extend a [Fibre Channel](#) inter-switch link; it connects only to an [E_Port](#) on a Fibre Channel switch.

B2D

[Data Recovery] Acronym for [Backup to Disk](#).

B2T

[Data Recovery] Acronym for [Backup to Tape](#).

backup

1. [Data Recovery] A collection of data stored on (usually removable) non-volatile [storage media](#) for purposes of [recovery](#) in case the original copy of data is lost or becomes inaccessible; also called a [backup copy](#).
To be useful for recovery, a backup must be made by copying the source data image when it is in a consistent state.
2. [Data Recovery] The act of creating a backup. See [archive](#).

backup client

[Data Recovery] A computer system containing online data to be backed up.

backup copy

[Data Recovery] A recoverable copy of a given set of data.

See [replica](#).

backup manager

[Data Recovery] An application program whose purpose is to schedule and manage [backup](#) operations.

backup policy

[Data Recovery] An IT installation's rules for how and when [backup](#) should be performed, such as which files or directories are to be backed up, the schedule on which backups should occur, which devices and [media](#) are eligible to receive the backups, how many copies are to be made, and actions to be performed if a backup does not succeed.

Backup to Disk (B2D)

[Data Recovery] [Backup](#) onto disk [media](#).

Backup to Tape (B2T)

[Data Recovery] [Backup](#) onto tape [media](#).

backup window

[Data Recovery] An interval of time during which a set of data can be backed up without seriously affecting applications that use the data.

For example, if an application accesses data from 8 AM until midnight, then the window between midnight and 8 AM is available for making [backup](#) copies. Offline backups require that applications not update data during the backup. Online backups typically use [point in time copy](#) technology to create consistent images of data for backup. If a backup uses different resources (storage devices, I/O paths, processing power) than the application, as is common with split [mirror](#) point-in-time copies, then the backup window is the time required to create the image. If the [online backup](#) shares resources with the applications using the data, as is common with copy-on-write

point in time copies, the backup window may be increased due to resource contention.

Bandwidth

1. [General] The numerical difference between the upper and lower frequencies of a band of electromagnetic radiation.
2. [Data Communication] A deprecated synonym for [data transfer capacity](#) that is often incorrectly used to refer to throughput.

bandwidth-length product

[Network] A figure of merit for optical fiber, usually expressed as MHz*kilometer.

As an example, a [Fibre Channel](#) link operating at 1 [Gb/s](#) using a fiber with a [bandwidth](#)-length product of 500 MHz*kilometer will support a link distance of approximately 500 meters.

baud

[Network] The maximum rate of signal state changes per second on a communications [circuit](#).

If each signal state change corresponds to a [code bit](#), then the baud rate and the bit rate are the same. It is also possible for signal state changes to correspond to more than one code bit, so the baud rate may be lower than the code bit rate.

BBB_credit

[Fibre Channel] Buffer-to-buffer [credit](#); used to determine how many frames can be sent to a recipient when [buffer to buffer flow control](#) is in use.

BCP

[General] Acronym for [Best Current Practice](#).

beginning running disparity

[Fibre Channel] For a data stream using [8B/10B encoding](#), the [running disparity](#) present at a [transmitter](#) or [receiver](#) when an [ordered set](#) is initiated.

BER

[Network] [Storage System] Acronym for [Bit Error Rate](#).

Berkeley RAID Levels

[Storage System] A classification of [disk array data protection](#) and [mapping](#) techniques developed by Garth Gibson, Randy Katz, and David Patterson in papers written while they were performing research into I/O subsystems at the University of California at Berkeley.

There are six Berkeley [RAID](#) Levels, usually referred to by the names [RAID Level 1](#), etc., through [RAID Level 6](#). See [RAID 0](#), [RAID 1](#), [RAID 2](#), [RAID 3](#), [RAID 4](#), [RAID 5](#), [RAID 6](#). Many other levels such as RAID 10, RAID 50 and so on have since been proposed.

Best Current Practice (BCP)

[General] A recommendation for what is currently believed to be the best manner of proceeding.

best effort (class of service)

[Fibre Channel] [Network] A [class of service](#) that does not guarantee delivery of packets, frames, or datagrams, but for which the network, fabric, or [interconnect](#) makes every reasonable delivery effort.

bidirectional authentication

[Data Security] Synonym for [mutual authentication](#).

big data

[Computer System] A characterization of datasets that are too large to be efficiently processed in their entirety by the most powerful standard computational platforms available.

big endian

[Computer System] A format for the storage and transmission of binary data in which the most significant bits are stored at the numerically lowest addresses, or are transmitted first on a [serial](#) link.

BIOS ([Basic Input Output System](#))

[Computer System] A relatively small program that resides in programmable, [non-volatile memory](#) on a personal computer and that is responsible for booting that computer and performing certain operating system independent I/O operations.

Standard BIOS interrupts are defined to allow access to the computer's disk, video and other hardware components (for example, INT13 for disk access).

bit

[Computer System] A binary digit.

bit error rate (BER)

[Network] [Storage System] The probability that a transmitted bit will be erroneously received.

The [BER](#) is measured by counting the number of bits in error at the output of a [receiver](#) and dividing by the total number of bits in the transmission. BER is typically expressed as a negative power of 10.

bit synchronization

[Data Communication] The process by which the [receiver](#) of a [serial](#) communication establishes its clocking used to locate code bits in a received data stream.

blade system

[Computer System] A computer or storage system composed of a chassis that provides power, cooling and other common infrastructure, and one or more removable [server](#) or storage units, usually called blades.

Blade systems are designed as a scalable solution to efficiently package and operate multiple processing or storage units in a single enclosure, and are designed for technicians to be able to easily add or replace hot-swappable boards in the field.

blanking plate

[General] [Energy] A solid plate that mounts over unused data center rack slots to maintain efficient air flow through components in the rack.

Blanking plates are also used for aesthetic reasons.

blind mating

[Hardware] The ability of pairs of components to be connected without the electrical or optical [connection](#) points being visible.

Blind mating is usually accomplished by mechanical guides (e.g., slots and rails) on the components.

block

1. [Storage System] The unit in which data is stored and retrieved on disk and tape devices; the atomic unit of data recognition (through a preamble and block header) and protection (through a [CRC](#) or [ECC](#)).
2. [Fibre Channel] A unit of application data from a single [information category](#) that is transferred within a single [sequence](#).

block addressing

[Storage System] An algorithm for uniquely identifying blocks of data stored on disk or tape [media](#) by number, and then translating these numbers into physical locations on the media.

See [C-H-S addressing](#).

block cipher

[Data Security] A symmetric encryption algorithm that operates on a block of plaintext, i.e., a string of bits of a defined length, to yield a block of ciphertext. [ISO/IEC 10116]

block services

[Storage System] A subsystem that provides block level access to storage for other systems or other layers of the same system. See [block](#).

block virtualization

[Storage System] The act of applying [virtualization](#) to one or more [block](#) based (storage) services for the purpose of providing a new aggregated, higher level—e.g., richer, simpler, more secure—block service to clients.

Block virtualization functions can be nested. A [disk drive](#), [RAID](#) system or [volume manager](#) all perform some form of block address to (different) block address [mapping](#) or [aggregation](#). See [file virtualization](#).

BNC (Bayonet Neill–Concelman) connector

[Network] A type of [coaxial cable](#) connector formerly used in Ethernet applications; the specification is contained in EIA/TIA 403-A and MIL-C-39012.

boot**booting****bootstrapping**

[Computer System] The process of loading Operating System code from a disk or other [storage device](#) into a computer's memory and preparing it to run.

Bootstrapping is an appropriate term since a code load typically occurs in steps, starting with a very simple program ([BIOS](#)) that initializes the computer's hardware and reads a [sequence](#) of data blocks from a fixed location on a pre-determined disk, into a fixed memory location. The data thus read is the code for the next stage of bootstrapping—usually an operating system loader. The loader completes the hardware setup and results in an executing operating system, in memory.

break mirror

[Storage System] Remove a [mirror](#) component from the mirror and make it a standalone [volume](#) in the system, voiding its [synchronization](#) relationship with the other mirror components.

bridge

1. [Fibre Channel] A [Fibre Channel](#) technology that provides a transparent fabric extension between two [switch](#) E_Ports

through the use of 2 B_Ports [tunneling](#) through some alternative technology, resulting in an Inter-Switch Link (ISL) that “appears” to be a direct link between switches.

For example, a bridge pair can take an incoming Fibre Channel [frame](#) from one B_Port on a Bridge, encapsulate that frame using FCIP (Fibre Channel over [IP](#)) and transmit the frame as [payload](#) over an IP network to the remote Bridge where the original frame is forwarded to the remote Fibre Channel Fabric switch E_Port through the remote Bridge’s B_Port.

2. [Fibre Channel] A Fibre Channel technology that enables traffic carried along part of the path from a source device by Fibre Channel, (for example commands, blocks, status and control between a [SCSI initiator](#) or [target](#) source device) to be extended to the destination device using an alternative physical transport network technology (for example [iSCSI](#) or [SCSI Interconnect](#)).

In some cases this “Bridge” is also referred to as a physical transport gateway, or storage router.

3. [Network] A device that connects multiple [LAN](#) segments at the physical address layer.

As opposed to a [hub](#), which indiscriminately rebroadcasts everything from one segment to the other, a bridge only retransmits traffic from one segment to another when the traffic is intended for the destination segment.

broadcast

[Fibre Channel] The simultaneous transmission of a message to all receivers (ports) connected to a communication facility.

Broadcast can be contrasted with unicast (sending a message to a specific receiver) and multicast (sending a message to select subset of receivers). In a [Fibre Channel](#) context, broadcast specifically refers to the sending of a message to all N_Ports connected to a fabric. See [multicast](#), [unicast](#).

buffer

[Computer System] A solid state memory device or programming construct, used to hold data momentarily as it moves along an I/O path or between software components.

buffer to buffer flow control

[Fibre Channel] Flow control that occurs between two directly connected [Fibre Channel](#) ports, e.g., an [N_Port](#) and its associated [F_Port](#).

A port indicates the number of frames that can be sent to it (its buffer [credit](#)) before the sender is required to stop transmitting and wait for the receipt of a "ready" indication. Buffer to buffer flow control is used only when an [NL_Port](#) is logged into another [NL_Port](#) on an [Arbitrated Loop](#) or when an [Nx_Port](#) is logged into an [FX_Port](#)." or "Flow control that occurs between two directly connected Fibre Channel ports, e.g., an [N_Port](#) and its associated [F_Port](#) or between two [E_Ports](#). A port indicates the number of frames that can be sent to it (its buffer credit), before the sender is required to stop transmitting and wait for the receipt of additional credit.

business continuity

[Data Security] Processes and/or procedures for ensuring continued business operations. [ISO/IEC 27000]

bypass circuit

[Fibre Channel] A [circuit](#) that removes a device from a data path (such as a [Fibre Channel arbitrated loop](#)) when valid signaling is lost, or a [controller](#) directs the removal of the device for any reason.

byte

[Computer System] An 8 bit unit of data.

Byte and bit ordering and meaning vary depending on context. It is necessary to consult the standards that apply in a given context to determine ordering and meaning.

C

C

CA

[Data Security] Acronym for [Certificate Authority](#).

cable plant

[Network] All of an installation's passive communications elements (e.g., optical fiber, twisted pair, or [coaxial cable](#), connectors, splices, etc.) between transmitters and receivers.

cache

1. [Computer System] To store data temporarily for expedited access.
2. [Computer System] The location in which data is stored temporarily.

There are a variety of cache types. Read cache holds data in anticipation that it will be requested. Write cache holds data written by a [client](#) until it can be stored on other (typically slower) [storage media](#) such as disk or tape. See [buffer](#), [disk cache](#), [write back cache](#), [write through cache](#).

canister

[Storage System] An enclosure for a single disk or tape.

Canisters are usually designed to [mount](#) in shelves that supply power, cooling, and [I/O interconnect](#) services to the devices. They are used to minimize RF emissions and to simplify insertion and removal of devices in multi-device storage subsystems. See [shelf](#).

CAP Theorem (Consistency, Availability, and Partition Tolerance)

A hypothesis that it is impossible for a distributed system to provide Consistency, Availability, and Partition Tolerance guarantees at the same time.

See [eventual consistency](#).

capacity optimization methods

[Storage System] Methods which reduce the consumption of space required to store a data set, such as [compression](#), [data deduplication](#), [thin provisioning](#), and delta snapshots.

[RAID 5](#) and 6 may also be considered as capacity optimizing methods, as they use less space than ordinary [mirroring](#) to perform a necessary function: protecting data from [storage device](#) failure.

capacity optimizing system

[Storage System] A system which employs at least one capacity optimization method.

capacity planning

[General] The process of optimizing supply of a given resource to satisfy current and future demand for that resource.

Common methods used for capacity planning include tracking, trending, forecasting and scenario planning to predict future demand.

carousel

[Data Recovery] A [media](#) handling [robot](#) in which the media are stored in and selected from a rotating wheel.

Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

[Network] A physical layer data transmission [protocol](#) used in [Ethernet](#) and fast Ethernet networks.

Carrier sense refers to [arbitration](#) for a shared link. Unlike "[always on](#)" physical protocols, carrier sense protocols require a [node](#) wishing to transmit to wait for the absence of carrier (indicating that another node is transmitting) on the link.

Multiple access refers to the party line nature of the link. A large number of nodes (up to 500 in the case of Ethernet) share access to a single link. Collision detection refers to the possibility that two nodes will simultaneously sense absence of carrier and begin to transmit, interfering with each other. Nodes are required to detect this interference, and cease transmitting. In the case of Ethernet, each node detecting a collision is required to wait for a random interval before attempting to transmit again.

cascading

[Fibre Channel] The process of connecting two or more [Fibre Channel](#) hubs or switches together to increase the number of ports or extend distances.

catalog

1. [Data Recovery] A stored list of backed up files and directories and the locations ([media](#) identifiers) of the [backup](#) copies.
2. [File System] A persistent data structure used by some file systems to keep track of the files they manage.

CBC

[Data Security] Acronym for [Cipher Block Chaining](#).

CC

[Data Security] Acronym for [Common Criteria](#).

CDB

[SCSI] Acronym for [Command Descriptor Block](#).

CDMI

[Standards] Acronym for [Cloud Data Management Interface](#).

CDP

[Data Recovery] Acronym for [Continuous Data Protection](#).

CDR

[Fibre Channel] Acronym for Clock and Data [Recovery](#).

certificate

[Data Security] A data structure signed with a [digital signature](#) that is based a [public key](#) and which asserts that the key belongs to a [subject](#) identified in the structure.

Certificate Authority (CA)

[Data Security] In a [Public Key Infrastructure \(PKI\)](#), the authority and organization responsible for issuing and revoking user certificates, and ensuring [compliance](#) with the PKI policies and procedures.

The reputation of the certificate authority determines the trust that may be placed in the identity assurance provided by the certificates issued by the authority.

Certificate Revocation List (CRL)

[Data Security] A time-stamped list of certificates, signed by the issuing [Certification Authority](#), that have been revoked by that [CA](#).

The CRL is made available to entities that need to rely on a certificate for [authentication](#).

chain of custody

[Legal] A process that tracks the movement of evidence through its collection, safeguarding, and analysis lifecycle by documenting each person who handled the evidence, the

date/time it was collected or transferred, and the purpose for the transfer. [NIST SP 800-72]

challenge

[Data Security] A step in an [authentication](#) dialog that must be answered using either a secret or process assumed to be known only by the other party.

A challenge can be as simple as “What’s your [password](#)?” or as complex as “Send me the result of a retinal scan of your right eye.”

Challenge Handshake Authentication Protocol (CHAP)

[Data Security] A [password](#)-based [authentication protocol](#) that uses a [challenge](#) to verify that a user has access rights to a system.

A hash of the supplied password with the challenge is sent for comparison so the [cleartext](#) password is never sent over the [connection](#).

changed block point in time copy

[Storage System] Deprecated synonym for [delta snapshot](#).

channel

1. [Storage System] The electrical circuits that sense or cause the state changes in recording [media](#) and convert between those state changes and electrical signals that can be interpreted as data bits.
2. [Computer System] Synonym for [I/O interconnect](#).

The term *channel* has other meanings in other branches of computer technology. The definitions given here are commonly used when discussing storage and networking. See [device channel](#), [I/O interconnect](#), host [I/O bus](#).

character

1. [Computer System] Synonym for byte.
2. [Fibre Channel] A 10-bit [information unit](#) transmitted and received by [FC-1](#), consisting of 8 bits of data encoded as a 10 bit [transmission character](#) using [8B/10B encoding](#).
Some transmission characters used in FC-1 correspond to special codes and some 10 bit sequences represent invalid transmission characters.

character cell interface

[Computer System] Synonym for [Command Line Interface](#).

check data

[Storage System] Synonym for [parity data](#).

checkpoint

1. [Data Recovery] The recorded state of an application at an instant of time, including data, in-memory variables, program counter, and all other context that would be required to resume application execution from the recorded state.
2. [File System] An activity of a [file system](#), such as the High Performance File System, (HPFS) or the Andrew File System (AFS), in which cached [metadata](#) (data about the structures of the file system) is periodically written to the file system's permanent store, allowing the file system to maintain consistency if an unexpected stop occurs.

checksum

[Data Security] A value computed across a set of data, used to detect change.

A checksum is often used for error and manipulation detection.

chunk

[Storage System] Deprecated synonym for [strip](#).

chunk size

[Storage System] Deprecated synonym for [stripe depth](#) and [strip size](#).

C-H-S addressing

[Storage System] Synonym for [Cylinder-Head-Sector addressing](#).

CID

[iSCSI] Acronym for [Connection Identifier](#).

CIFS

[File System] Acronym for [Common Internet File System](#).

CIM

[Management] [Network] Acronym for [Common Information Model](#).

cipher

[Data Security] A cryptographic system where plaintext is rearranged through transposition and/or substitution under direction of a cryptographic key.

When a cipher is applied to plaintext to produce ciphertext, the process is called [encryption](#). When the cipher is applied to ciphertext to produce plaintext, the process is called [decryption](#).

cipher suite

[Data Security] A named combination of a [key exchange](#) algorithm (for [authentication](#)), a bulk [encryption](#) algorithm, a [message authentication code](#) (MAC) algorithm, and a pseudorandom function (PRF) that may be negotiated and used to establish the security settings for a network [connection](#) using the [Transport Layer Security](#) (TLS) or [Secure Sockets Layer](#) (SSL) network [protocol](#).

ciphertext

[Data Security] Data that has been encrypted.

See [cleartext](#).

C

Cipher Block Chaining (CBC)

[Data Security] A [block cipher mode of operation](#), in which each block of [plaintext](#) is XORed with the previous [ciphertext](#) block before being encrypted, making each ciphertext block dependent on all preceding plaintext blocks.

circuit

[Fibre Channel] [Network] Synonym for [communication circuit](#).

CJTPAT

[Data Communication] [Shorthand for Compliant Jitter Tolerance Pattern](#).

CKD (architecture)

[Storage System] Synonym for [Count-Key-Data](#) disk architecture.

Class 1

[Fibre Channel] A [connection](#)-oriented class of [Fibre Channel](#) communication service in which the entire [bandwidth](#) of the link between two ports is dedicated for communication between the ports and not used for other purposes.

Class 1 is also known as [dedicated connection service](#), and is not widely implemented. See [intermix](#).

Class 2

[Fibre Channel] A connectionless [Fibre Channel](#) communication service which multiplexes frames from one or more N_Ports or NL_Ports.

Class 2 frames are explicitly acknowledged by the [receiver](#), and notification of delivery failure is provided. This [class of service](#) includes end to end flow control.

Class 3

[Fibre Channel] A connectionless [Fibre Channel](#) communication service that multiplexes frames to or from one or more N_Ports or NL_Ports.

Class 3 frames are datagrams, that is they are not explicitly acknowledged, and delivery is on a "[best effort](#)" basis.

class of service

1. [Network] A mechanism for managing traffic in a network by specifying message or packet priority or delivery acknowledgement.

Network mechanisms include [identification](#) and grouping of data packets based on a priority [label](#) (in the packet header) or via mechanisms such as "per hop behavior", defined by the IETF's [Differentiated Services](#).

2. [Fibre Channel] The characteristics and guarantees of the transport layer of a [Fibre Channel circuit](#).

Fibre Channel classes of service include [connection](#)-based services ([Class 1](#)), acknowledged [frame](#) delivery with end to end flow control ([Class 2](#)), and packetized frame datagrams ([Class 3](#)). Different classes of service may simultaneously exist in a fabric. The form and reliability of delivery in Class 3 circuits may vary with the [topology](#).

cleartext

[Data Security] Alternative term for [plaintext](#). Stating that data is in cleartext implies that the data is not scrambled or rearranged, and is in its raw form.

CLI

[Computer System] Acronym for [Command Line Interface](#).

client

1. [Computer System] An [intelligent device](#) or system that requests services from other intelligent devices, systems, or appliances.
See [server](#).
2. [General] An asymmetric relationship with a second party (a server) in which the client initiates requests and the server responds to those requests.

client-side data deduplication

[Capacity Optimization] Deprecated synonym for source [data deduplication](#).

clone

[Data Management] Synonym for [snapshot](#).

Clones and snapshots are full copies. See [delta snapshot](#).

cloud auditor

[Cloud] A party trusted conduct independent assessment of cloud services, [information system](#) operations, performance and [information security](#) of the cloud implementation.

cloud carrier

[Cloud] An intermediary that provides connectivity and transport of cloud services between cloud providers and cloud consumers.

cloud consumer

[Cloud] A person or organization that uses cloud services.

Cloud Data Management Interface (CDMI)

[Standards] A SNIA Architecture standard for [Data storage as a Service \(DaaS\)](#).

[CDMI](#) is an interface for both the data path and the control path of [cloud storage](#).

CDMI can also be used to manage storage in Cloud Computing deployments.

cloud digital archive service

[Data Management] A cloud-based offering providing a [digital archive](#) service.

cloud infrastructure

[Cloud] A set of data processing components that can be automatically provisioned by consumers, accessed over a network and that provide [secure multitenancy](#).

cloud provider

[Cloud] An entity responsible for making cloud services available to cloud consumers. [ISO/IEC 17788].

cloud security audit

[Cloud] Systematic evaluation of a cloud system by assessing how well it conforms to a set of established security criteria.

cloud service

[Cloud] A function useful to a [cloud consumer](#) provided by a [cloud provider](#).

cloud storage

[Services] Synonym for [Data storage as a Service](#).

cluster

[Computer System] A collection of computers that are interconnected (typically at high speeds) for the purpose of improving reliability, [availability](#), serviceability, [load balancing](#) and/or performance.

Often, clustered computers have access to a common pool of storage, and run special software to coordinate the component computers' activities.

CMIP

[Management] [Network] Acronym for [Common Management Information Protocol](#).

coaxial cable

[Network] An electrical transmission [medium](#) consisting of two concentric conductors separated by a dielectric material with the spacings and material arranged to give a specified electrical impedance.

See [triaxial cable](#).

code bit

[Computer System] A bit (binary digit) of an encoded datum.

Sequences of code bits make up symbols, each of which corresponds to a data element (word, byte, or other unit).

code byte

[Computer System] A byte of an encoded datum.

Sometimes called a symbol. Code bytes are the output of [encoding](#) or [encryption](#) processes. In communication theory contexts, a code byte is often referred to as a *code word*. See [data byte](#).

code violation

[Fibre Channel] The error condition that occurs when a received [transmission character](#) cannot be decoded into a [valid data byte](#) or [special code](#) using the validity checking rules specified by the [transmission code](#).

cold backup

[Data Recovery] Synonym for [offline backup](#).

See [hot backup](#), [online backup](#).

cold data

[Data Management] Data that is accessed infrequently.

cold storage

[Data Management] Data storage device, system, or service used to store cold data at a cost that is at least an order of magnitude less than the cost of primary storage.

Cold Storage features large capacity, energy saving and long-term data preservation, in order to achieve low-cost rather than performance.

cold swap

[Computer System] The [substitution](#) of a [replacement unit](#) (RU) in a system for a defective one, where external power must be removed from the system in order to perform the substitution.

A cold [swap](#) is a physical substitution as well as a functional one. See [automatic swap](#), [hot swap](#), [warm swap](#).

comma character

[Fibre Channel] In an encoded data stream using [8B/10B encoding](#), either of the seven bit sequences 0011111 or 1100000.

Command Descriptor Block (CDB)

[SCSI] A [sequence](#) of bytes that defines a single [SCSI](#) command sent to a SCSI [target](#).

A CDB may have a fixed length of up to 16 bytes or a variable length of between 12 and 260 bytes. A CDB may specify a [logical block address](#); contrast with [C-H-S addressing](#).

C

Command Line Interface (CLI)

[Computer System] A form of human interface to intelligent devices characterized by non-directive prompting and [character](#) string user input.

CLIs are used by system consoles and remote shell sessions (RSH, SSH). They are very useful for scripting and other administrative purposes, but are usually perceived by end users to be more difficult to comprehend and use than graphical user interfaces (GUIs).

command security

[SCSI] The application of security techniques such as [authentication](#), [integrity](#) checking and [encryption](#) to individual [SCSI](#) commands.

Common Criteria (CC)

[Data Security] A multi-part International Standard that is meant to be used as the basis for evaluation of security properties of IT products and systems.

The CC is specified in ISO/IEC 15408-1:1999, ISO/IEC 15408-2:1999, and ISO/IEC 15408-3:1999.

Common Information Model (CIM)

[Data Management] [Network] An [object oriented](#) description of the entities and relationships in a business' management

environment maintained by the [Distributed Management Task Force](#).

CIM is divided into a Core Model and Common Models. The Core Model addresses high-level concepts (such as systems and devices), as well as fundamental relationships (such as dependencies). The Common Models describe specific problem domains such as computer system, network, user or device management. The Common Models are subclasses of the Core Model and may also be subclasses of each other.

Common Internet File System (CIFS)

[Network] A [network file system](#) access [protocol](#) primarily used by Windows clients to communicate file access requests to Windows servers.

CIFS was originally called [Server Message Block](#) (SMB). Today, other implementations of the CIFS protocol allow other clients and servers to use it for intercommunication and interoperation with Microsoft operating systems.

Common Management Information Protocol (CMIP)

[Management] [Network] A network management [protocol](#) built on the Open Systems Interconnection (OSI) communication model.

CMIP is more complete, and therefore larger than, [SNMP](#).

Common Schema Definition Language (CSDL)

[Management] An [OASIS](#) standard language used to define a [model](#) over which an [OData service](#) acts.

communication circuit

1. [Fibre Channel] A bidirectional path for message [exchange](#) within a [Fibre Channel](#) fabric.
2. [Network] A specific logical or physical path between two points over which communications occur.

communications security

[Network] [Data Security] Protection of information while it's being transmitted, particularly via telecommunications.

A particular focus of communications security is message [authenticity](#). Communications security may include [cryptography](#), transmission security, emission security, and physical security.

community cloud

[Cloud] A [cloud infrastructure](#) shared by several organizations and supporting a specific community that has shared concerns (e.g., mission, security requirements, [policy](#), and [compliance](#) considerations).

compensating control

[Data Security] A way - also known as a band-aid - of mitigating a known [risk](#) where it may not be feasible to deploy specific technical enablement.

complex array

[Storage System] A [disk array](#) whose [control software](#) protects and maps data according to more complex algorithms than those of the [Berkeley RAID Levels](#).

The most common complex arrays are multi-level disk arrays, which perform more than one level of data address [mapping](#), and adaptive arrays, which are capable of changing data address mapping dynamically.

compliance

1. [General] The state of being in accordance with a standard, specification, or clearly defined requirements.
2. [Legal] The state of being in accordance with legal requirements.

The "compliance market" is centered around storage and systems that support the retention and discovery of data as required by law or regulation.

Compliant Jitter Tolerance Pattern (CJTPAT)

[Data Communication] A test pattern for jitter testing.

compression

[General] Synonym for [data compression](#).

compression ratio

[Storage System] A [space reduction](#) ratio that only includes the effects of [compression](#).

compromise

[Data Security] An [incident](#) that subjects data to [unauthorized disclosure](#), modification, destruction, or loss.

compute virtualization

[Computer System] Software that enables a single server hardware platform to support multiple concurrent instances of an operating system and applications.

computer security

[Data Security] Measures and controls that ensure [confidentiality](#), [integrity](#), and [availability](#) of [information system](#) assets including hardware, software, [firmware](#), and information being processed, stored, and communicated.

concatenation

[Network] [Storage System] A logical joining of two series of data, usually represented by the symbol "|".

In data communications, two or more datums are often concatenated to provide a unique name or reference (e.g., [S_ID](#) | [X_ID](#)). [Volume](#) managers concatenate disk address spaces to present a single larger address spaces.

concurrency

[Computer System] The property of overlapping in time, often in reference to the execution of I/O operations or I/O requests.

concurrent copy

[Storage System] A hybrid [point in time copy](#) mechanism which creates a split [mirror](#) copy by copying blocks from the source as they are requested by the host, while copying so-far unrequested blocks in the background until the mirror is complete.

A concurrent copy initially occupies at least the amount of storage required to hold accessed blocks and grows to occupy as much storage as the copy source.

concurrent operations

[Computer System] Operations that overlap in time.

The concept of concurrent I/O operations is central to the use of independent access arrays in [throughput](#)-intensive applications.

conditioning

[General] The processing of a signal for the purpose of making it conform more closely to an ideal.

[Power conditioning](#) is used to minimize voltage and frequency variations in an external power. Signal conditioning is used to reduce noise in logic or data signals.

confidentiality

[Data Security] The property that data cannot be accessed by unauthorized parties.

Confidentiality may be created by the use of [encryption](#) or access controls.

configuration

1. [Storage System] The process of installing or removing hardware or software components required for a system or subsystem to function.
2. [Storage System] Assignment of the operating parameters of a system, subsystem or device, such as designating a [disk array](#)'s [member](#) disks or extents and parameters such as [stripe depth](#), [RAID](#) model, [cache](#) allowance, etc.

3. [Storage System] The collection of a system's hardware and software components and operating parameters. See [array configuration](#), [physical configuration](#).

configuration management

[General] The management of system features and behaviors through the control of changes made to hardware, software, [firmware](#) documentation and related resources throughout the life cycle of an [information system](#).

Congestion Notification (CN)

[Network] A [DCB](#) component that specifies protocols, procedures and managed objects that support congestion management of long-lived data flows within network domains of limited [bandwidth](#) delay.

connection

1. [Fibre Channel] Short form of [dedicated connection](#).
2. [iSCSI] A communication path between the [initiator](#) and [target](#) using a [TCP/IP](#) connection.

In [iSCSI](#), one or more connections make up a session. Connections carry control messages, [SCSI](#) commands, parameters, and data within iSCSI PDUs.

Connection ID

[Fibre Channel] A value that uniquely identifies an [NVMeoFC](#) connection.

connection identifier

[iSCSI] An identifier generated by the [initiator](#) and sent to the [target](#) upon logging in or out, that uniquely identifies each [connection](#) within a session.

connection initiator

[Fibre Channel] An [N_Port](#) that initiates a [Class 1 connection](#) with a destination N_Port through a connect-request and which receives a valid response from the destination N_Port to establish the connection.

connection recipient

[Fibre Channel] An [N_Port](#) that receives a [Class 1](#) connect-request from a [connection initiator](#) and accepts the connection request by transmitting a valid response.

connectionless buffer

[Fibre Channel] A receive buffer used in a [connectionless service](#) that is capable of receiving connectionless frames.

connectionless frame

[Fibre Channel] A [frame](#) used in a [connectionless service](#) (i.e., [Class 1](#) frames with [SOF](#)(C1), [Class 2](#), and [Class 3](#) frames referred to individually or collectively).

connectionless integrity service

[Data Security] A security service that provides [data integrity](#) service for an individual [IP datagram](#) by detecting modification of the datagram without regard to the ordering of the datagram in a stream of datagrams.

connectionless service

[Fibre Channel] Communication between two [N_Ports](#) or [NL_Ports](#) without a [dedicated connection](#).

consistency group

[Storage System] A collection of replication sets grouped together to ensure write order consistency across all the replication sets' primary volumes.

An operation on a consistency group, such as changing replication from asynchronous to synchronous, applies to all the replication sets within the consistency group, and consequently their volumes.

consistent volume

1. [Storage System] A [volume](#) that satisfies the consistency criteria of the system on which it is hosted.
2. [File System] In [LTFS](#), a volume in which all partitions are complete, and the last [LTFS Index](#) in the Index [Partition](#) has a back pointer to the last LTFS Index in the Data Partition.

If an [LTFS volume](#) is not consistent, some form of [recovery](#) may be necessary.

console

1. [Computer System] A device for graphical or textual visual output from a computer system.
2. [Computer System] In systems, network and device management, an application that provides graphical and textual feedback regarding operation and status, and that may accept operator commands and input influencing operation and status.

Sophisticated consoles designed for the management of many systems from one location are sometimes called enterprise management consoles.

content-agnostic data deduplication

[Storage System] A [data deduplication](#) method that does not require awareness of specific application data formats.

See [content-aware data deduplication](#).

content-aware data deduplication

[Storage System] A [data deduplication](#) method that leverages knowledge of specific application data formats.

See [content-agnostic data deduplication](#).

Continuous Data Protection (CDP)

[Data Recovery] A class of mechanisms that continuously capture or track data modifications enabling [recovery](#) to previous points in time.

continuously increasing relative offset

[Fibre Channel] A transmission control algorithm in which the frames containing the subblocks that comprise a [block](#) of information are transmitted strictly in the order of the subblocks.

Continuously increasing [relative offset](#) offers simpler reassembly and detection of lost frames compared to [random relative offset](#).

control software

[Storage System] A body of software that provides common control and management for one or more disk arrays or tape arrays.

Control software presents the arrays of disks or tapes it controls to its [operating environment](#) as one or more virtual disks or tapes. Control software may execute in a disk [controller](#) or intelligent [host bus adapter](#), or in a [host computer](#). When it executes in a disk controller or adapter, control software is often referred to as [firmware](#).

controller

1. [Storage System] The control logic in a disk or tape that performs command [decoding](#) and execution, host data transfer, serialization and deserialization of data, error detection and correction, and overall management of device operations.
2. [Management] The control logic in a [storage subsystem](#) that performs command [transformation](#) and routing, [aggregation](#) ([RAID](#), [mirroring](#), [striping](#), or other), high-level error [recovery](#), and performance optimization for multiple storage devices.

controller based array**controller based disk array**

[Storage System] A [disk array](#) whose [control software](#) executes in a [disk subsystem controller](#).

controller cache

[Storage System] A cache that resides within a [controller](#) and whose primary purpose is to improve disk or [array](#) I/O performance.

See [cache](#), [disk cache](#), [host cache](#).

controlling FCF

[Fibre Channel] A controlling switch that supports [lossless Ethernet MACs](#).

controlling switch

[Fibre Channel] A switch able to control a set of [FCDFs](#) in order to create a distributed switch.

converged infrastructure

[Computer System] The pooling of compute, storage, and networking resources using either common management tools or common (shared) physical resources.

Copy On Write (COW)

[Storage System] [Backup] A technique for maintaining a [point in time copy](#) of a collection of data by copying only data that is modified after the instant of [replicate](#) initiation; the original source data is used to satisfy read requests for both the source data itself and for the unmodified portion of the point in time copy.

See [pointer remapping](#).

copyback

[Storage System] The replacement of a properly functioning [array member](#) by another disk, including copying of the member's contents to the replacing disk.

Copyback, which is most often used to create or restore a particular [physical configuration](#) for an array (e.g., a particular arrangement of array members on device I/O interconnects), is accomplished without [reduction](#) of the array.

Core N_Port_Name

[Fibre Channel] A set of entities with the same [Core Switch Name](#) that may host multiple Virtual Switches.

A Core Switch may be a set of ports in a physical chassis, or in multiple physical chassis.

Core Switch

[Fibre Channel] An [N_Port Name](#) associated with the Physical N_Port of a VFT Tagging N_Port, and not with any other [FC Port](#) within the scope of its [Name Identifier](#) format.

Core Switch_Name

[Fibre Channel] In a [Virtual Fabric](#) capable [Switch](#), the [Switch_Name](#) identifying the [Core Switch](#).

Count-Key-Data (CKD)

[Storage System] A disk data organization model in which the disk is assumed to consist of a fixed number of tracks, each having a maximum data capacity.

Multiple records of varying length may be written on each track of a Count-Key-Data disk, and the [usable capacity](#) of each track depends on the number of records written to it. The [CKD architecture](#) derives its name from the record format, which consists of a field containing the number of bytes in the key and data fields and a record address, an [optional](#) key field by which particular records can be easily recognized, and the data itself. CKD is the storage architecture used by IBM Corporation's System 390 series of mainframe computer systems. See [fixed block architecture](#).

counter measure

[Data Security] Any action, device, procedure, technique, or other measure that reduces the [vulnerability](#) of or [threat](#) to a system.

covert channel

[Data Security] An unintended and/or unauthorized communications path that can be used to transfer information in a manner that violates a security [policy](#).

COW

[Computer System] Acronym for [Copy On Write](#).

credentials

[Data Security] Information, passed from one entity to another, used to establish the sending entity's [identity](#) and/or access rights.

credit

1. [Fibre Channel] The number of receive buffers allocated to a transmitting [N_Port](#), [NL_Port](#), or [F_Port](#).
2. [Fibre Channel] For links using [buffer to buffer flow control](#), the number of receive buffers allocated to a transmitting [N_Port](#), [NL_Port](#), or [F_Port](#).

The credit is the maximum number of outstanding frames that can be transmitted by that [N_Port](#), [NL_Port](#), or [F_Port](#) without causing a buffer overrun condition at the [receiver](#).

CRC

[Data Communication] [Storage System] Acronym for [Cyclic Redundancy Check](#).

CRL

[Data Security] Acronym for [Certificate Revocation List](#).

CRU

[General] Acronym for [Customer Replaceable Unit](#).

cryptanalysis

[Data Security] A set of operations performed in converting encrypted information to plaintext without initial knowledge of the algorithm and/or key employed in the [encryption](#).

cryptographic erase

[Data Security] Method of sanitization in which the encryption key for the encrypted target data is sanitized, making recovery of the decrypted target data infeasible. [ISO/IEC 27040]

cryptographic algorithm

[Data Security] An algorithm whose outputs have cryptanalytic security properties with respect to its inputs, or vice versa.

cryptographic erasure

[Data Security] A method for rendering encrypted data unrecoverable by securely deleting the [keying material](#) required to decrypt the data.

The encrypted data itself is not modified. The protection offered by cryptographic erasure is bounded by the work factor involved in discovering the [decryption](#) key or mounting a cryptanalytic [attack](#) on the [encryption](#) algorithm itself.

cryptographic hash function

[Data Security] A function that maps [plaintext](#) strings of any length to bit strings of fixed length, such that it is computationally infeasible to find correlations between inputs and outputs, and such that given one part of the output, but not the input, it is computationally infeasible to predict any bit of the remaining output.

Cryptographic hash functions have many [information security](#) applications, notably in digital signatures, message [authentication](#) codes (MACs), and other forms of authentication. The output from a cryptographic hash function is known as a [message digest](#) or [hash value](#).

cryptography

[Data Security] The principles, means and methods for rendering information unintelligible, and for restoring encrypted information to intelligible form.

cryptology

[Data Security] The field of knowledge encompassing both [cryptography](#) and [cryptanalysis](#).

cryptoperiod

[Data Security] The time span during which a specific key is authorized for use or in which the keys for a given system or application may remain in effect. [NIST SP 800-57 Part 1]

cryptosystem

[Data Security] A system for encrypting and decrypting data.

CSDL

[Management] Shorthand for [Common Schema Definition Language](#).

C

CSMA/CD

[Network] Acronym for [Carrier Sense Multiple Access with Collision Detection](#).

cumulative incremental backup

[Data Recovery] A [backup](#) in which all data objects modified since the last full backup are copied.

To restore data when cumulative incremental backups are in use, only the latest full backup and the latest cumulative [incremental backup](#) are required. See [differential incremental backup](#), [full backup](#).

current running disparity

[Fibre Channel] The [running disparity](#) present at a [transmitter](#) when the [encoding](#) of a [valid data byte](#) or [special code](#) is initiated, or at a [receiver](#) when the [decoding](#) of a [transmission character](#) is initiated.

Customer Replaceable Unit (CRU)

[General] A unit, or component of a system that is designed to be replaced by “customers;” i.e., individuals who may not be trained as computer system service personnel.

See [Field Replaceable Unit](#).

cut through (switching)

[Fibre Channel] A switching technique that allows a routing decision to be made and acted upon as soon as the destination address of a [frame](#) is received.

Cyclic Redundancy Check (CRC)

[Data Communication] [Storage System] A scheme for checking the [integrity](#) of data that has been transmitted or stored and retrieved.

A CRC consists of a fixed number of bits computed as a function of the data to be protected, and appended to the data. When the data is read or received, the function is recomputed, and the result is compared to that appended to the data. Cyclic [redundancy](#) checks differ from error correcting codes in that they

can detect a wide range of errors, but are not capable of correcting them. See [error correcting code](#).

Cylinder-Head-Sector (C-H-S) addressing

[Storage System] A form of [addressing](#) data stored on a disk in which the cylinder, head/platter combination, and relative [sector](#) number on a track are specified.

See [block addressing](#).

C

D

D

D_ID

[Fibre Channel] A three-byte field [encoding](#) the Destination_ID, that contains the [address identifier](#) of the [destination Nx_Port](#).

DSaaS

[Services] Acronym for [Data storage as a Service](#).

DAC

1. [Data Security] Acronym for [Discretionary Access Control](#).
2. [Hardware] Acronym for [Digital Analog Converter](#).

daemon

[Operating System] A process that is kept running on a computer system to service a particular set of requests.

By way of example, lpd is a daemon in UNIX that handles printing requests. Daemons are independent processes, and not part of an application program. Application requests may be serviced by a daemon.

DAS

[Storage System] Acronym for [Direct Attached Storage](#).

data

[Computer System] The digital representation of anything in any form.

data at rest

[Data Security] Data stored on stable [non-volatile](#) storage. [ISO/IEC 27040].

data authentication

[Legal] The process of substantiating that the data is an accurate representation of what it purports to be. [SWGDE/ SWGIT Glossary]

data availability

[Storage System] The amount of time that data is accessible by applications during those time periods when it is expected to be available.

See [availability](#), [high availability](#).

data breach

[Data Security] A compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to protected data transmitted, stored or otherwise processed. [ISO/IEC 27040]

data byte

[Network] [Storage System] A byte of user data as presented to a storage or communication facility.

See [code byte](#), [data character](#).

Data Center Bridging (DCB)

[Network] The suite of [Ethernet protocol](#) extensions defined for reliable storage transports such as [FCoE](#).

DCB includes the following protocols: IEEE 802.1Qau (CN), IEEE 802.1Qaz (ETS and DCBX), and IEEE 802.1Qbb (PFC).

A data center [bridge](#) implements the above protocols and capabilities for use in the data center.

Data Center Bridging eXchange protocol (DCBX)

[Network] A [DCB](#) component for discovery and [exchange](#) of DCB information.

data character

[Fibre Channel] [Network] Any [transmission character](#) associated by the [transmission code](#) with a [valid data byte](#).

data classification

[Data Management] An organization of data into groups for management purposes.

A frequent purpose of a classification scheme is to associate service level objectives with groups of data based on their value to the business.

D

data compression

[General] The process of encoding data to reduce its size.

Lossy compression (i.e., compression using a technique in which a portion of the original information is lost) is acceptable for some forms of data (e.g., digital images) in some applications, but for most IT applications, lossless compression (i.e., compression using a technique that preserves the entire content of the original data, and from which the original data can be reconstructed exactly) is required.

data deduplication

[Storage System] The replacement of multiple copies of data—at variable levels of granularity—with references to a shared copy in order to save storage space and/or [bandwidth](#).

See also [inline data deduplication](#), [post-process data deduplication](#).

data deduplication ratio

[Storage System] A [space reduction](#) ratio that only includes the effects of [data deduplication](#).

Data Encryption Standard (DES)

[Data Security] A cryptographic [data protection](#) algorithm published by the [National Institute of Standards and Technology](#) in [Federal Information Processing Standard](#) (FIPS) Publication 46.

This algorithm is obsolete.

data frame

[Fibre Channel] A [frame](#) containing information meant for [FC-4](#) ([ULP](#)) or the link application.

data in flight

[Data Security] Synonym for [data in motion](#).

data in motion

[Data Security] Data being transferred from one location to another.

data in transit

1. [Data Security] Synonym for [data in motion](#).
2. [Legal] Data in motion across a jurisdictional boundary. Jurisdictions (usually nation states) may have policies and enforcement points that determine whether data may cross their borders.

data in use

[Data Security] Data in the process of being created, retrieved, manipulated, updated, or deleted.

data ingestion

[Data Management] A process for depositing data into a storage system.

data integrity

[Data Security] The property that data has not been altered or destroyed in an unauthorized manner [ISO 7498-2:1988].

[Data Management] The property that data has not been altered or destroyed, in an unintended manner, due to physical or logical events.

data lake

[Data management] A large repository for storing data in an unstructured way, in anticipation of future analytics.

This term originated in the [big data](#) community.

Data Lifecycle Management (DLM)

[Data Management] The policies, processes, practices, services and tools used to align the business value of data with the most appropriate and cost-effective storage infrastructure from the time data is created through its final disposition.

Data is aligned with business requirements through management policies and service levels associated with performance, [availability](#), recoverability, cost, etc. DLM is a subset of [ILM](#).

data management

[Management] The discipline and function of oversight and control of data resources.

data management services

[Data Management] A set of services that control of data from the time it is created until it no longer exists.

[Data Management](#) Services are not in the data path; rather, they provide control of, or utilize, data in the delivery of their services. This includes services such as data movement, data [redundancy](#), and data deletion.

data manager

[File System] A computer program whose primary purpose is to present a convenient view of data to applications, and map that view to an internal representation on a system, subsystem or device.

File systems and database management systems are the most common forms of a data manager.

data model

[Data Management] A repository-specific representation of a data model.

A database representation of the [CIM](#) schemas is an example of a data model.

data optimization

[Storage System] The process of reducing the amount of storage space used to store ingested data, using [capacity optimization methods](#).

data portability

[Data Communication] The ability to transfer data from one system to another without being required to recreate or reenter data descriptions.

data preservation

[Data Management] The processes of ensuring the fidelity and continued existence of stored data over a period of time.

data protection

[Data Management] The combination of [data integrity](#), [data availability](#), and [confidentiality](#).

data reliability

[Data Management] The length of the statistically expected continuous span of time over which data stored by a population of identical storage subsystems can be correctly retrieved, expressed as [Mean Time to Data Loss](#) (MTDL).

data replication

[Storage System] Continuously maintaining a secondary copy of data—possibly at a remote site—from a primary [volume](#) for the purposes of providing [high availability](#) and [redundancy](#).

Data replication is used for [disaster recovery](#) and business continuance, among other uses.

data repository

[Data Security] A central place of storage in which data is kept and maintained in an organized way.

data resource domain

[Management] The category of resources that exclusively encompass data services.

data retention

[Long Term Retention] Preserving the existence and [integrity](#) of data for some period of time or until certain events have transpired, or any combination of the two.

Retention requirements are expressed either as a time period, an event (e.g., the death of a patient), or a combination (e.g., 3 years after said death). Multiple requirements may be active, and some (e.g., judicial holds) may trump others.

data service

[Data Management] A set of functions that treat data without interpretation.

This treatment may, for example, involve copying, movement, security and/or protection, but not the actual storage of the data.

data shredding

[Data Management] A process for deleting data that is intended to make the data unrecoverable.

One such process consists of repeated overwrites of data on disk. Data shredding is not generally held to make data completely unrecoverable in the face of modern forensic techniques—that requires shredding of the disks themselves. Forensic techniques, however, do require physical access to the [storage media](#).

Data storage as a Service (DSaaS)

[Services] Delivery of appropriately configured virtual storage and related data services over a network, based on a request for a given service level.

Typically, DSaaS hides limits to scalability, is either self-provisioned or provisionless and is billed based on consumption.

data stripe depth

[Storage System] Synonym for [user data extent stripe depth](#).

data striping

[Storage System] A [disk array](#) data [mapping](#) technique in which fixed-length sequences of [virtual disk](#) data addresses are mapped to sequences of [member disk](#) addresses in a regular rotating pattern.

[Disk striping](#) is commonly called [RAID Level 0](#) or [RAID 0](#) because of its similarity to common RAID data mapping techniques. It includes no [redundancy](#), however, so strictly speaking, the appellation RAID is a misnomer.

data transfer capacity

[Computer System] The maximum rate at which data can be transmitted.

[Bandwidth](#) is sometimes expressed in terms of signaling capacity and sometimes in terms of data transmission capacity inclusive of [protocol](#) overhead (e.g., [Fibre Channel](#)). See [throughput](#), [data transfer rate](#).

data transfer device

[SCSI] A [removable media storage device](#) in a [library](#).

Examples are magnetic disk drives, cartridge tape drives, optical disk drives, and CD-ROM drives.

data transfer-intensive (application)

[Computer System] An I/O intensive application that makes large—usually sequential—I/O requests.

data transfer rate

[Computer System] The amount of data per unit time actually moved across an [I/O interconnect](#) in the course of executing an [I/O load](#).

The data transfer capacity of an [I/O subsystem](#) is an upper bound on its data transfer rate for any I/O load. For [disk subsystem](#) I/O, data transfer rate is usually expressed in MBytes/second (millions of bytes per second, where 1 million = 10^6) or Gbits/second (billions of bits per second, where 1 billion = 10^9). See [data transfer capacity](#).

Database Management System (DBMS)

[Database] An set of computer programs with a user and/or programming interface that supports the definition of the format of a database and the creation of and access to its data.

A database management system removes the need for a user or program to manage low level database storage. It also provides security for and assures the [integrity](#) of the data it contains.

Types of database management systems are relational (table-oriented), network, hierarchical and [object oriented](#).

datagram

[Fibre Channel] [Network] A message sent between two communicating entities for which no explicit link level acknowledgement is expected.

Datagrams are often said to be sent on a [best effort](#) basis.

DBMS

[Database] Acronym for [Database Management System](#).

DCB

[Network] Acronym for [Data Center Bridging](#).

decoding

[Fibre Channel] Validity checking of received transmission characters and generation of valid data bytes and special codes from those characters.

decryption

[Data Security] The operations performed in converting encrypted information to [plaintext](#) with full knowledge of the algorithm and key(s) used to encrypt it.

Decryption is the intended method for an authorized user to decrypt encrypted information.

dedicated connection

[Fibre Channel] A [communication circuit](#) between two N_Ports maintained by a [Fibre Channel](#) fabric.

The port resources used by a dedicated [connection](#) cannot be used for other purposes during the life of the dedicated connection.

dedicated connection service

[Fibre Channel] Synonym for [Class 1](#) service.

deduplication

See [data deduplication](#).

defense-in-depth

[Data Security] An information assurance strategy integrating people, technology, and operations capabilities to establish multiple security barriers across layers and dimensions of a protected system. [NIST SP 800-53]

degaussing

1. [Data Security] A procedure that renders data unreadable by applying a strong magnetic field to the [media](#).
2. [Data Security] Applying a degaussing procedure.

Degaussing is also called demagnetizing and erasure. Both of these terms are misleading, because in magnetic digital media the individual magnetic domains are not erased or demagnetized, but simply made to line up in the same direction, which eliminates any previous digital structure.

degraded mode

[Storage System] A mode of [RAID array](#) operation in which not all of the array's [member](#) disks are functioning, but the array as a whole is able to respond to application read and write requests to its virtual disks.

delimiter

[Fibre Channel] An [ordered set](#) used to indicate a [frame](#) boundary.

delta snapshot

[Data Recovery] A type of [point in time copy](#) that preserves the state of data at an instant in time, by storing only those blocks that are different from an already existing full copy of the data.

delta-based data deduplication

[Storage System] A method of performing [data deduplication](#) by storing or transmitting data in the form of differences from a baseline [point in time copy](#).

See [hash-based data deduplication](#).

DEN

[Network] Acronym for [Directory Enabled Network](#).

Denial of Service (DoS)

[Data Security] Result of any action or series of actions that prevents any part of an [information system](#) from functioning.

DES

[Data Security] Acronym for [Data Encryption Standard](#).

This algorithm is obsolete.

Desktop Management Interface (DMI)

[Management] [Network] Initiative that became a precursor to the [Distributed Management Task Force](#) (DMTF).

destination identifier

[Fibre Channel] An address contained in a [Fibre Channel frame](#) that identifies the destination of the frame.

destination Nx_Port

[Fibre Channel] The [Nx_Port](#) to which a [frame](#) is addressed.

device

[Storage System] Synonym for [storage device](#).

device bus**device I/O bus**

[Storage System] Synonyms for [I/O interconnect](#).

device channel

[Storage System] A [channel](#) used to connect storage devices to a [host bus adapter](#) or an [intelligent controller](#).

The preferred term is [I/O interconnect](#).

device fanout

[Storage System] The ability of a [storage controller](#) to connect host computers to multiple storage devices using a single [host I/O interconnect](#) address.

Device [fanout](#) allows computer systems to connect to substantially more storage devices than could be connected directly.

DF_ID

[Fibre Channel] Acronym for Destination [Fabric Identifier](#).

DH

[Data Security] Acronym for [Diffie-Hellman](#).

DH-CHAP

[Data Security] Acronym for [Diffie-Hellman augmented Challenge Handshake Authentication Protocol](#).

DHCP

[Network] Acronym for [Dynamic Host Control Protocol](#).

differential incremental backup

[Data Recovery] A [backup](#) in which data objects modified since the last [full backup](#) or [incremental backup](#) are copied.

To restore data when [differential](#) incremental backups are in use, the newest full backup and all differential backups newer than the newest full backup are required. See [cumulative incremental backup](#), [full backup](#).

Differential Mirror Resynchronization (DMR)

Differential resynchronization

[Data Recovery] Synonyms for [incremental mirror resynchronization](#).

differential (signaling)

[SCSI] A [SCSI](#) electrical signaling technique in which each control and data signal is represented by a voltage differential between two signal lines.

Differential signaling can be used over longer distances than the alternative [single ended signaling](#). See [single ended \(signaling\)](#).

Differentiated Services

[Management] A [protocol](#) defined by the [IETF](#) for managing network traffic based on the type of packet or message being transmitted.

The Differentiated Services protocol is often abbreviated as [DiffServ](#). DiffServ rules define how a packet flows through a network based on a 6 bit field (the Differentiated Services Code Point) in the [IP](#) header. The Differentiated Services Code Point specifies the "per hop behavior" ([bandwidth](#), queuing and forward/drop status) for the packet or message.

Diffie-Hellman (DH)

[Data Security] A key agreement [protocol](#) that was developed by W. Diffie and M. E. Hellman in allowing two entities to [exchange](#) a [secret key](#) over an insecure [medium](#) without any prior secrets.

Diffie-Hellman augmented Challenge Handshake Authentication Protocol (DH-CHAP)

[Data Security] A [password](#) based [Authentication](#) and [key management protocol](#) that uses the CHAP algorithm ([RFC 1994](#)) augmented with an [optional Diffie-Hellman](#) algorithm.

DH-CHAP provides bidirectional and may provide [unidirectional Authentication](#) between a [Fibre Channel Initiator](#) and [Responder](#). DH-CHAP is defined by Fibre Channel – Security Protocols - 2 (FC-SP-2).

DiffServ

[Management] Abbreviation for [Differentiated Services](#).

digest

[Data Security] A binary string of some fixed length derived by a computationally efficient function from a binary input string of arbitrary length.

A key feature of cryptographic digests is that given a digest, it is computationally infeasible to find another [plaintext](#) string that generates the same digest.

Digital Analog Converter (DAC)

[Hardware] A device that converts a discretely valued (digital) input to a continuously valued (analog) output.

digital archive

[Data Management] A storage repository or service used to secure, retain, and protect digital information and data for periods of time less than that of [long-term data retention](#).

A digital [archive](#) can be an infrastructure component of a complete [digital preservation service](#), but is not sufficient by itself to accomplish digital preservation, i.e., long-term data retention.

digital forensics

[Legal] The [identification](#), collection, [preservation](#) and analysis of digital evidence for use in legal proceedings.

Digital Linear Tape (DLT)

[Data Recovery] A family of tape device and [media](#) technologies.

digital object auditing

[Long Term Retention] A methodology to verify and detect threats to the validity of [digital preservation](#) objects.

Digital object auditing is a process of routine periodic testing of stored digital objects, usually using cryptographic techniques, by comparing their previous signatures and time stamps to their current to verify that change, loss of access, or data loss has not occurred.

digital preservation

[Long Term Retention] Ensuring continued access to, and usability of, digital information and records, especially over long periods of time.

digital preservation object

[Long Term Retention] A collection of data, [metadata](#) and possibly other resources treated as a unit for [digital preservation](#) purposes.

A [preservation object](#) provides the functionality required to assure the future ability to use, secure, interpret, and verify [authenticity](#) of the metadata, information, and data in the container and is the foundational element for digital preservation of information and data.

digital preservation service

[Long-Term Retention] A service providing [digital preservation](#).

A digital preservation service includes a comprehensive management and curation function that controls its supporting infrastructure, information, data, and storage services in accordance with the requirements of the information objects it manages to accomplish the goals of digital preservation.

digital signature

[Data Security] A cryptographically derived binary string used to assure information [authenticity](#), [integrity](#), and [nonrepudiation](#).

Digital signatures can generally be externally verified by entities not in possession of the key used to sign the information. For example, a [secure hash](#) of the information encrypted with the [originator's private key](#) when an [asymmetric cryptosystem](#) is used. Some algorithms that are used in digital signatures cannot be used to encrypt data. (e.g., [DSA](#)).

Digital Signature Algorithm (DSA)

[Data Security] A subset of the [Digital Signature Standard](#) that represents a specific [public key](#) algorithm that is only used for digital signatures.

The [secret key](#) used in DSA operates on the message hash generated by [SHA-1](#); to verify a signature, one recomputes the hash of the message, uses the public key to decrypt the signature and then compares the results.

This algorithm is obsolete.

Digital Signature Standard (DSS)

[Data Security] A standard for [digital signature](#) that is published by the [National Institute of Standards and Technology \(NIST\)](#) in [Federal Information Processing Standard \(FIPS\)](#) Publication 186-4.

DSS specifies [DSA](#) as the algorithm for digital signatures and [SHA-x](#) for hashing.

DIMM

[Hardware] Acronym for [Dual Inline Memory Module](#).

Direct Attached Storage (DAS)

[Storage System] One or more dedicated storage devices connected to one or more servers.

direct routing method

[SCSI] A method used by expanders to route connection requests to directly attached devices, including other expanders.

directory

1. [File System] A mechanism for organizing information. Directories are usually organized hierarchically. I.e., a directory may contain both information about files and objects, and other directories. They are used to organize collections of files and other objects for application or human convenience.
2. [File System] A file or other persistent data structure in a [file system](#) that contains information about other files.
3. [Management] An [LDAP](#)-based repository consisting of class definitions and instances of those classes. Microsoft's [Active Directory](#) (AD) and Novell's NetWare Directory Service (NDS) are examples of enterprise-wide LDAP directories.

D

Directory Enabled Network (DEN)

[Management] [Network] An initiative of the [DMTF](#) to map the [CIM schema](#) to an [LDAP Directory](#).

DEN's goals are to provide a consistent and standard [data model](#) to describe a network, its elements and its policies/rules. Policies are defined to provide [quality of service](#) or to manage to a specified [class of service](#).

directory tree

[File System] A collective term for a [directory](#), all of its files, and the directory trees of each of its subdirectories.

Disaster Recovery (DR)

[General] The [recovery](#) of data, access to data and associated processing through a comprehensive process of setting up a [redundant](#) site (equipment and work space) with recovery of [operational](#) data to continue business operations after a loss of use of all or part of a data center.

This involves not only an essential set of data but also an essential set of all the hardware and software to continue processing of that data and business. Any disaster recovery may involve some amount of down time.

discard policy

[Fibre Channel] An error handling [policy](#) that allows an [N_Port](#) or [NL_Port](#) to discard data frames received following detection of a missing [frame](#) in a [sequence](#).

disconnection

[Fibre Channel] The process of removing a [dedicated connection](#) between two N_Ports.

discovery

1. [Legal] Process by which each party obtains information held by another party or non-party concerning a matter.

[ISO/IEC 27050-1]

Discovery is applicable more broadly than to parties in adversarial disputes. Discovery is also the disclosure of hardcopy documents, Electronically Stored Information and tangible objects by an adverse party. In some jurisdictions the term disclosure is used interchangeably with discovery.

2. [Storage System] The process of finding devices attached to a storage infrastructure.

3. [Networking] The process of finding network interfaces in a networking infrastructure.

Discretionary Access Control (DAC)

[Data Security] A type of [access control](#) that allows a [principal](#) owning an object to grant or deny access to other principals.

disk

disk drive

[Storage System] A non-volatile, randomly addressable, re-writable data [storage device](#).

This definition includes rotating magnetic and optical disks and *solid-state disks*, or non-volatile electronic storage elements. It

does not include specialized devices such as *write-once-read-many* ([WORM](#)) optical disks, nor does it include so-called *RAM disks* implemented using software to control a dedicated portion of a [host computer](#)'s volatile random access memory.

disk array

[Storage System] A set of disks from one or more commonly accessible disk subsystems, combined with a body of [control software](#).

The control software presents the disks' storage capacity to hosts as one or more virtual disks. Control software is often called [firmware](#) or microcode when it runs in a disk [controller](#). Control software that runs in a [host computer](#) is usually called a [volume manager](#).

disk array subsystem

[Storage System] A [disk subsystem](#) that includes [control software](#) with the capability to organize its disks as disk arrays.

disk block

[Storage System] The unit in which data is stored and retrieved on a [fixed block architecture](#) disk.

Disk blocks are of fixed usable size (with the most common being 512 bytes), and are usually numbered consecutively. Disk blocks are also the unit of on-disk protection against errors; whatever mechanism a disk employs to protect against data errors (e.g., [ECC](#)) protects individual blocks of data. See [sector](#).

disk cache

1. [Storage System] A cache that resides within a disk.
2. [Storage System] A cache that resides in a [controller](#) or host whose primary purpose is to improve disk or [array](#) I/O performance. See [cache](#), [controller cache](#), [host cache](#).

disk image backup

[Data Recovery] [Windows] A [backup](#) consisting of a copy of each of the blocks comprising a disk's usable storage area.

A disk image backup incorporates no information about the objects contained on the disk beyond what is stored in the image itself, and hence cannot always be used for individual object [restoration](#).

disk scrubbing

[Storage System] A function that reads all of the user data and [check data](#) blocks in a [RAID array](#) and relocates them if [media](#) defects are found.

disk shadowing

[Storage System] Deprecated synonym for [mirroring](#).

disk striping

[Storage System] Synonym for [data striping](#).

disk subsystem

[Storage System] A [storage subsystem](#) that supports only disk devices.

disparity

[Fibre Channel] For a data stream using [8B/10B encoding](#), the difference between the number of ones and the number of zeros in a [transmission character](#).

disposition

[Legal] Range of processes associated with implementing records retention, destruction or transfer decisions that are documented in disposition authorities or other instruments.
[ISO 30300:2011]

disposition policy

[Data Management] A [policy](#) that defines when [lifecycle deletion](#) should occur, and/or what actions to perform.

distributed FCF

[Fibre Channel] A set of FDFs associated with at least one controlling [FCF](#) that controls the operations of the set of FDFs.

Distributed Management Task Force (DMTF)

[Management] An industry organization that develops management standards for computer system and enterprise environments.

DMTF standards include [WBEM](#), [CIM](#), [DMI](#), [DEN](#) and [ARM](#). The DMTF has a web site at www.dmtf.org.

distributed switch

[Fibre Channel] A set of [FCDFs](#) associated with at least one controlling switch that controls the operations of the set of FCDFs.

DLM

[Data Management] Acronym for [Data Lifecycle Management](#).

DLT

[Storage System] Acronym for [Digital Linear Tape](#).

DMI

[Management] [Network] Acronym for [Desktop Management Interface](#).

DMR

[Data Recovery] Acronym for [Differential Mirror Resynchronization](#).

DMTF

[Management] Acronym for [Distributed Management Task Force](#).

DNS

[Network] Acronym for [Domain Name Service](#).

Document Type Definition (DTD)

[Standards] In [XML](#), a specification of the permissible tags or "markup codes" in a document, and their meanings.

XML tags are delimited by the characters, "<" and ">". When a DTD is available for a document, a universal reader (program) can parse the document and display or print it.

domain

1. [General] A shared user [authorization](#) database that contains users, groups, and their security policies.
2. [Network] A set of interconnected network elements and addresses that are administered together and that may communicate.
3. [Fibre Channel] The highest level in a three-level [addressing](#) hierarchy used in the [Fibre Channel address identifier](#). A domain typically is associated with a single Fibre Channel [switch](#).

domain controller

1. [Windows] A Windows [server](#) that contains a copy of a user account database. A Windows [domain](#) may contain both primary and [backup](#) domain controllers.
2. [Fibre Channel] The control function accessible directly by an [N_Port](#) attached to a [switch](#) and also addressable in other domains using the Domain Controller [address identifier](#) of ""FF [FC](#) nn"" hex, where nn is the remote Domain Controller being accessed.

Domain Name Service (DNS)

[Network] A computer program that converts between [IP](#) addresses and symbolic names for nodes on a network in a standard way.

Most operating systems include a version of DNS. The service is defined by the [IETF](#) Standard RFCs 974, 1034, 1035, 1122, and 1123, and over a hundred subsequent RFCs that have not yet achieved full standard status.

DoS

[Data Security] Acronym for [Denial of Service](#).

double buffering

[Computer System] A technique used to increase [data transfer rate](#) by constantly keeping two I/O requests for consecutively addressed data outstanding.

A software component begins a double-buffered I/O stream by making two I/O requests in rapid [sequence](#). Thereafter, each time an I/O request completes, another is immediately made, leaving two outstanding. If a [disk subsystem](#) can process requests fast enough, double buffering allows data to be transferred at a disk or [disk array's full volume transfer rate](#).

DR

[General] Acronym for [Disaster Recovery](#).

DRAM

[Hardware] Acronym for [Dynamic Random Access Memory](#).

drive

[Storage System] Synonym for [storage element](#) (e.g., [disk drive](#) or [tape drive](#)).

drive letter

[Windows] A single letter of the alphabet by which applications and users identify a [partition](#) or physical or [virtual disk](#) to the Windows operating system.

driver**driver software**

[Computer System] Synonyms for [I/O driver](#).

DSA

[Data Security] Acronym for [Digital Signature Algorithm](#).

DSS

[Data Security] Acronym for [Digital Signature Standard](#).

DTD

[General] Acronym for [Document Type Definition](#).

dual active (components)

[Computer System] A pair of components, such as the controllers in a failure tolerant [storage subsystem](#) that share a task or class of tasks when both are functioning normally, but take on the entire task or tasks when one of the components fails.

Dual active controllers are connected to the same set of storage devices, and improve both I/O performance and [failure tolerance](#) compared to a single controller. Dual active components are also called [active-active](#) components.

Dual Inline Memory Module (DIMM)

[Hardware] A set of random access memory integrated circuits or chips mounted on a circuit board, providing a 64-bit or greater data path using connectors on both sides of a single edge.

dual parity

[Storage System] An extension of single [parity RAID](#) techniques in which [parity data](#) is stored in two independent locations.

Dual parity is applicable to multiple RAID levels (e.g., [RAID 3](#), 4, and 5); the result is some form of [RAID 6](#).

due care

[Data Security] The responsibility that managers and their organizations have a duty to provide for information security to ensure that the type of control, the cost of control, and the deployment of control are appropriate for the system being managed. [NIST SP 800-30]

duplicate

1. [Data Management] A general term for a copy of a collection of data, including point in time copies.
2. [Data Management] The action of making a duplicate as defined above.
See [replicate](#), [snapshot](#).
3. [Data Management] Any [redundant](#) component in a system.

duplicate data

[Storage System] Data which is [redundant](#) with data that is already in a dataset or I/O stream.

Dynamic Host Control Protocol (DHCP)

[Network] An [Internet protocol](#) that allows nodes to dynamically acquire ("lease") network addresses for periods of time rather than having to pre-configure them.

DHCP greatly simplifies the administration of large networks, and networks in which nodes such as laptops frequently join and depart.

dynamic mapping

[Storage System] A form of [mapping](#) in which the correspondence between addresses in the two address spaces can change over time.

See [algorithmic mapping](#), [tabular mapping](#).

Dynamic Random Access Memory (DRAM)

[Hardware] Byte-addressable computer memory that requires periodic refreshing.

E

E

E_Port

[Fibre Channel] The “Expansion” port within a [Fibre Channel switch](#) that connects to another Fibre Channel switch or [bridge](#) device via an inter-switch link.

E_Ports are used to link Fibre Channel switches to form a multi-switch fabric.

EAL

[Data Security] Acronym for [Evaluation Assurance Level](#).

EB

EByte

[General] Shorthand for [Exabyte](#).

Ebit

[General] Shorthand for [Exabit](#).

EBU

[Standards] Acronym for [European Broadcast Union](#).

ECC

[Storage System] [Data Communication] Acronym for [Error Correcting Code](#).

economizer

[Energy] Heat exchanger technology used to leverage colder external air to provide data center cooling.

Dry side economizers use cooler outdoor air; wet side economizers use cooling towers or chillers.

EcoStor™

[Standards] [Storage System] A family of SNIA standards for storage power management and related technologies.

EDE

[Data Security] Acronym for [Encryption-Decryption](#)-Encryption.

e-discovery

[Data Security] Short for [electronic discovery](#).

EE_buffer

[Fibre Channel] A buffer associated with [end-to-end flow control](#).

EE_credit

[Fibre Channel] A [credit](#) scheme used to manage [end-to-end flow control](#) during the [exchange](#) of frames between two communicating devices.

effective capacity

[Storage System] The amount of data stored on a storage system, plus the amount of unused [formatted capacity](#) in that system.

There is no way to precisely predict the effective capacity of an unloaded system. This measure is normally used on systems employing space optimization technologies.

An estimated calculation may be made as follows. Let D = the size of data already stored, F_d be the formatted capacity used to store that data, and F_t be the total formatted capacity on the system. Then the estimated effective capacity E_e is given by the formula $E_e = D / (F_d / F_t)$. No unused formatted capacity is used in the estimation calculation.

effective capacity power efficiency

[Storage System] The ratio of the [effective capacity](#) of an [idle](#) storage system to the amount of power required to maintain the system in a [ready idle](#) state.

egress routing function

[Fibre Channel] An entity within a [Routing Function](#) that performs the [egress routing function role](#).

egress routing function role

[Fibre Channel] A process within a [Routing Function](#) that validates the [frame](#), translates the [S_ID](#), and then forwards the frame to the [Native Fabric](#).

Eibit

[General] Shorthand for [Exbibit](#).

EiB**EiByte**

[General] Shorthand for [Exbibyte](#).

electrical efficiency

[Computer System] The efficiency of any electrical device which transforms one type of power into another.

Efficiency is defined as output power divided by input power expressed as a percentage. All electrical components in a computer system, such as PDUs, UPSs and power supplies, incur some degree of power loss. Determining the total power loss in smaller systems with one [power supply](#) can be done by straightforward measurement of wall plug power and the total power supplied at the power supply's outputs. Larger systems require more complex methods.

electronic discovery

[Legal] Discovery that includes the identification, preservation, collection, processing, review, analysis, or production of Electronically Stored Information. [ISO/IEC 27050-1]

Although electronic discovery is often considered a legal process, its use is not limited to the legal domain. See [e-discovery](#).

electronic storage element

[Storage System] Synonym for [Solid State Disk](#).

Electronically Stored Information (ESI)

[Legal] Data or information of any kind and from any source, whose temporal existence is evidenced by being stored in, or on, any electronic medium. [ISO/IEC 27040]

Electronically Stored Information (ESI) includes traditional e-mail, memos, letters, spreadsheets, databases, office documents, presentations, and other electronic formats commonly found on a computer. ESI also includes system, application, and file-associated [metadata](#) (3.26) such as timestamps, revision history, file type, etc. Electronic medium can take the form of, but is not limited to, storage devices and storage elements.

embedded controller

embedded storage controller

[Storage System] An intelligent [storage controller](#) that mounts in a [host computer](#)'s housing and attaches directly to a host's internal [I/O interconnect](#), which is attached to storage devices mounted inside the host computer's housing.

Embedded controllers obviate the need for [host bus adapters](#) and external host I/O interconnects. Embedded storage controllers differ from host bus adapters in that they provide functions beyond I/O interconnect [protocol](#) conversion (e.g., [RAID](#)).

Emerald

[Storage Systems] SNIA Emerald™ Power Efficiency Measurement Specification or SNIA Emerald™ Program.

Emerald Specification

[Storage Systems] SNIA Emerald™ Power Efficiency Measurement Specification.

Defines a uniform taxonomy of storage subsystems and a standard way of measuring power efficiency of the storage

subsystems defined in the taxonomy. For more detailed information, please consult the SNIA Emerald Program website (<https://www.snia.org/emerald>).

Enc_Header

[Fibre Channel] An encapsulation header used for forwarding [FC](#) frames from a source [Routing Function](#) to a destination Routing Function.

Encapsulating Security Payload (ESP)

[Data Security] A component of [IPsec](#) that permits the specification of various [confidentiality](#) mechanisms.

encoding

[Fibre Channel] Generation of transmission characters from valid data bytes and special codes.

encryption

[Data Security] The conversion of [plaintext](#) to encrypted text with the intent that it only be accessible to authorized users who have the appropriate [decryption](#) key.

End Of Frame (EOF)

[Fibre Channel] A group of ordered sets that delineates the end of a [frame](#).

end-to-end encryption

[Data Security] [Encryption](#) of information at its origin and [decryption](#) at its intended destination without intermediate decryption.

end-to-end flow control

1. [Network] Control of message flow between the two end parties to a communication on a network.
2. [Fibre Channel] Flow control that occurs between two communicating [Fibre Channel](#) Nx-Ports.

end-to-end security

[Data Security] Safeguarding information in an information system from point of origin to point of destination. [CNSSI-4009]

energy efficiency

[Computer System] The [power efficiency](#) of a system over time.

While power and energy efficiency look about the same to a layman, the numbers may be different (even neglecting the units) on account of temporal variations in supply voltages, power and load factors and so on.

Enhanced Transmission Selection (ETS)

[Network] A [DCB](#) component that specifies a [frame](#) scheduling mechanism to support the allocation of [bandwidth](#) amongst traffic classes that share a link.

ENode MAC address

[Fibre Channel] [Network] The [MAC](#) address used by the ENode during the [FCoE Initialization Protocol](#) (FIP).

Enterprise Resource Management (ERM)

[Management] [Network] Software that manages all aspects of an organization's assets, systems, services and functions.

ERM systems manage a set of resources in the wider perspective of an organization's entire business. Managing in an enterprise context requires that entities be named uniquely and locatable within the enterprise, that heterogeneity of platforms and services may be assumed, and that the dynamic nature of the environment is taken into account.

Enterprise Systems Connection (ESCON)

[Storage System] A 200 [Mbps serial I/O interconnect](#) used on IBM Corporation's Enterprise System 9000 data center computers.

Similar to [Fibre Channel](#) in many respects, ESCON is based on [redundant](#) switches to which computers and storage subsystems connect using serial optical connections.

entropy

[Data Security] A measure of the amount of uncertainty that an attacker faces to determine the value of a secret. [NIST SP 800-63]

The value is sometimes measured in bits of [security strength](#), where a value of 0 indicates no security strength (i.e., full predictability or no randomness) and a positive value indicates increasing security strength.

entry/exit slot

[Storage System] A location in a [library](#) through which a removable [volume](#) can be inserted or removed.

EOF

1. [Fibre Channel] Acronym for [End of Frame](#).
2. [File System] A designation or marker for the end of a file.

erasure coding

[Data Recovery] A forward error correction technology used to provide data resiliency and long-term data integrity, by spreading data blocks and parity information across multiple storage devices or systems that may be in multiple physical locations.

Both the level of resiliency and where erasure coding is applied (at the array, at the node, or at the system level) can significantly affect how much processing overhead it consumes.

ERM

[Management] [Network] Acronym for [Enterprise Resource Management](#).

Error Correcting Code (ECC)

[Storage System] [Data Communication] A scheme for checking the correctness of data that has been stored and retrieved, and correcting it if necessary.

An ECC consists of a number of bits computed as a function of the data to be protected, and appended to the data. When the data and ECC are read, the function is recomputed, the result is

compared to the ECC appended to the data, and correction is performed if necessary. Error correcting codes differ from cyclic [redundancy](#) checks in that the latter can detect errors, but are not generally capable of correcting them. See [cyclic redundancy check](#).

ESCON

[Storage System] Acronym for [Enterprise Systems Connection](#).

ESI

[Legal] Acronym for [Electronically Stored Information](#).

ESP

[Data Security] Acronym for [Encapsulating Security Payload](#).

Ethernet

[Network] A local area networking technology based on packetized transmissions between physical ports over a variety of electrical and optical [media](#).

Ethernet can transport any of several upper layer protocols, the most popular of which is [TCP/IP](#). Ethernet standards are maintained by the IEEE 802.3 committee.

The unqualified term Ethernet usually refers to 10 [Mbps](#) transmission on multi-point copper. Fast Ethernet is used to denote 100 Mbps transmission, also on multipoint copper facilities. Ethernet and Fast Ethernet both use [CSMA/CD](#) physical signaling. [Gigabit Ethernet](#) (abbreviated GBE) transmits at 1250 [Megabaud](#) (1 [Gbit](#) of data per second) using [8b/10b encoding](#) with constant transmission detection.

Ethernet adapter

[Network] An [adapter](#) that connects an [intelligent device](#) to an [Ethernet](#) network., usually called an Ethernet [network interface card](#), or Ethernet NIC.

See [NIC](#).

European Broadcast Union (EBU)

[Standards] An alliance of public service media organizations, with members in 56 countries.

In the domains of networks and storage systems, the EBU cooperates with relevant organizations including [SMPTE](#), VSF, AMWA and others.

eventual consistency

A behavior of a distributed system that does not provide immediate consistency guarantees.

See [CAP Theorem](#).

evidence preservation

[Legal] A process to maintain and safeguard the integrity and/or original condition of the potential digital evidence. [ISO/IEC 1WD 27037]

EVSN

[Data Recovery] Acronym for [External Volume Serial Number](#).

Exabit (Ebit)

[General] Shorthand for 1,000,000,000,000,000,000 (10^{18}) bits.

The SNIA uses the base 10 convention commonly found in I/O-related and scientific literature rather than the base 2 convention (1,152,921,504,606,846,976, i.e., 2^{60}) common in computer system and software literature.

See also [Exbibit](#).

Exabyte (EB)

[General] Shorthand for 1,000,000,000,000,000,000 (10^{18}) bytes.

The SNIA uses the base 10 convention commonly found in I/O-related and scientific literature rather than the base 2 convention (1,152,921,504,606,846,976, i.e., 2^{60}) common in computer system and software literature.

See also [Exbibyte](#).

Exbibit (Eibit)

[General] Shorthand for 1,152,921,504,606,846,976 (2^{60}) bits.

Binary notation is most commonly used for semiconductor memory sizes.

See also [Exabit](#).

Exbibyte (EiB)

[General] Shorthand for 1,152,921,504,606,846,976 (2^{60}) bytes.

Binary notation is most commonly used for semiconductor memory sizes.

See also [Exabyte](#).

exchange

[Fibre Channel] A set of one or more non-concurrent related sequences passing between a pair of [Fibre Channel](#) ports.

An exchange encapsulates a “conversation” such as a [SCSI](#) task or an [IP](#) exchange. Exchanges may be bidirectional and may be short or long lived. The parties to an exchange are identified by an [Originator Exchange Identifier](#) (OX_ID) and a [Responder Exchange Identifier](#) (RX_ID).

Exchange_Identifier

[Fibre Channel] A generic term denoting either an [Originator Exchange Identifier](#) ([OX_ID](#)) or a [Responder Exchange Identifier](#) ([RX_ID](#)).

exchange status block

[Fibre Channel] A data structure that contains the state of an [exchange](#).

An [originator N_Port](#) or [NL_Port](#) has an Originator Exchange Status [Block](#) and a [Responder N_Port](#) or [NL_Port](#) has a Responder Exchange Status Block for each concurrently active exchange.

exclusive connection

[Fibre Channel] A [Class 1 dedicated connection](#) without [intermix](#).

expansion card

expansion module

[Computer System] A collective term for [optional](#) adapters in the form of printed [circuit](#) modules that can be added to intelligent devices.

Expansion cards include [host bus adapters](#), network interface cards, as well as [NVRAM](#), [console](#), and other special purpose adapters.

expansion slot

[Computer System] A mounting and internal bus attachment device within an [intelligent device](#) into which expansion cards are inserted.

expired data

[Data Management] Data that is no longer required to be retained for any reason, becoming a candidate for [permanent deletion](#).

Data may become expired when it has reached its defined [retention period](#) or when an event makes it obsolete and it has no further value to the organization. See [disposition policy](#).

explicit addressing

[Storage System] A form of [addressing](#) in which the data's address is explicitly specified in the access request.

See [implicit addressing](#).

exploit

[Data Security] A defined way to breach the security of an IT system through a [vulnerability](#).

E

export

1. [Computer System] Synonym for present, i.e., to cause to appear or make available.
2. [Computer System] To move objects, such as data, from within a system to a location outside the system, usually requiring a [transformation](#) during the move.

[Disk array control software](#) exports virtual disks to its [host environment](#). In file systems, a [directory](#) may be exported or made available for access by remote clients.

extended file attribute

[File System] An element of file [metadata](#).

Extended_Header

[Fibre Channel] A [sequence](#) of words that may be present in a [frame](#) between the [SOF delimiter](#) and the [Frame_Header](#) to support frame handling functions not enabled by the [Frame_Header](#).

eXtensible Access Method (XAM)

[Standards] An interface standardized by the SNIA that provides applications with standard methods for storing data and associated [metadata](#) on [fixed content storage](#).

The XAM [Application Programming Interface](#) (API) is being standardized by SNIA.

eXtensible Markup Language (XML)

[Standards] A universal format for structured documents and data on the World Wide Web.

The World Wide Web Consortium is responsible for the XML specification. See www.w3.org.

extent

1. [Storage System] A set of consecutively addressed [FBA](#) disk blocks that is allocated to consecutive addresses of a single file.

2. [Storage System] A set of consecutively located tracks on a [CKD](#) disk that is allocated to a single file.
3. [Storage System] A set of consecutively addressed disk blocks that is part of a single [virtual disk-to-member disk array mapping](#).

A single disk may be organized into multiple extents of different sizes, and may have multiple (possibly) non-adjacent extents that are part of the same virtual disk-to-member disk array mapping. This type of extent is sometimes called a [logical disk](#).

external controller

external disk controller

external storage controller

[Storage System] An intelligent [storage controller](#) that mounts outside its [host computer](#)'s enclosure and attaches to hosts via external I/O interconnects.

External storage controllers usually mount in the enclosure containing the disks they control.

External Volume Serial Number (EVSN)

[Data Recovery] A human-readable [volume serial](#) number on a removable volume.

eye

[Data Communication] The center region of an [eye diagram](#) that does not occur for correctly formed signals, that distinguishes presence of signal (region above the eye) from absence of signal (region below the eye).

eye diagram

[Data Communication] A diagram used to specify optical or electrical signal transition characteristics for transmitters, in which the horizontal axis represents normalized time from pulse start and the vertical axis represents normalized amplitude.

eye opening

[Data Communication] Quantitative measure of the space in an [eye diagram](#) that does not occur for correctly formed signal

E

transitions, and that prevents signal values from incorrectly being identified as high or low.

F

F_Port

[Fibre Channel] The “Fabric” port within a [Fibre Channel](#) fabric [switch](#) that provides a point-to-point link attachment to a single [N_Port](#).

F_Ports are intermediate ports in virtual point-to-point links between end system ports, for example the N_Port on an end node to the F_Port on a switch to the F_Port in that switch to the N_Port on the other end node using a single Fibre Channel fabric switch. An F_Port is assumed to always refer to a port to which non-loop PN_Ports are attached to a Fabric, and does not include FL_Ports [FC-FS-2].

F_Port name

[Fibre Channel] A [Name Identifier](#) associated with an [F_Port](#). fabric

[Fibre Channel] An entity consisting of one or more Switches that [interconnect](#) various Nx_Ports attached to it, and capable of routing frames using only the [D_ID](#) information in an [FC-2 frame](#) header.

Fabric_Identifier (F_ID)

[Fibre Channel] An identifier assigned to each Fabric in an [Inter-Fabric Routing](#) environment.



Fabric_Name

[Fibre Channel] A [Name Identifier](#) associated with a fabric.

Fabric Login

[Fibre Channel] The process by which a [Fibre Channel node](#) establishes a logical [connection](#) to a fabric [switch](#).

Fabric Provided MAC Address (FPMA)

[Fibre Channel] [Network] A [MAC](#) address that is assigned by an FCF and is fabric-wide unique.

failback

[Computer System] The [restoration](#) of a failed system component's share of a load to a replacement component after a failback event.

When a failed [controller](#) in a [redundant configuration](#) is replaced, the devices that were originally controlled by the failed controller are usually *failed back* to the replacement controller to restore the I/O balance, and to restore [failure tolerance](#). Similarly, when a defective fan or [power supply](#) is replaced, its load, previously borne by a redundant component can be *failed back* to the replacement part.

failed over

[Computer System] A [mode of operation](#) for failure tolerant systems in which a component has failed and its function has been assumed by a [redundant](#) component.

A system that protects against single failures operating in failed over mode is not failure tolerant, since failure of the redundant component may render the system unable to function. Some systems (e.g., clusters) are able to tolerate more than one failure; these remain failure tolerant until no redundant component is available to protect against further failures.

failover

[Computer System] The automatic [substitution](#) of a functionally equivalent system component for a failed one.

The term failover is most often applied to intelligent controllers connected to the same storage devices and host computers. If one of the controllers fails, failover occurs, and the survivor takes over its [I/O load](#).

failure tolerance

[Computer System] The ability of a system to continue to perform its function (possibly at a reduced performance level) when one or more of its components has failed.

Failure tolerance in disk subsystems is often achieved by including [redundant](#) instances of components whose failure would make the system inoperable, coupled with facilities that allow the [redundant components](#) to assume the function of failed ones.

FAN

[File System] [Network] Acronym for [File Area Network](#).

F

fanout

[Storage System] Synonym for [device fanout](#).

fast mirror resynchronization

[Data Recovery] A technique for reducing the time required to [synchronize](#) a split [mirror](#) with the set of storage devices from which it was split.

Fast [mirror resynchronization](#) requires that a list of changes to the original set of data since moment of splitting be kept. When the split mirror is rejoined to the original set of volumes, only the data items identified in the list are copied from the original to the split mirror rather than the entire contents of the devices.

fast SCSI

[SCSI] A form of [SCSI](#) that provides 10 megatransfers per second.

Wide fast SCSI has a 16-bit data path, and transfers 20 MBytes per second. Narrow fast SCSI transfers 10 MBytes per second. See [wide SCSI](#), [Ultra SCSI](#), [Ultra2 SCSI](#), [Ultra3 SCSI](#).

fault tolerance

[Computer System] Synonym for [failure tolerance](#).

FBA

[Storage System] Acronym for [Fixed Block Architecture](#).

FC

[Fibre Channel] Acronym for [Fibre Channel](#).

FC-0

[Fibre Channel] The [Fibre Channel protocol](#) level that encompasses the physical characteristics of the interface and data transmission [media](#).

FC-1

[Fibre Channel] The [Fibre Channel protocol](#) level that encompasses [8B/10B encoding](#), and transmission protocol

FC-2

[Fibre Channel] The [Fibre Channel protocol](#) level that encompasses signaling protocol rules and the organization of data into frames, sequences, and exchanges.

FC-2M

[Fibre Channel] The [Fibre Channel protocol](#) sublevel, that routes frames between VN_Ports and LCFs, based on the [D_ID](#) in the [Frame Header](#) and the [VF_ID](#) in the [VFT Header](#) if there is a VFT_Header.

FC-2P

[Fibre Channel] The [Fibre Channel protocol](#) sublevel, that defines the rules and provides mechanisms that shall be used to transfer frames via the [FC-1](#) level.

FC-2V

[Fibre Channel] The [Fibre Channel protocol](#) sublevel, that defines functions and facilities that a [VN Port](#) may provide for use by an [FC-4](#) level, regardless of the [FC-1](#) that is used.

FC-3

[Fibre Channel] The [Fibre Channel protocol](#) level that defines a set of services that are common across multiple Nx_Ports of a [node](#).

[FC-3](#) includes protocols for Basic Link Services, Extended Link Services and Hunt Groups.

FC-4

[Fibre Channel] The [Fibre Channel protocol](#) level that encompasses the [mapping](#) of upper layer protocols ([ULP](#)) such as [IP](#) and [SCSI](#) to lower protocol layers ([FC-0](#) through [FC-3](#)).

An example of an FC-4 standard is the mapping of SCSI commands to Fibre Channel (FCP-3).

FC-AE

[Fibre Channel] Shorthand for [Fibre Channel Avionics Environment](#).

FC-AL**FC-AL-2**

[Fibre Channel] Shorthand for [Fibre Channel Arbitrated Loop](#).

In this and other FC-related entries, the numbers denote versions of the spec, developed and maintained by the [INCITS T11](#) committee, that bears that name. The listed version is current as of this writing.

FC-AV

[Fibre Channel] Shorthand for [Fibre Channel](#) Audio Video.

FC-BB**FC-BB-6**

[Fibre Channel] Shorthand for [Fibre Channel Backbone](#).

When used, the number denotes a version of the spec. The listed version is current as of this writing.

FC-DA

[Fibre Channel] Shorthand for [Fibre Channel Device Attach](#).

FC-FS

FC-FS-4

[Fibre Channel] Shorthand for [Fibre Channel Framing and Signaling](#).

When used, the number denotes a version of the spec. The listed version is current as of this writing.

FC-GS

FC-GS-7

[Fibre Channel] Shorthand for [Fibre Channel Generic Services](#).

When used, the number denotes a version of the spec. The listed version is current as of this writing.

FC-IFR

[Fibre Channel] Shorthand for [Fibre Channel Inter-Fabric Routing](#).

FC-LS

FC-LS-3

[Fibre Channel] Shorthand for [Fibre Channel Link Services](#).

When used, the number denotes a version of the spec. The listed version is current as of this writing.

FC-MI

FC-MI-3

[Fibre Channel] Shorthand for [Fibre Channel Methodologies for Interconnects](#).

When used, the number denotes a version of the spec. The listed version is current as of this writing.

FC-NVMe

[Fibre Channel] Shorthand for [Fibre Channel NVMe](#).

FC-PI

FC-PI-5

FC-PI-6

[Fibre Channel] Shorthand for [Fibre Channel Physical Interface](#).

When used, the number denotes a version of the spec. The listed versions are current as of this writing.

FC_Port

[Fibre Channel] A port that is capable of transmitting and receiving [Fibre Channel](#) frames according to the [FC-0](#), [FC-1](#), [FC-2](#), and [FC-3](#) levels of the Fibre Channel standards.

An FC_Port includes an LCF and at least one [Nx_Port](#). The following are FC_Ports: PN_Ports, L_Ports, F_Ports, FL_Ports, Fx_Ports, E_Ports, and B_Ports.

FC-SB

FC-SB-2

FC-SB-3

[Fibre Channel] Shorthand for [Fibre Channel Single Byte \(command set\)](#).

FC-SP

[Fibre Channel] Shorthand for [Fibre Channel Security Protocols](#).

FC-SW

FC-SW-6

[Fibre Channel] Shorthand for [Fibre Channel Switched \(fabric interconnect\)](#).

When used, the number denotes a version of the spec. The listed versions are current as of this writing.

FC-VI

[Fibre Channel] Shorthand for [Fibre Channel Virtual Interface](#).

FC Entity

[Fibre Channel] [Network] The interface between an [FC Switching Device](#) or an FC stack and the [FCoE Entity](#).

Each FC Entity contains a single instance of either a VE_Port, a VF_Port, or a [VN_Port](#).

FCA

[Fibre Channel] Shorthand for [Fibre Channel](#) Association.

FCDF

[Fibre Channel] Shorthand for [Fibre Channel Data-Plane Forwarder](#)

FCF

[Fibre Channel] Shorthand for [FCoE Forwarder](#).

FCIA

[Fibre Channel] Shorthand for [Fibre Channel Industry Association](#).

FCoE

[Fibre Channel] [Network] Acronym for [Fibre Channel over Ethernet](#).

FCoE Controller

[Fibre Channel] [Network] A functional entity, coupled with a [Lossless Ethernet MAC](#), that instantiates VE_Ports, VF_Ports, and VN_Ports, and/or creates [FCoE_LEPs](#).

FCoE Entity

[Fibre Channel] [Network] The interface between the [FC Entity](#) and a [Lossless Ethernet MAC](#). Each [FCoE](#) Entity contains one or more [FCoE_LEPs](#).

FCoE Forwarder (FCF)

[Fibre Channel] [Network] A [Fibre Channel](#) Switching Device with one or more Lossless [Ethernet](#) MACs, each coupled with an [FCoE Controller](#), and optionally one or more Lossless Ethernet bridging devices and optionally an [FC](#) Fabric interface.

An FCF forwards FCoE frames addressed to one of its FCF-MACs based on the [D_ID](#) of the encapsulated FC frames.

FCoE Initialization Protocol (FIP)

[Fibre Channel] [Network] A [protocol](#) that enables the discovery and [instantiation](#), and maintenance of [FCoE](#) devices.

FCoE Link Endpoint (FCoE_LEP)

[Fibre Channel] [Network] The data forwarding component of an [FCoE Entity](#) that handles [FC frame](#) encapsulation/decapsulation,

and transmission/reception of encapsulated frames through a single [Virtual Link](#).

FCoE Node (ENode)

[Fibre Channel] [Network] A [Fibre Channel Node](#) with one or more Lossless [Ethernet](#) MACs, each coupled with an [FCoE Controller](#).

FCP

[Fibre Channel] Shorthand for [Fibre Channel Protocol](#).

FCP-*n*

[SCSI] A series of standards that describes the operation of the [SCSI protocol](#) over [Fibre Channel](#) links.

FDDI

[Network] Acronym for [Fiber Distributed Data Interface](#).

FDDI adapter

[Network] An [adapter](#) that connects an [intelligent device](#) to an [FDDI](#) network.

Both FDDI-fiber adapters that connect to optical fiber FDDI networks, and FDDI-TP adapters that connect to twisted copper pair FDDI networks exist. Although network interface cards are usually referred to as NICs rather than as adapters, the term *FDDI adapter* is more common than FDDI NIC. See [NIC](#).

Federal Information Processing Standard (FIPS)

[Data Security] Standards (and guidelines) produced by [NIST](#) for government-wide use in the specification and procurement of Federal computer systems.

Federal Rules of Civil Procedure (FRCP)

[Legal] A set of regulations that specify procedures for civil legal suits within United States District (federal) Courts.

Federal district courts in all fifty states are required to follow these rules. Many state courts' civil procedural rules closely follow or adopt similarly worded rules.

See also [FRCP](#)

F

federated deduplication

[Storage System] [Deduplication](#) across multiple storage systems.

Federated Management Architecture Specification

[Management] [Network] A specification that defines a set of [Java](#) APIs for heterogeneous storage resource and storage network management.

This specification is a central technology of Jiro.

Fiber Distributed Data Interface (FDDI)

[Network] An [ANSI](#) standard for a [token ring](#) Metropolitan Area Networks (MANs), based on the use of optical fiber cable to transmit data at a rate of 100 Mbits/second.

Both optical fiber and twisted copper pair variations of the FDDI physical standard exist. FDDI is a completely separate set of standards from [Fibre Channel](#). The two are not directly interoperable.

fibres

[Fibre Channel] The international spelling of the American word *fiber*.

The British spelling was selected for the [Fibre Channel](#) technology, though the American spelling is used to describe the fiber optic technologies defined for Fibre Channel.

Fibre Channel (FC)

[Fibre Channel] A [serial I/O interconnect](#) capable of supporting multiple protocols, including access to open system storage ([FCP](#)), access to mainframe storage ([FICON](#)), and networking ([TCP/IP](#)).

[Fibre Channel](#) supports point to point, [arbitrated loop](#), and switched topologies with a variety of copper and optical links running at speeds from 1 [Gb/s](#) to 10 Gb/s. The committee standardizing Fibre Channel is the [INCITS](#) Fibre Channel ([T11](#)) Technical Committee.

Fibre Channel Arbitrated Loop (FC-AL)

[Fibre Channel] A form of [Fibre Channel interconnect](#) in which up to 126 nodes are connected in a loop [topology](#), with each [node's L_Port transmitter](#) connecting to the L_Port [receiver](#) of the next node on the loop.

Nodes connected to a Fibre Channel Arbitrated Loop arbitrate for the single transmission that can occur on the loop at any instant using a Fibre Channel Arbitrated Loop protocol that is different from Fibre Channel switched and point to point protocols. An arbitrated loop may be private (no fabric connection) or public (attached to a fabric by an FL_Port). The network is defined by the FC-AL-2 standard INCITS 332 - 1999 [R2004].

Fibre Channel Avionics Environment (FCAE)

[Fibre Channel] The technical report describing a specific subset of [Fibre Channel](#) for use in defense and avionic applications.

Fibre Channel Backbone (FC-BB)

[Fibre Channel] A standard that defines mappings for transporting [Fibre Channel](#) over different network technologies, including operation of [Fibre Channel over Ethernet](#) (FCoE).

Fibre Channel Data-Plane Forwarder (FCDF)

[Fibre Channel] A simplified FC switching entity that forwards FC frames via A_Ports and F_Ports through an FCDF Switching Element.

Fibre Channel Device Attach (FC-DA)

[Fibre Channel] A technical report that selects and restricts logical options from the [Fibre Channel Framing and Signaling](#), [Fibre Channel Protocol](#) for [SCSI](#), [Fibre Channel Arbitrated Loop](#), [Fibre Channel Generic Services](#), and [Fibre Channel Single Byte Command Set](#) standards.

The intent of the technical report is to facilitate [interoperability](#) between devices whether they are connected in a loop or fabric [topology](#).

Fibre Channel Framing and Signaling (FC-FS)

[Fibre Channel] A standard describing the framing and signaling requirements for [Fibre Channel](#) links.

Fibre Channel Generic Services (FC-GS)

[Fibre Channel] A standard describing in detail the Generic Services introduced in [FC-FS-2](#), i.e., the name services, management services, and discovery services.

Fibre Channel Industry Association (FCIA)

[Fibre Channel] A mutual benefit corporation formed under the non-profit corporation laws of the State of California, whose members consist of companies that manufacture [Fibre Channel](#) systems, components, software, and tools, as well as provide Fibre Channel education and services to end-user customers.

Fibre Channel Interaction Space

[Fibre Channel] The set of [Fibre Channel](#) ports, devices, and Fabrics that are connected by Fibre Channel links or are accessible by a common instance of an administrative tool or tools.

Fibre Channel Inter-Fabric Routing (FC-IFR)

[Fibre Channel] A standard that specifies a set of protocols and methods to enable selective communication among Nx_Ports connected to different Fabrics.

Fibre Channel Link Services (FC-LS)

[Fibre Channel] A standard describing the Link Services for [Fibre Channel](#) links.

Fibre Channel Methodologies for Interconnects (FC-MI)

[Fibre Channel] A technical report specifying common methodologies for both [arbitrated loop](#) and switched environments, with the intention of facilitating [interoperability](#) between devices whether they are connected in a loop or Fabric [topology](#).

Fibre Channel NVMe (FC-NVMe)

[Fibre Channel] The standard that describes the [Fibre Channel](#) mapping for communication between an [NVMe host](#) and an [NVM](#) subsystem.

Fibre Channel over Ethernet (FCoE)

[Fibre Channel] [Network] A technology that encapsulates [Fibre Channel](#) frames in [Ethernet](#) frames, allowing [FC](#) traffic to be transported over Ethernet networks.

Fibre Channel Physical Interface (FC-PI)

[Fibre Channel] The [ANSI](#) standard that describes the point-to-point physical interface of a high-performance [serial](#) link for support of the higher level protocols associated with [HIPPI](#), [IPI](#), [SCSI](#) and others.

Fibre Channel Protocol (FCP)

[Fibre Channel] The [serial SCSI](#) command [protocol](#) used on [Fibre Channel](#) interconnects.

FCP standardization is the responsibility of the [INCITS TC-T10](#) committee.

Fibre Channel Security Protocols (FCSP)

[Fibre Channel] An [ANSI](#) standard that describes the protocols used to implement security in a [Fibre Channel](#) fabric.

This standard includes the definition of protocols to authenticate Fibre Channel entities, protocols to set up session keys, protocols to negotiate the parameters required to ensure [frame-by-frame integrity](#) and [confidentiality](#), and protocols to establish and distribute policies across a Fibre Channel fabric.

Fibre Channel Service Protocol (FSP)

[Fibre Channel] A [FC-4 protocol](#) that defines all services independently of [topology](#) or fabric type.

Fibre Channel Single Byte (command set) (FC-SB)

[Fibre Channel] The industry standard command [protocol](#) for [ESCON](#) over [Fibre Channel](#).

The second and third versions of this protocol are known as [FC-SB-2](#) and [FC-SB-3](#) respectively.

Fibre Channel Switched (fabric interconnect) (FC-SW)

[Fibre Channel] A standard that describes the requirements for an interconnecting fabric consisting of multiple fabric [switch](#) devices to support the [ANSI/INCITS Fibre Channel](#) protocols.

Fibre Channel Virtual Interface (FC-VI)

[Fibre Channel] A standard for application-level distributed interprocess communication based on Intel Corporation's V1.0 Virtual Interface (VI) Architecture; formerly known as VIA.

Fibre Connect (FICON)

[Fibre Channel] IBM Corporation's implementation of the [Fibre Channel Single Byte Command Set](#) standards., developed to provide a Fibre Channel compatible implementation of [ESCON](#).

FICON

[Fibre Channel] Acronym for [Fibre Connect](#).

Field Replaceable Unit (FRU)

[Computer System] A unit, or component of a system that is designed to be replaced "in the field;" i.e., without returning the system to a factory or repair depot.

Field replaceable units may either be customer-replaceable, or their replacement may require trained service personnel. See [Customer Replaceable Unit](#).

file

[File System] An abstract data object made up of (a.) an ordered [sequence](#) of data bytes stored on a disk or tape, (b.) a symbolic name by which the object can be uniquely identified, and (c.) a set of properties, such as ownership and access permissions that allow the object to be managed by a [file system](#) or [backup manager](#).

Unlike the permanent address spaces of [storage media](#), files may be created and deleted, and in most file systems, may expand or contract in size during their lifetimes.

File Area Network (FAN)

[File System] [Network] A [namespace](#)-based network-oriented infrastructure for files that includes a decoupling layer that separates logical file access from physical file location, and enables a variety of services (e.g., replication and [migration](#)) to be applied to files and file systems.

file extent

[File System] A logically contiguous region of file data.

file level deduplication

[File System] Reduction of file copies by replacing duplicates with pointers to a single original file.

See [data deduplication](#).

file mark

[Storage System] A data separator within a [volume](#).

file server

[File System] A computer whose primary purpose is to serve files to clients.

A file [server](#) may be a general purpose computer that is capable of hosting additional applications or a special purpose computer capable only of serving files. See [filer](#).

file system

[File System] A software component that imposes structure on the address space of one or more physical or virtual disks so that applications may deal more conveniently with abstract named data objects of variable size (files).

File systems are often supplied as operating system components, but are also implemented and marketed as independent software components.

Spelling *filesystem* as a single word is also correct, especially when the term is used as an adjective.

file system virtualization

1. [File System] The act of aggregating multiple file systems into one large virtual [file system](#), so that users access data objects through the virtual file system and are unaware of the underlying [partitioning](#).
2. [File System] The act of providing additional new or different functionality, e.g., a different file access [protocol](#), on top of one or more existing file systems.

file virtualization

1. [File System] The use of [virtualization](#) to present several underlying file or [directory](#) objects as one single composite file.
2. [File System] The use of virtualization to provide [HSM](#) like properties in a storage system.
3. [File System] The use of virtualization to present an integrated file interface when file data and [metadata](#) are managed separately in the storage system. See [block virtualization](#).

filer

[File System] An intelligent network [node](#) whose hardware and software are designed to provide file services to [client](#) computers.

Filers are pre-programmed by their vendors to provide file services, and are not normally user programmable. See [appliance](#), [file server](#).

fill word [Out of Order. Fix it?]

[Fibre Channel] A [transmission word](#) that is an [idle](#) or an ARBx [primitive signal](#).

Fill words are transmitted between frames, primitive signals, and primitive sequences to keep a [fibre channel](#) network active.

FIM

[Data Recovery] Acronym for [Frozen Image Method](#).

fingerprint

[Storage System] An identifier derived from the data, used to detect [redundancy](#).

FIPS

[Data Security] Acronym for [Federal Information Processing Standard](#).

firmware

[Computer System] Low-level software for booting and operating an [intelligent device](#).

Firmware generally resides in read-only memory (ROM) on the device.

First Burst

[Fibre Channel] An optimization for the transmission, by an initiator, of the first DATA [IU](#) in a Data Series for a write operation.

Fixed Block Architecture (FBA)

[SCSI] A model of disks in which storage space is organized as linear, dense address spaces of blocks of a fixed size.

Fixed block architecture is the disk model on which [SCSI](#) is predicated. See [count-key-data](#).

fixed content

1. [Data Management] Content that does not change.
2. [Data Management] Content that is prevented from change by the storage container in which it is kept.

fixed content storage

[Storage System] Storage systems and technology specialized for storing [fixed content](#) (i.e., data that does not change).

fixed-length segmentation

[Storage System] [Partitioning](#) a byte stream into parts that are a constant number of bytes when performing [compression](#) or [hash-based data deduplication](#).

See [variable-length segmentation](#).

FL_Port

[Fibre Channel] A "Fabric Loop" port within a [Fibre Channel switch](#), capable of [Fibre Channel Arbitrated Loop](#) operations and connected to one or more NL_Ports via a Fibre Channel Arbitrated Loop.

An FL_Port becomes a shared entry point for public NL_Port devices to a Fibre Channel fabric. FL_Ports are intermediate ports in virtual point-to-point links between end ports that do not reside on the same loop, for example the NL_Port on an end [node](#) to the FL_Port on a switch to the [F_Port](#) in that switch to the [N_Port](#) on that end node through a single Fibre Channel fabric switch.

flash array

[Storage System] Synonym for [solid state storage array](#).

flash memory

[Hardware] A type of non-volatile memory used in [solid state storage](#).

flash memory array

[Storage System] Synonym for [solid state storage array](#).

FLOGI

[Fibre Channel] Short for [Fabric LOGIn](#).

flywheel UPS

[Energy] A [UPS](#) that uses the momentum of a spinning disk or wheel to temporarily generate electricity in the event of a data center power failure.

Flywheel energy storage technology provides the bridge between normal power distribution and backup diesel generators and can replace conventional battery rooms.

FMR

[Data Recovery] Acronym for [Fast Mirror Resynchronization](#).

FOB

[Solid State] Industry-speak for the new out-of-the-box state of an [FRU](#), especially in reference to flash storage.

forensic copy

[Data Security] An accurate bit-for-bit reproduction of the information contained on an electronic device or associated media, whose validity and integrity has been verified using an accepted algorithm. [NIST SP 800-72]

F

formatted capacity

[Storage System] The total amount of bytes available to be written after a system or device has been formatted for use, e.g., by an object store, filesystem or [block services](#) manager.

Formatted capacity, also called [usable capacity](#), is less than or equal to [raw capacity](#). It does not include areas set aside for system use, spares, [RAID](#) parity areas, [checksum](#) space, host- or filesystem-level remapping, "right sizing" of disks, disk labeling and so on. However, it may include areas that are normally [reserved](#)—such as [snapshot](#) setasides—if they can alternatively be configured for ordinary data storage by the storage admin.

formatting

[Storage System] The preparation of a disk for use by writing required information on the [media](#).

Disk controllers format disks by writing [block](#) header and trailer information for every block on the disk. Host software

components such as [volume](#) managers and file systems format disks by writing the initial structural information required for the volume or [file system](#) to be populated with data and managed.

forward error correction (FEC)

[Data Recovery] A set of algorithms that perform corrections that allow for recovery of one or more bit errors.

frame

[Fibre Channel] An ordered series of words that is the basic unit of data transmission in a [Fibre Channel](#) network.

A Fibre Channel frame consists of a [Start of Frame](#) Word (SoF) (40 bits); a Frame Header (8 Words or 320 bits); data (0 to 524 Words or 0 to 2192 ten bit encoded bytes; a [CRC](#) (One Word or 40 bits); and an [End of Frame](#) (EoF) (40 bits). See [data frame](#).

frame content

[Fibre Channel] The information contained in a [frame](#) between its Start-of-Frame and End-of-Frame delimiters, excluding the delimiters.

Frame_Header

[Fibre Channel] A [sequence](#) of words that follows the [SOF delimiter](#) and any Extended_Headers in a [frame](#) to control link operations and device [protocol](#) transfers as well as detect missing or out of order frames.

Frame Scrambling

[Fibre Channel] A technique for lowering the electromagnetic emission from [Fibre Channel](#) equipment by [encoding frame content](#) in a way to minimize repetitive bit sequences.

Frame Scrambling is required for operation at 8GFC.

FRCP

[Legal] Acronym for [Federal Rules of Civil Procedure](#).

free capacity

Deprecated synonym for [free space](#).

free space

1. [Data Management] The amount of capacity reported to an end user as unused [assigned capacity](#).
In a simple world, free space is normally the same as assigned capacity less the amount of assigned capacity already written. But restrictions such as quotas and interactions between systems using different arithmetic may cause the reported free space to vary from the actual quantity.
2. [Storage System] The amount of capacity reported to the storage admin as unused [formatted capacity](#).

front domain

[Fibre Channel] A [domain](#) presented by a [front domain switch](#).

front domain switch

[Fibre Channel] A [switch](#) within an [Inter-Fabric Router](#) that provides connectivity to the Fabrics that are interconnected by the Inter-Fabric Router.

F

FRU

[Computer System] Acronym for [Field Replaceable Unit](#).

frozen image

[Data Recovery] Synonym for [point in time copy](#).

Frozen Image Method (FIM)

[Data Recovery] A method by which a [frozen image](#) of a set of data can be generated.

Split [mirrors](#) and copy-on-write snapshots are the two common methods of generating frozen images.

FSP

[Fibre Channel] Acronym for [Fibre Channel Service Protocol](#).

full backup

[Data Recovery] A [backup](#) in which all of a defined set of data objects are copied, regardless of whether they have been modified since the last backup.

A full backup is the basis from which incremental backups are taken. See [cumulative incremental backup](#), [differential incremental backup](#).

full duplex

[Data Communication] Concurrent transmission and reception of data on a single link.

full volume transfer rate

[Storage System] The average rate at which a single disk transfers a large amount of data (e.g., more than one cylinder) in response to one [I/O request](#).

The full-volume [data transfer rate](#) accounts for any delays (e.g., due to inter-[sector](#) gaps, inter-track switching time and seeks between adjacent cylinders) that may occur during the course of a large data transfer. Full volume transfer rate may differ depending on whether data is being read or written. If this is true, it is appropriate to speak of full-volume read rate or full-volume write rate. Also known as [spiral data transfer rate](#).

Fx_Port

[Fibre Channel] A [Switch](#) Port capable of operating as an [F_Port](#) or [FL_Port](#).

G

G_Port

[Fibre Channel] A “Generic” Fabric Port, that can operate as either an [E_Port](#) or an [F_Port](#).

A G_Port can determine the operating mode at [switch](#) port [initialization](#), F_Port when an [N_Port](#) attachment is determined, E_Port when an E_Port attachment is determined.

G

garbage collection

[Computer System] The process of reclaiming resources that are no longer in use.

Garbage collection has uses in many aspects of computing and storage. For example, in flash storage, background garbage collection can improve write performance by reducing the need to perform whole block erasures prior to a write. See also [trim](#).

gateway

[Network] A device that receives data via one [protocol](#) and transmits it via another.

Gb

Gbit

[General] Shorthand for [Gigabit](#).

GB**GByte**

[General] Shorthand for [Gigabyte](#).

GB/W

[General] Short for [Gigabytes](#) gigabytes per watt.

GB/W is a metric for evaluating the storage capacity provided per unit of power.

GBE

[Network] Shorthand for [Gigabit Ethernet](#).

GBIC

[Fibre Channel] Acronym for [Gigabit Interface Converter](#).

Gbps/W

[General] Short for [Gigabits](#) per second per watt.

Gbps/W is a metric for evaluating bandwidth provided per unit of power.

geometry (of a disk)

[Storage System] The mathematical description of the layout of blocks on a disk.

The primary aspects of a disk's geometry are the number of recording bands and the number of tracks and blocks per track in each, the number of data tracks per cylinder, and the number and layout of [spare](#) blocks [reserved](#) to compensate for [media](#) defects.

Gibit

[General] Shorthand for [Gibibit](#).

GiB**GiByte**

[General] Shorthand for [Gibibyte](#).

GiB/W

[General] Short for Gibibytes per watt.

GiB/W measures capacity in units of 230 bytes/watt, while GB/W uses units of 109 bytes/watt.

Gibibit (Gibit)

[General] Shorthand for 1,073,741,824 (2^{30}) bits.

Binary notation is most commonly used for semiconductor memory sizes.

See also [Gigabit](#).

Gibibyte (GiB)

[General] Shorthand for 1,073,741,824 (2^{30}) bytes.

Binary notation is most commonly used for semiconductor memory sizes.

See also [Gigabyte](#).

Gibps/W

[General] Short for [Gibibits](#) per second per watt.

Gibps/W measures bandwidth in units of 230 bits/watt, in contrast to Gbps/W, which measures it in units of 109 bits/watt.

GID

[Management] [Data Security] Abbreviation for "[group identifier](#)" (Group Identifier).

Gigabit (Gb)

[General] Shorthand for 1,000,000,000 (10^9) bits.

The SNIA uses the base 10 convention commonly found in I/O-related and scientific literature rather than the base 2 convention (1,073,741,824, i.e., 2^{30}) common in computer system and software literature.

For [Fibre Channel](#), this refers to a bit transmission rate of 1,062,500,000 bits per second.

See also [Gibibit](#).

Gigabit Ethernet (GBE)

[Network] A group of [Ethernet](#) standards in which data is transmitted at 1 [Gbit](#) per second, using a 1250 [Megabaud](#) line rate and an adaptation of the [Fibre Channel](#) Physical Layer [8b/10b encoding](#).

GBE standards are handled by IEEE 802.3.

Gigabit Interface Converter (GBIC)

[Fibre Channel] A [transceiver](#) that converts between electrical signals internal to a [Fibre Channel](#) or [Ethernet](#) device and the external optical or electrical interface of that device.

These devices are obsolete and have been replaced by smaller, cheaper, and faster devices, including SFP, SFP+, XFP and related XAUI-based modules.

Gigabyte (GB)

[General] Shorthand for 1,000,000,000 (10^9) bytes.

The SNIA uses the base 10 convention commonly found in I/O-related and scientific literature rather than the base 2 convention (1,073,741,824, i.e., 2^{30}) common in computer system and software literature.

See also [Gibibyte](#).

Gigabyte System Network (GSN)

1. [Network] A common name for the [HIPPI-6400](#) standard for 800 [MByte](#) per second links.
2. [Network] A network of devices that implement the HIPPI-6400 standard.

GL_Port

[Fibre Channel] A "Generic Loop" Port, able to operate as an [E_Port](#), [F_Port](#) or [FL_Port](#).

A GL_Port can determine operating mode at [switch](#) port [initialization](#), FL_Port when an [NL_Port](#) attachment is determined, F_Port when an [N_Port](#) attachment is determined, E_Port when an E_Port attachment is determined.

GLM

[Fibre Channel] Acronym for Gigabaud Link Module.

Graphical User Interface (GUI)

[Computer System] A form of user interface to intelligent devices characterized by pictorial displays and highly structured, forms oriented input.

A GUI is valued for perceived ease of use compared with a [command line interface](#).

Green Storage Initiative (GSI)

[Standards] [Energy] An initiative within the SNIA with a special interest in marketing, education, promotion and development of green storage technologies and support for the technical work of the Green Storage [TWG](#).

greenwashing

[Energy] A result of excessive marketing and ineffective engineering.

In fond memory of Tom Clark, who penned this definition ca. 2008.

G

Group Identifier (GID)

[Data Security] A collection of computer user identifiers and possibly other group identifiers used as a convenience in assigning resource access rights or [operational](#) privileges.

groupid

[Data Security] Shorthand for [group identifier](#).

GSI

[Standards] Acronym for the SNIA [Green Storage Initiative](#).

GSN

[Network] Acronym for [Gigabyte System Network](#).

GUI

[Computer System] Acronym for [Graphical User Interface](#).

H

hacker

[Data Security] An unauthorized user who attempts to gain and/or succeeds in gaining access to an [information system](#).

halt

[Computer System] To stop all activity in a computer system in an orderly manner.

hard link

[File System] A path that provides a different name for a file.

Hard links are independent references to the same file; the file content is not deleted until every hard link to the file is deleted.

hard zone

[Fibre Channel] A [zone](#) consisting of zone members that are permitted to communicate with one another via the fabric.

Hard zones are enforced by fabric switches that prohibit communication among members not in the same zone on a [frame](#) by frame basis, based on the source and destination [addressing](#). Well-known addresses are implicitly included in every zone.

H

hash value

[Data Management] A value deterministically derived from data and assumed to be unique enough within the [domain](#) of that data for the purposes of its application.

hash-based data deduplication

[Storage System] A method of performing [data deduplication](#) by calculating and comparing hash values.

See [delta-based data deduplication](#).

Hashed Message Authentication Code (HMAC)

[Data Security] A value calculated over the contents of a message (usually using a cryptographic hash algorithm) that can be used to demonstrate that the contents of the message have not been changed during transmission.

HBA

[Computer System] Acronym for [Host Bus Adapter](#).

heuristic

[General] An approximation for a calculation that is too expensive to perform in its entirety.

Hierarchical Storage Management (HSM)

[Data Management] The automated [migration](#) of data objects among storage devices, usually based on inactivity.

Hierarchical storage management is based on the concept of a cost-performance storage hierarchy. By accepting lower access performance (higher access times), one can store objects less expensively. By automatically moving less frequently accessed objects to lower levels in the hierarchy, higher cost storage is freed for more active objects, and a better overall cost to performance ratio is achieved.

High Availability (HA)

[Computer System] The ability of a system to perform its function continuously (without interruption) for a significantly

longer period of time than the reliabilities of its individual components would suggest.

High [availability](#) is most often achieved through [failure tolerance](#). High availability is not an easily quantifiable term. Both the bounds of a system that is called highly available and the degree to which its availability is extraordinary must be clearly understood on a case-by-case basis.

High Performance Parallel Interface (HIPPI)

[Network] [Standards] An [ANSI](#) standard for an 800 [Mbit](#)/second I/O interface primarily used in supercomputer networks.

The subsequent 6400 Mbit per second I/O interface standard, HIPPI-6400, is more commonly referred to as the [Gigabyte System Network](#) (GSN) standard.

high speed serial direct connect

[Fibre Channel] A form factor that allows quick connect/disconnect for [Fibre Channel](#) copper interfaces.

HIPPI

[Network] [Standards] Acronym for [High Performance Parallel Interface](#).

HMAC

[Data Security] Acronym for [Hashed Message Authentication Code](#).

host

[Computer System] A [host computer](#).

host adapter

[Computer System] Synonym for [host bus adapter](#).

host based array

host based disk array

[Storage System] A [disk array](#) whose [control software](#) executes in one or more host computers rather than in a disk [controller](#).

The [member](#) disks of a host-based array may be part of different disk subsystems. See [controller based array](#).

host based virtualization

[Computer System] [Virtualization](#) implemented in a [host computer](#).

host bus

[Computer System] Synonym for [host I/O interconnect](#).

Host Bus Adapter (HBA)

[Computer System] An [I/O adapter](#) that connects a [host computer](#) bus to an [I/O interconnect](#).

Adapter is the preferred term for [Fibre Channel](#) and [SCSI](#) interconnects. The term [NIC](#) is used for networking interconnects such as [Ethernet](#) and [token ring](#).

host cache

[Storage System] A [cache](#) that resides within a [host computer](#) whose primary purpose is to improve disk or [array](#) I/O performance.

Host cache may be associated with a [file system](#) or database, in which case, the data items stored in the cache are file or database entities. Alternatively, host cache may be associated with the device [driver](#) stack, in which case the cached data items are sequences of disk blocks. See [cache](#), [controller cache](#), [disk cache](#).

host computer

[Computer System] Any computer system to which disks, disk subsystems, or file servers are attached and accessible for data storage and I/O.

Mainframes, servers, workstations and personal computers, as well as multiprocessors and clustered computer complexes, are all referred to as host computers in SNIA publications.

host environment

[Computer System] A [storage subsystem](#)'s [host computer](#) or host computers, inclusive of operating system and other required software instance(s).

The term *host environment* is used in preference to host computer to emphasize that multiple host computers are being discussed, or to emphasize the importance of the operating system or other software in the discussion.

host I/O interconnect

[Computer System] An I/O interconnect used to connect a [host computer](#)'s [host bus adapter](#) to storage subsystems or storage devices.

See [I/O interconnect](#), [channel](#).

host-side data deduplication

[Capacity Optimization] Deprecated synonym for source [data deduplication](#).

hot aisle/cold aisle

[Energy] Arranging IT equipment in racks such that heat is exhausted in designated aisles while cool air is supplied in the alternating aisles.

hot backup

[Data Recovery] Synonym for [online backup](#).

See [cold backup](#), [offline backup](#).

hot banding

[Storage] Inserting ranges of addresses that are accessed with greater frequency into a synthetically generated workload.

Hot banding is intended to reward caching behavior on the part of the storage system being measured.

hot disk

[Storage System] A disk whose capacity to execute I/O requests is saturated by the aggregate [I/O load](#) directed to it from one or more applications.

hot file

[File System] A frequently accessed file.

Hot files are generally the root cause of hot disks, although this is not always the case. A [hot disk](#) can also be caused by [operating environment](#) I/O, such as paging or swapping.

hot spare (disk)

[Storage System] A disk being used as a [hot standby](#) component.

hot standby (component, controller)

[Computer System] A [redundant](#) component in a failure tolerant subsystem that is powered and ready to operate, but that does not operate as long as all of its [target](#) primary components are functioning.

Hot standby components increase [storage subsystem availability](#) by allowing systems to continue to function when a component such as a [controller](#) fails. When the term *hot standby* is used to denote a disk, it specifically means a disk that is spinning and ready to be written to, for example, as the target of a [rebuilding](#) operation.

hot swap

[Computer System] The [substitution](#) of a [replacement unit](#) (RU) in a system for a defective unit, where the substitution can be performed while the system is performing its normal functioning normally.

Hot swaps are physical operations typically performed by humans. See [automatic swap](#), [cold swap](#), [warm swap](#).

hot swap adapter

[Computer System] An [adapter](#) that can be hot swapped into or out of an [intelligent device](#).

Some adapters that are called hot swap adapters should more properly be termed [warm swap adapters](#), because the function they perform is interrupted while the [substitution](#) occurs.

Houlderize

[General] The term used to describe flip/flopping; when an opinion continually switches back and forth between two or more choices.

For example: Design choice "A" is selected; but a week later, design choice "B" is selected; then after another week of consideration, the design choice is switched back to "A".

HSM

[Data Recovery] Acronym for [Hierarchical Storage Management](#).

HSSDC

[Fibre Channel] Acronym for [High Speed Serial Direct Connect](#).

HTML

[Standards] Acronym for [HyperText Markup Language](#).

HTTP

[Standards] Acronym for [HyperText Transfer Protocol](#).

hub

[Network] A communications infrastructure element to which nodes on a multi-point bus or loop are physically connected.

Commonly used in [Ethernet](#) and [Fibre Channel](#) networks to improve the manageability of connecting devices to a bus structure, both managing physical cables and supporting the addition or removal of nodes from the bus while it is operating. Hubs maintain the logical loop [topology](#) of the network of which they are a part, while creating a "hub and spoke" physical [star](#) layout. Unlike switches, hubs do not aggregate [bandwidth](#).

hub port

[Fibre Channel] A port on a [Fibre Channel hub](#) whose function is to pass data transmitted on the physical loop to the next port on the hub.

Hub ports include loop healing port bypass functions. Some hubs have additional management functionality. There is no definition of a hub port in any Fibre Channel standard.

H

hybrid array

[Storage System] A storage [array](#) consisting of multiple types of storage devices.

hybrid cloud

[Cloud] A composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability.

Hybrid DIMM

[Hardware] A [dual in-line memory module](#) that contains multiple types of [volatile](#) and non-volatile memory technologies.

hybrid drive

[Storage System] A [disk drive](#) that consists of multiple types of storage media.

hyper-converged storage system

[Storage System] A storage product that combines server, client, storage, network, and management software oriented towards storage in a single unit.

HyperText Markup Language (HTML)

[Standards] A computer language consisting of a set of tags or "markup" codes that describe how a document is displayed by a web browser.

HTML tags are delimited by the characters "<" and ">". For example, the markup code "<p>" indicates that a new paragraph is beginning, while "</p>" indicates that the current paragraph is ending.

HyperText Transfer Protocol (HTTP)

[Standards] An application level [protocol](#), usually run over [TCP/IP](#), that enables the [exchange](#) of files via the World Wide Web.

I

I_T nexus

[SCSI] A relationship specified in [SAM-2](#) between a [SCSI Initiator Port](#) and a [SCSI Target Port](#).

IaaS

[Services] Acronym for [Infrastructure as a Service](#).

ICMP

[Network] Acronym for [Internet Control Message Protocol](#).

IDE

[Storage System] Acronym for [Integrated Drive Electronics](#).

idempotency

[General] A property of an operation in which the same result is obtained no matter how many times the operation is performed.

In an environment with a single writer, writing a [block](#) of data to a disk is an idempotent operation, whereas writing a block of data to a tape is not, because writing a block of data twice to the same tape results in two adjacent copies of the block.

identification

[Data Security] The process of determining the unique [identity](#) of an entity.

I

identity

[Data Security] Representation of an actual user (or application or service or device).

An example is the assignment of the user name joej (the identity) to represent the human user Joe Jones for purposes of [authentication](#) and [authorization](#).

idle

[Storage System] A state in which a storage system is serving no user-initiated I/O requests, but is ready to service them upon arrival with normal [latency](#).

Storage systems may perform extensive system-initiated I/O during idle periods as they execute routine background housekeeping tasks.

idle power

[Energy] The power consumption of a system when powered on but with no active workload.

Idle word

[Fibre Channel] In a data stream using 8B10B [encoding](#), an [ordered set](#) of four transmission characters normally transmitted between frames to indicate that a [fibre channel](#) network is [idle](#).

IDS

[Data Security] Acronym for [Intrusion Detection System](#).

IETF

[Network] [Standards] Acronym for [Internet Engineering Task Force](#).

iFCP

[Storage System] A gateway-to-gateway [protocol](#) that provides [fibre channel](#) fabric services to fibre channel devices over a [TCP/IP](#) network.

ignored (field)

[Fibre Channel] A field that is not interpreted by its [receiver](#).

IKE

[Network] [Data Security] Acronym for [Internet Key Exchange](#).

IMA

[iSCSI] Acronym for [iSCSI Management API](#).

ILM

[Data Management] Acronym for [Information Lifecycle Management](#).

implicit addressing

[Storage System] A form of [addressing](#) usually used with tapes in which the data's address is inferred from the form of the access request.

Tape commands that do not include an explicit [block](#) address but implicitly specify the *next* or *previous* block from the current tape position, from which the block address must be inferred by the device. See [explicit addressing](#).

import/export element

[SCSI] Synonym for [entry/exit slot](#).

IMR

[Data Recovery] Acronym for [Incremental Mirror Resynchronization](#).

in-band (transmission)

[Network] [Fibre Channel] Transmission of a separate data stream, such as management information, over the same [medium](#) as the primary data stream.

See [out-of-band](#).

in-band data deduplication

[Storage System] Deprecated synonym for [inline data deduplication](#).

in-band virtualization

[Computer System] [Virtualization](#) functions or services that are in the data path.

In a system that implements [in-band](#) virtualization, virtualization services such as address [mapping](#) are performed by the same functional components used to read or write data. See [out-of-band virtualization](#)

incident

[Data Security] An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. [NIST FIPS 200]

incineration

[Data Security] A method of sanitization that reduces a storage device or element to ash, in an approved facility. [ISO/IEC 27040]

INCITS

[Standards] Shorthand for International Committee for [Information Technology](#) Standards.

INCITS is one of about 100 standards organizations accredited by ANSI to prepare national standards and make recommendations to ANSI concerning international standards. INCITS assigns technical committees to prepare standards associated with information technology, including JPEG, [computer security](#), biometric information, [SCSI](#) (Technical Committee [T10](#)), [Fibre Channel](#) (Technical Committee [T11](#)), and many more.

INCITS T10

[SCSI] [Standards] The [INCITS SCSI](#) Storage Interfaces Technical Committee (INCITS TC T10).

The INCITS T10 Technical Committee is the standards development committee accredited by INCITS to develop SCSI standards for communication between host devices (initiators) to [storage device](#) controllers (targets).

INCITS T11

[Fibre Channel] [Standards] The [INCITS Fibre Channel Interfaces Technical Committee](#) (INCITS TC T11).

The INCITS T11 Technical Committee is the standards development committee accredited by INCITS to develop standards related to Fibre Channel, related [serial](#) storage interfaces, and certain storage management interfaces.

incremental backup

[Data Recovery] Any [backup](#) in which only data objects modified since the time of some previous backup are copied.

Incremental backup is a collective term for cumulative incremental backups and [differential](#) incremental backups. See [cumulative incremental backup](#), [differential incremental backup](#), [full backup](#).

incremental mirror resynchronization

incremental resynchronization

[Data Recovery] A technique for reducing the time required to [synchronize](#) a split [mirror](#) with the set of storage devices from which it was split.

Incremental [mirror resynchronization](#) requires that a list of changes to the original set of data since moment of splitting be kept. When the split mirror is rejoined to its original set of volumes, only the data items identified in the list are copied from the original to the split mirror (rather than the entire contents of the devices).

independent access array

[Storage System] A [disk array](#) whose data [mapping](#) is such that different [member](#) disks can execute multiple application I/O requests concurrently.

See [parallel access array](#).

InfiniBand

[Computer System] A interconnect between computer system(s) and computer system component(s).

This includes computer system to computer system connectivity and computer system component to computer system component connectivity.

infinite buffer

[Fibre Channel] A term indicating that at the [FC-2](#) level, the amount of buffering available at the [Sequence Recipient](#) is assumed to be unlimited.

Buffer overrun must be prevented by each [ULP](#) by choosing an appropriate amount of buffering per sequence based on its [maximum transfer unit](#) size.

information

[Data Management] Data that is interpreted within a context such as an application or a process.

information assurance

[Data Security] Measures that protect and defend information and information systems by ensuring their [availability](#), [integrity](#), [authentication](#), [confidentiality](#), and [nonrepudiation](#).

Information [assurance](#) encompasses system reliability and strategic [risk management](#), and includes providing for [restoration](#) of information systems using protection, detection, and reaction capabilities.

information category

[Fibre Channel] A [frame](#) header field indicating the category to which the frame [payload](#) belongs (e.g., [Solicited Data](#), [Unsolicited Data](#), [Solicited Control](#) and [Unsolicited Control](#)).

Information Lifecycle Management (ILM)

[Data Management] The policies, processes, practices, services and tools used to align the business value of information with the

most appropriate and cost-effective infrastructure from the time information is created through its final disposition.

Information is aligned with business requirements through management policies and service levels associated with applications, [metadata](#) and data.

information management

[Data Management] The discipline and function of oversight and control of information resources.

information management services

[Data Management] The processes associated with managing information as it progresses through various lifecycle states associated with a Business Process.

These services [exploit](#) information about data content and relationships in making decisions. Examples include records management and content management applications.

information model

[Data Management] A repository-independent definition of entities (i.e., objects) and the relationships and interactions between these entities.

The [CIM](#) schemas are an example of an information model. An information model differs from a [data model](#), which is repository-specific.

I

information resource domain

[Management] The category of resources that exclusively encompass information services.

information security

[Data Security] [Preservation](#) of the [confidentiality](#), [integrity](#) and [availability](#) of information.

[ISO/IEC 27000]

information service

[Management] A set of functions that treat data within an interpretation context.

information system

[Data Security] The entire infrastructure, organization, personnel and components for the collection, processing, storage, transmission, display, dissemination and disposition of information.

Information Technology (IT)

[General] All aspects of information creation, access, use, storage, transport and management.

The term *Information Technology* addresses all aspects of computer and storage systems, networks, users and software in an enterprise.

Information Unit (IU)

1. [Fibre Channel] An related collection of data specified by [FC-4](#) to be transferred as a single [FC-2 sequence](#).
2. [SCSI] A delimited and sequenced set of information in a format appropriate for transport by the service delivery subsystem.

A [SCSI](#) IU may contain a command, data, response, or task management request.

infrastructure-based virtualization

[Computer System] [Virtualization](#) implemented in the storage fabric, in separate devices designed for the purpose, or in network devices.

Examples are separate devices or additional functions in existing devices that aggregate multiple individual [file system](#) appliances or [block](#) storage subsystems into one such virtual service, functions providing transparent block or file system [mirroring](#) functions, or functions that provide new security or management services.

Infrastructure as a Service (IaaS)

[Services] Delivery over a network of an appropriately configured virtual computing environment, based on a request for a given service level.

Typically, IaaS is either self-provisioned or provisionless and is billed based on consumption.

ingress Routing Function role

[Fibre Channel] A process within a [Routing Function](#) that translates the [D_ID](#), translates embedded N_Port_IDs and stores the [Exchange](#) context if needed, adds the IFR_Header and [Enc_Header](#) if needed, and then forwards the [frame](#) to the next hop Routing Function or [Egress Routing Function](#).

inherent cost

[Computer System] The cost of a system expressed in terms of the number and type of components it contains.

The concept of inherent cost allows technology-based comparisons of [disk subsystem](#) alternatives by expressing cost in terms of number of disks, ports, modules, fans, power supplies, cabinets, etc. Because it is inexpensively reproducible, software is generally assumed to have negligible inherent cost.

initial relative offset

[Fibre Channel] The [relative offset](#) of the [block](#) or sub-block transmitted by the first [frame](#) in a [sequence](#), specified by an [upper layer protocol](#).

The initial relative offset need not be zero.

initialization

1. [Fibre Channel] The startup and initial [configuration](#) of a device, element, system, piece of software or network.
2. [Fibre Channel] For [FC-1](#), the period beginning with power on and continuing until the [transmitter](#) and [receiver](#) at that level become [operational](#).

initiator

1. [Computer System] The system component that originates an I/O command over an [I/O interconnect](#).
2. [SCSI] The endpoint that originates a [SCSI](#) I/O command [sequence](#).

I/O adapters, network interface cards, and intelligent I/O interconnect control ASICs are typical initiators. See [LUN](#), [originator](#), [target](#), [target port identifier](#).

initiator NVMe_Port

[Fibre Channel] [NVMe_Port](#) which is the NVM host port for an NVMeoFC association.

initiator port identifier

[SCSI] The [interconnect](#) address of an [initiator](#).

Initiator Session Identifier (ISID)

[iSCSI] The unique identifier that an [initiator](#) assigns to its end point of the session.

When combined with the [iSCSI Initiator Name](#), the Initiator Session Identifier provides a worldwide unique name for its [SCSI Initiator Port](#).

inline data deduplication

[Storage System] [Data deduplication](#) performed before writing the deduplicated data.

See [post-process data deduplication](#)

inode

[File System] A persistent data structure in a UNIX or UNIX-like [file system](#) that describes the location of some or all of the disk blocks allocated to the file.

instantiation

[General] The creation of an instance of a class or [object oriented](#) abstraction.

Integrated Drive Electronics (IDE)

[Computer System] A type of hardware interface widely used to connect hard disks, CD-ROMs and tape drives to a PC, but also used in other systems.

The IDE interface is officially known as the [ATA](#) specification.

integrity

[Data Security] Property of protecting the accuracy and completeness of assets.

[ISO/IEC 27000]

intelligent controller

[Storage System] Synonym for [storage controller](#).

intelligent device

[Computer System] A computer, [storage controller](#), [storage device](#), or [appliance](#).

Intelligent Peripheral Interface (IPI)

[Network] A high-performance standards-based [I/O interconnect](#).

Inter-Fabric

[Fibre Channel] The entire interconnection of Fabrics and Inter-Fabric Routers.

Inter-Fabric Router

[Fibre Channel] A device that performs [Inter-Fabric Routing](#) and consists of a [Routing Function](#), [Translate Domain](#) switches, and [Front Domain](#) switches.

Inter-Fabric Routing

[Fibre Channel] The process of forwarding frames through a specific [Routing Function](#), including the translation of [N_Port](#) IDs.

interconnect

[Computer System] A physical facility by which system elements and devices are connected together and through which they can communicate with each other.

I/O buses and networks are both interconnects.

interface connector

[Fibre Channel] An optical or electrical connector that connects the [media](#) to the [Fibre Channel transmitter](#) or [receiver](#).

An interface connector consists of both a [receptacle](#) and a plug.

Intermediate Routing Function

[Fibre Channel] A process within a [Routing Function](#) that validates the [frame](#) headers, updates the IFR_Header, removes and adds a new [Enc_Header](#), then forwards the frame to the next hop Routing Function.

intermix

[Fibre Channel] A [Fibre Channel class of service](#) that provides a full [bandwidth](#) dedicated [Class 1 connection](#), but allows connectionless [Class 2](#) and [Class 3](#) traffic to share the link during intervals when bandwidth is unused.

International Organization for Standardization (ISO)

[Standards] A worldwide federation of national standards bodies from more than 145 countries; a non-governmental organization whose work results in international agreements that are published as International Standards and other types of ISO documents.

Internet Control Message Protocol (ICMP)

[Network] A control [protocol](#) strongly related to [IP](#) and [TCP](#), and used to convey a variety of control and error indications.

Internet Engineering Task Force (IETF)

[Network] [Data Security] [Standards] A large open international community of network designers, operators, vendors, and researchers concerned with evolution and smooth operation of the Internet.

The IETF is the standards body responsible for Internet standards called RFCs, including [SNMP](#), [TCP/IP](#) and [policy](#) for [QoS](#). The IETF has a web site at www.ietf.org.

Internet Key Exchange (IKE)

[Network] [Data Security] A [protocol](#) specified by the IETF that performs mutual authentication between two parties and establishes an IKE Security Association (SA) that includes shared secret information that can be used to efficiently establish SAs for Encapsulating Security Payload (ESP) or Authentication Header (AH) and a set of [cryptographic algorithms](#) to be used by the SAs to protect the traffic that they carry.

IKEv2 is defined in RFC-4306.

IKE Version 2 (IKEv2) is not compatible with Version 1.

Internet Protocol (IP)

[Network] A [protocol](#) that provides connectionless [best effort](#) delivery of datagrams across heterogeneous physical networks.

See [TCP](#), [UDP](#).

Internet Small Computer Systems Interface (iSCSI)

[Storage System] A transport [protocol](#) that provides for the [SCSI](#) protocol to be carried over a [TCP](#) based [IP](#) network, standardized by the [Internet Engineering Task Force](#) and described in [RFC 3720](#).

Internet Storage Name Service (iSNS)

[iSCSI] A [protocol](#) and mechanism for intelligent discovery of storage devices in an [IP](#) network.

interoperability

[Computer System] The ability of systems to work with or use data and protocols from other systems.

interrupt

[Computer System] A hardware or software signal that causes a computer to stop executing its instruction stream and [switch](#) to another stream.

Software interrupts are triggered by application or other programs. Hardware interrupts are caused by external events, to notify software so it can deal with the events. The ticking of a clock, completion or reception of a transmission on an [I/O interconnect](#) or network, application attempts to execute invalid instructions or [reference data](#) for which they do not have access rights, and failure of some aspect of the computer hardware itself are all common causes of hardware interrupts.

interrupt switch

[Computer System] A human-activated [switch](#) present on some intelligent devices that is used to generate interrupts.

Interrupt switches are usually used for debugging purposes.

intracabinet specification

[Fibre Channel] A [Fibre Channel](#) specification for copper cabling that allows up to 13m total cable length within a single enclosure, which may contain multiple devices.

intrusion

[Data Security] A deliberate or accidental set of events that potentially causes unauthorized access to, activity against, and/or activity in, an [information technology](#) (IT) system.

intrusion detection

[Data Security] The process of identifying that an [intrusion](#) has been attempted, is occurring, or has occurred.

Intrusion Detection System (IDS)

[Data Security] A technical system that is used to identify and respond to intrusions in IT systems.

I/O

[Computer System] Shorthand for input/output.

I/O is the process of moving data between a computer system's main memory and an external device or interface such as a [storage device](#), display, printer, or network connected to other computer systems. This encompasses *reading*, or moving data into a computer system's memory, and *writing*, or moving data from a computer system's memory to another location.

I/O adapter

[Computer System] An [adapter](#) that converts between the timing and [protocol](#) requirements of a system's memory bus and those of an [I/O interconnect](#) or network.

In the context of storage subsystems, I/O adapters are contrasted with embedded storage controllers, that not only adapt between buses and interconnects, but also perform transformations such as device fan-out, data caching, and [RAID](#). [host bus adapters](#) (HBAs) and [Ethernet](#) NICs are types of I/O adapters.

I/O bottleneck

[Computer System] Any resource in the I/O path (e.g., device [driver](#), [host bus adapter](#), [I/O interconnect](#), [intelligent controller](#), or disk) whose performance limits the performance of a [storage subsystem](#) as a whole.

I/O bus

[Computer System] Synonym for [I/O interconnect](#).

I/O device

[Computer System] Synonym for [I/O adapter](#).

I/O driver

[Computer System] A [host computer](#) software component (usually part of an operating system) whose function is to control the operation of peripheral controllers or adapters attached to the host computer.

I/O drivers manage communication and data transfer between applications and I/O devices, using [host bus adapters](#) as agents. In some cases, drivers participate in data transfer, although this is rare with disk and tape drivers, since most host bus adapters and controllers contain specialized hardware to perform data transfers.

I/O intensity

[Computer System] A characterization of applications that describes how strongly their performance depends on the performance of the [I/O subsystem](#) that provides their I/O services.

I/O intensive applications may be either data transfer intensive or I/O [request intensive](#) or both.

I/O interconnect

[Computer System] Any path used to transfer data and control information between components of an [I/O subsystem](#).

An I/O [interconnect](#) consists of wiring (either cable or backplane), connectors, and all associated electrical drivers, receivers, transducers, and other required electronic

components. I/O interconnects are typically optimized for the transfer of data, and tend to support more restricted configurations than networks. See [channel](#), [device channel](#), [network](#).

I/O load

[Computer System] A [sequence](#) of I/O requests made to an [I/O subsystem](#).

The requests that comprise an I/O load include both user I/O and host overhead I/O, such as swapping, paging, and [file system](#) activity.

I/O load balancing

[Computer System] Synonym for [load balancing](#).

I/O operation

[Computer System] A read, write, or control function performed to, from or within a computer system.

See [I/O request](#).

I/O power efficiency

1. [Storage System] The ratio of maximum [IOPS](#) deliverable by a system, to the input power required to deliver those IOPS.
2. [Storage System] The ratio of maximum [bandwidth](#) readable or writable by a system, to the input power required to achieve that bandwidth.

I/O request

[Computer System] A request by an application to read or write a specified amount of data.

In the context of real and virtual disks, I/O requests specify the transfer of a number of blocks of data between consecutive [disk block](#) addresses and contiguous memory locations. See [I/O operation](#).

I/O subsystem

[Computer System] A collective term for the set of devices and software components that operate together to provide data transfer services.

A [storage subsystem](#) is one type of I/O subsystem.

IOPS

IOPs

iops

[Storage System] Shorthand for [I/O Operations](#) per second.

IOPs can also be the plural of *IOP* (short for I/O operation), depending on context.

IOPS/W

[Energy] Input/Output Operations per Second per Watt.

IOPS/W is a metric for evaluating storage I/O performance per unit of power.

IP

[Network] Acronym for [Internet Protocol](#).

IP SAN

[iSCSI] [Block](#)-level Storage Area Networks over [TCP/IP](#) using the [iSCSI protocol](#).

IP Security (IPsec)

[Network] [Data Security] A suite of cryptographic algorithms, protocols and procedures used to protect information, authenticate communications, control access, and provide non-[repudiation](#) at the [IP](#) layer.

The two key protocols in IPsec are the [Authentication Header](#) (AH) and [Encapsulating Security Payload](#) (ESP) protocols.

IP Storage

[iSCSI] [Storage Networking](#) over [TCP/IP](#) networks.

IP Storage includes [block](#)-level [SAN](#) solutions using [iSCSI](#), [iFCP](#) and FCIP protocols as well as file-level [NAS](#) solutions using protocols such as [CIFS](#) and [NFS](#).

IPI

[Computer System] Acronym for [Intelligent Peripheral Interface](#).

IPsec

[Network] [Data Security] Shorthand for [IP Security](#).

iSCSI

[Storage System] Acronym for [Internet Small Computer Systems Interface](#).

iSCSI device

[iSCSI] A [SCSI Device](#) using an [iSCSI](#) service delivery subsystem, in other words an iSCSI-specific transport mechanism for SCSI commands and responses (information units).

iSCSI initiator name

[iSCSI] The worldwide unique name of an [iSCSI initiator](#).

iSCSI initiator node

[iSCSI] Another name for the [iSCSI initiator](#); an [iSCSI Node](#) within the iSCSI [Client](#) Network Entity.

iSCSI initiator port

[iSCSI] Another name for a [SCSI Initiator Port](#) used for [iSCSI](#).

iSCSI layer

[iSCSI] The layer that builds/receives [iSCSI](#) PDUs and relays/receives them to/from one or more [TCP](#) connections that form an [iSCSI session](#).

iSCSI Management API (IMA)

[iSCSI] A specification for a C language based [API](#) for managing [iSCSI](#) capable HBAs and NICs, along with the device drivers that control them.

iSCSI name

[iSCSI] The name of an [iSCSI initiator](#) or iSCSI [target](#).

iSCSI network entity

[iSCSI] A device or gateway that is accessible from the [IP](#) network and has one or more [iSCSI](#) Network Portals.

iSCSI Network Portal

[iSCSI] A component of an [iSCSI Network Entity](#) that has a [TCP/IP](#) address and can be used by a [node](#) within that entity for connections to another [iSCSI node](#).

An [Initiator](#) iSCSI Network Portal is identified by its IP address. A [target](#) iSCSI Network Portal is identified by its IP address and listening TCP port.

iSCSI Node

[iSCSI] A single [iSCSI initiator](#) or iSCSI [target](#).

iSCSI Portal Group

[iSCSI] A set of [iSCSI](#) Network Portals within an [iSCSI Node](#).

When a session has multiple connections, all connections in a session must use the portals in a single iSCSI Portal Group.

iSCSI Portal Group Tag

[iSCSI] A tag identifying all portals in an [iSCSI Portal Group](#) within an [iSCSI Node](#).

All portals in the group have the same iSCSI Portal Group Tag.

iSCSI SAN

[iSCSI] [Block](#)-level Storage Area Networks over [TCP/IP](#) using the [iSCSI protocol](#).

iSCSI Session

[iSCSI] The top level relationship between a specific [initiator](#) and [target](#), equivalent to the [I_T nexus](#).

A session can contain one or more connections.

iSCSI Session Identifier (ISID)

[iSCSI] A unique identifier for a session between an [iSCSI initiator](#) and [target](#).

iSCSI Target Name

[iSCSI] The worldwide unique name of an [iSCSI target](#).

iSCSI Target Node

[iSCSI] Another name for the [iSCSI target](#), i.e., an [iSCSI Node](#) within the iSCSI [Server](#) Network Entity.

iSCSI Target Port

[iSCSI] Another name for a [SCSI Target Port](#) used for [iSCSI](#).

ISID

[iSCSI] Acronym for [Initiator Session Identifier](#).

iSNS

[iSCSI] Acronym for [Internet Storage Name Service](#).

iSNS Discovery Domain

[iSNS] Grouping of storage nodes for facilitating discovery and login control of these nodes.

ISO

[Standards] Acronym for [International Organization for Standardization](#).

IT

[General] Acronym for [Information Technology](#).

IT security

[Data Security] All aspects related to defining, achieving, and maintaining confidentiality, integrity, availability, non-repudiation, accountability, authenticity, and reliability of information assets. [ISO/IEC 1335]

IU

[General] Shorthand for [Information Unit](#).

J

Java

[Computer System] An [object oriented](#) computer programming language that is similar to C++.

JBOD

[Storage System] Shorthand for Just a Bunch Of Disks.

Originally used to mean a collection of disks without the coordinated control provided by [control software](#); today the term JBOD most often refers to a cabinet of disks whether or not [RAID](#) functionality is present. See [disk array](#).

Jini

[Computer System] A [Java](#)-based architecture and supporting services for publishing and discovering devices and services on a network.

jitter

[Fibre Channel] Deviation in timing that a bit stream encounters as it traverses a physical [medium](#).

J

K

K28.5

[Fibre Channel] A special 10-bit [character](#) used to indicate the beginning of a [Fibre Channel](#) command.

Kb

Kbit

[General] Abbreviations for [Kilobit](#).

KB

KByte

[General] Abbreviations for [Kilobyte](#).

key

[Data Security] A [sequence](#) of bits used for cryptographic operations and/or for producing other keys.

The same [plaintext](#) encrypted with different keys yields different ciphertexts, each of which requires a different key for [decryption](#). In a [symmetric cryptosystem](#) the [encryption](#) and decryption keys are the same. In an [asymmetric cryptosystem](#) the encryption and decryption keys are different.

K

key backup

[Data Security] A process used in a cryptographic system that can restore access to data by providing for key deposit and [recovery](#).

Key [backup](#) is sometimes used as a replacement term for [key escrow](#), which has become encumbered with additional meanings.

key escrow

[Data Security] A process in which the storage of a cryptographic key is entrusted to a third party escrow [agent](#) who will disclose it only to the owner or another authorized user.

Key escrow systems are used to ensure that access to encrypted data can be restored in case of key loss due to error, disaster or a malicious act.

key exchange

[Data Security] A cryptographic [protocol](#) and procedure in which two communicating entities determine a shared key in a fashion such that a third party who reads all of their communication cannot effectively determine the value of the key.

A common approach to key [exchange](#) requires such a third party to compute a discrete logarithm over a large field in order to determine the key value, and relies for its security on the computational intractability of the discrete logarithm problem.

key management

[Data Security] The supervision and control of the process by which keys are generated, stored, protected, transferred, loaded, used, revoked and destroyed.

Key Management Interoperability Protocol (KMIP)

[Data Security] An [OASIS](#) standard that establishes a single, comprehensive [protocol](#) for communication between enterprise [key management](#) servers and cryptographic clients.

key pair

[Data Security] A [public key](#) and its corresponding [private key](#) as used in [public key cryptography](#) (i.e., asymmetric cryptosystems).

key recovery

[Data Security] A system characterized by the presence of some mechanism for obtaining exceptional access to a cryptographic key in case of loss by error, disaster, or malicious intent.

See also [key escrow](#).

key value storage

[Storage System] A type of object storage interface where a [key](#) is used to address the associated object.

key wrapping

[Data Security] A method of encrypting keys (along with associated integrity information) that provides both confidentiality and integrity protection using a symmetric [key](#).
[NIST SP 800-57 Part 1]

keying material

[Data Security] A key or [authentication](#) information in physical or magnetic form.

KiB**KiByte**

[General] Shorthand for [Kibibyte](#).

Kibibit (Kibit)

[General] Shorthand for 1,024 (2^{10}) bits.

Binary notation is most commonly used for semiconductor memory sizes.

See also [Kilobit](#).

K

Kibibyte (KiB)

[General] Shorthand for 1,024 (2^{10}) bytes.

Binary notation is most commonly used for semiconductor memory sizes.

See also [Kilobyte](#).

Kibit

[General] Shorthand for [Kibibit](#).

Kilobit (Kb)

[General] 1,000 (10^3) bytes.

The SNIA uses the base 10 convention commonly found in I/O-related and scientific literature rather than the base 2 convention (1,024, or 2^{10}) common in computer system and software literature.

See also [Kibibit](#).

Kilobyte (KB)

[General] 1,000 (10^3) bytes.

The SNIA uses the base 10 convention commonly found in I/O-related and scientific literature rather than the base 2 convention (1,024, or 2^{10}) common in computer system and software literature.

See also [Kibibyte](#).

KMIP

[Data Security] Acronym for [Key Management Interoperability Protocol](#).



L_Port

[Fibre Channel] An [FC_Port](#) that contains functions associated with the [Arbitrated Loop topology](#).

label

[Data Recovery] An identifier associated with a removable [media](#) or cartridge.

Labels may be humanly readable, machine readable, or both. See [external volume serial number](#), [media ID](#).

laboratory attack

[Data Security] Use of sophisticated signal recovery equipment in a laboratory environment to recover information from data storage media. [NIST SP 800-88]

Magnetic force microscopes and other similar equipment can be used to recover data from magnetic [media](#) that has been erased or damaged.

LAN

[Network] Acronym for [Local Area Network](#).

LANE

[Network] Acronym for [Local Area Network Emulation](#).



lane

[Fibre Channel] One of multiple point-to-point physical connections that make up a single link.

LAN-free backup

[Data Recovery] A [backup](#) methodology that moves data over a [SAN](#) without using [LAN](#) resources.

large read request**large write request****large I/O request**

[Storage System] An [I/O request](#) that specifies the transfer of a large amount of data.

'Large' depends on the context, but typically refers to requests for 64 KBytes or more of data. See [small I/O request](#).

laser

[Network] In the context of [serial](#) data communication networks, a solid-state element that emits light, usually in the near-infrared or infrared spectrum, modulated to carry binary information at very high data rates along an optical fiber.

The term *laser* was originally an acronym for "light amplification by stimulated emission of radiation."

latency

1. [Computer System] Synonym for [I/O request](#) execution time, the time between the making of an I/O request and completion of the request's execution.
2. [Computer System] Short for [rotational latency](#), the time between the completion of a seek and the instant of arrival of the first [block](#) of data to be transferred at the disk's [read/write head](#).

latent fault

[Computer System] A failure of a system component that has not been recognized because the failed aspect of the component has not been exercised since the occurrence of the failure.

A field-developed [media](#) defect on a disk surface is a latent fault until an attempt is made to read the data in a [block](#) that spans the defect.

LBA

[Storage System] Acronym for [Logical Block Address](#).

LC

[Network] An optical fiber connector complying with international standard IEC 61754-20:2002.

LC connectors are the most common connector in optical data communications networks, including [Ethernet](#) and [Fibre Channel](#). A dual LC connector is used, carrying separate fibers for transmitted and received data.

LDAP

[Network] Acronym for [Lightweight Directory Access Protocol](#).

LDM

[Storage System] Acronym for [Logical Disk Manager](#).

least privilege

[Data Security] The security objective of granting users only those accesses they need to perform their official duties. [NIST SP 800-12]

LED

[Computer System] Acronym for [Light Emitting Diode](#).

legal hold

[Legal] Process of suspending the normal disposition or processing of records and [Electronically Stored Information](#) as a result of current or anticipated litigation, audit, government investigation or other such matters. [ISO/IEC 27050-1]

The issued communication that implements the legal hold can also be called a "hold," "preservation order," "suspension order," "freeze notice," "hold order," or "hold notice."

library

[Storage System] A [storage device](#) containing a [robotic media handler](#) capable of storing multiple pieces of removable media and loading and unloading them from one or more drives in arbitrary order.

lifecycle deletion

[Storage System] The deletion of data at the end of its lifecycle.

See [disposition policy](#).

Light Emitting Diode (LED)

[Computer System] A [multimode](#) light source based on inexpensive optical diodes.

Available in a variety of wavelengths; 1300 nanometer wavelength is typical for data communications. The practical transfer rate limit for LEDs is 266 [Mbps](#).

Lightweight Directory Access Protocol (LDAP)

[Network] An [IETF protocol](#)—originally a subset of the X.500 protocol—for creating, accessing and removing objects and data from a [directory](#).

LDAP provides the ability to search, compare, add, delete and modify directory objects, as well as modifying the names of these objects. It also supports *bind*, *unbind* and *abandon* (cancel) operations for a session. LDAP got its name from its goal of being a simpler form of DAP (Directory Access Protocol).

Linear Tape File System (LTFS)

1. [File System] A self-describing, self-contained tape storage format intended for interchange of data between different software systems.

See ISO/IEC 20919.

2. [File System] A software or hardware implementation of a [file system](#) using the LTFS tape format.

Linear Tape Open (LTO)

[Tape] An open standard magnetic tape technology developed in cooperation by HP, IBM and Quantum.

link

1. [General] A physical [connection](#) (electrical or optical) between two nodes of a network.
2. [Fibre Channel] Two unidirectional fibers or conductors transmitting in opposite directions and their associated transmitters and receivers.
3. [Fibre Channel] The full-duplex [FC-0](#) level association between [FC-1](#) entities in directly attached ports.
4. [Fibre Channel] The point to point physical connection from one element of a [Fibre Channel](#) fabric to the next.
5. [Fibre Channel] A collection of multiple lanes.

LIP

[Fibre Channel] Acronym for [Loop Initialization Primitive](#).

LISM

[Fibre Channel] Acronym for [Loop Initialization Select Master](#).

litigation hold

[Legal] Synonym for [legal hold](#).

load balancing

[Computer System] The adjustment of system and/or application components and data so that application I/O or computational demands are spread as evenly as possible across a system's physical resources.

[I/O load balancing](#) may be done manually (by a human) or automatically (by some means that does not require human intervention). See [load optimization](#), [load sharing](#).

L

load optimization

[Computer System] The manipulation of an [I/O load](#) in such a way that performance is optimal by some objective metric.

Load optimization may be achieved by load balancing across several components, or by other means, such as request reordering or interleaved execution. See [load balancing](#), [load sharing](#).

load sharing

[Storage System] The division of an [I/O load](#) or task among several [storage subsystem](#) components, without any attempt to equalize each component's share of the work.

See [I/O load balancing](#), [load optimization](#).

load/store architecture

[Computer System] A CPU architecture in which memory is only accessed through load and store instructions, and all other instructions access data in registers only.

load/store operations

[Computer System] Operations that move data between CPU registers and memory.

local area network

[Network] A communications infrastructure—typically [Ethernet](#)—designed to use dedicated wiring over a limited distance (typically a diameter of less than five kilometers) to connect a large number of intercommunicating nodes.

See [wide area network](#).

Local Area Network Emulation (LANE)

[Network] A collection of protocols and services that combine to create an emulated [local area network](#) using [ATM](#) as the underlying network.

Local area network emulation enables intelligent devices with ATM connections to communicate with remote [LAN](#)-connected devices as if they were directly connected to the LAN.

local backup

[Data Recovery] A [backup](#) methodology that utilizes host resources to copy data to a backup location that is under control of the same host.

local F_Port

[Fibre Channel] The [F_Port](#) to which a particular [N_Port](#) is directly attached by a link.

locking

[General] Any method of managing concurrent access to a resource.

logical block

[Storage System] A [block](#) of data stored on a disk or tape, and associated with an address for purposes of retrieval or overwriting.

The term *logical block* is typically used to refer to the host's view of data [addressing](#) on a physical device. Within a [storage device](#), there is often a further conversion between the logical blocks presented to hosts and the physical [media](#) locations at which the corresponding data is stored. See [physical block](#), [virtual block](#).

logical block address

[Storage System] The address of a [logical block](#), i.e., the offset of the block from the beginning of the block address space of the logical device that contains it.

Logical block addresses are typically used in hosts' I/O commands. The [SCSI](#) disk command [protocol](#), for example, uses logical block addresses.

logical disk

[Storage System] A set of consecutively addressed disk blocks that is part of a single virtual disk to [physical disk mapping](#).

Logical disks are used in some [array](#) implementations as constituents of logical volumes or partitions. Logical disks are normally not visible to the [host environment](#), except during [array configuration](#) operations. See [extent](#), [virtual disk](#).

logical disk manager

[Windows] A name for the [volume](#) management [control software](#) in the Windows NT operating system.

Logical Unit (LU)

[SCSI] The addressable entity within a [SCSI target](#) that executes I/O commands.

Logical Unit Number (LUN)

1. [SCSI] The [SCSI](#) identifier of a [logical unit](#) within a [target](#).
2. [SCSI] Industry shorthand, when phrased as "lun", for the logical unit indicated by the logical unit number.

logical volume

[Storage System] A [virtual disk](#), also called a virtual disk, or [volume set](#), made up of logical disks.

long wavelength laser

[Fibre Channel] A [laser](#) with a wavelength 1300 nm or longer; usually 1300 or 1550 nanometers; widely used in the telecommunications industry.

long-term data retention

[Data Management] The practice of archiving data for extended periods of time, including 'forever'.

Issues related to security and [media](#), application and display formats must all be addressed for successful long-term retention. See [data preservation](#).

long-term preservation

[Long Term Retention] The act of maintaining information, in a correct and independently understandable form, over a period of decades or longer.

See [digital preservation](#).

loop initialization

[Fibre Channel] The [protocol](#) by which a [Fibre Channel Arbitrated Loop](#) network initializes upon power up or recovers after a failure or other unexpected condition.

Loop Initialization Primitive (LIP)

[Fibre Channel] A [Fibre Channel](#) primitive used to (1) initiate a procedure that results in unique [addressing](#) for all nodes, (2) indicate a loop failure, or (3) reset a specific [node](#).

During a LIP, the nodes present on the [arbitrated loop](#) identify themselves and acquire addresses on the loop for communication. No data can be transferred on an arbitrated loop until a LIP is complete.

Loop Initialization Select Master (LISM)

[Fibre Channel] The process by which a temporary [Fibre Channel arbitrated loop](#) master is determined during [loop initialization](#).

loop port state machine

[Fibre Channel] Logic that monitors and performs the tasks required for [initialization](#) and access to a [Fibre Channel arbitrated loop](#).

loop switch

[Fibre Channel] A [Fibre Channel switch](#) operating at the layer 2 level allowing multiple dynamic point-to-point connections between devices using the [FC-AL protocol](#).

Loop switches do not implement the Fibre Channel Switch Fabric protocols ([FC-SW-x](#) standards).

loopback

[Fibre Channel] An [FC-1 operational](#) mode in which information passed to the FC-1 [transmitter](#) is shunted directly to the FC-1 [receiver](#).

When a [Fibre Channel](#) interface is in loopback mode, the loopback signal overrides any external signal detected by the receiver.

L

lossless Ethernet bridging element

[Fibre Channel] [Network] An [Ethernet](#) bridging function supporting the minimum required capabilities of Lossless Ethernet MACs.

lossless Ethernet MAC

[Fibre Channel] [Network] A [full duplex Ethernet MAC](#) that supports at least 2.5KB jumbo frames and implements extensions to avoid Ethernet [frame](#) loss due to congestion (e.g., the Ethernet Pause mechanism).

lossless Ethernet network

[Fibre Channel] [Network] An [Ethernet](#) network composed only of [full duplex](#) links, Lossless Ethernet MACs, and Lossless Ethernet bridging elements.

LTFS

[File System] Acronym for [Linear Tape File System](#).

LTFS Index

[File System] [Metadata](#) which describes the file data types and locations on an [LTFS volume](#).

LTFS Volume

[File System] A tape cartridge utilizing the [LTFS](#) format.

LTO

[Storage System] Acronym for [Linear Tape Open](#).

LU

[SCSI] Acronym for [Logical Unit](#).

LUN

[SCSI] Acronym for [Logical Unit Number](#).

LWL

[Fibre Channel] Acronym for [Long Wavelength Laser](#).

M

M.2

[Hardware] A card form factor and connector interface defined by the PCI-SIG that is most commonly used for [solid state storage](#).

M.2 interfaces to [PCI](#) Express, SATA-IO, and USB.

MAC

1. [Network] Acronym for [Media Access Control](#).
2. [Data Security] Acronym for [Message Authentication Code](#).
3. [Data Security] Acronym for [Mandatory Access Control](#).

magnetic remanance

[Data Security] Residual magnetic information remaining on a magnetic [medium](#) after the medium has been degaussed.

MAID

[Storage System] Shorthand for [Massive Array of Idle Disks](#).

malware

[Computer system] Malicious software designed specifically to damage or disrupt a system, attacking confidentiality, integrity and/or [availability](#). [ISO/IEC 27033-1]

M

Examples are a [virus](#), [worm](#), [Trojan horse](#), spyware, adware or other entity that infects a system.

MAM

[Storage System] Acronym for [Medium Auxiliary Memory](#).

MAN

[Network] Acronym for [Metropolitan Area Network](#).

Managed Object Format (MOF)

[Management] The syntax and formal description of the classes and associations in a [CIM schema](#).

MOF can be translated to [XML](#) using a [Document Type definition](#) published by the [DMTF](#).

management framework

[Management] A structure and set of services exposed for use by management applications and other services in the management environment.

Management Information Base (MIB)

[Management] The specification and formal description of a set of objects and variables that can be read and possibly written using the [SNMP protocol](#).

Various standard MIBs are defined by the [IETF](#)., and vendor-specific MIBs are quite common as well.

mandatory (provision)

[Standards] A provision in a standard that must be supported in order for an implementation of the standard to be compliant with the standard.

Mandatory Access Control (MAC)

[Data Security] A type of [access control](#) based on the security clearance of the [subject](#) and the classification of the object.

The control is [mandatory](#) in that a subject is not allowed to change either their security clearance or the classification of an object.

map

[Operating System] The assignment of virtual addresses to a portion of a file (e.g., POSIX).

mapping

[Storage System] Conversion between two address spaces, such as the conversion between [physical disk block](#) addresses and the block addresses of the virtual disks presented to operating environments by [control software](#).

mapping boundary

[Storage System] A [virtual disk block](#) address of some significance to a [disk array](#)'s [mapping](#) algorithms.

The first and last blocks of a user data space [stripe](#) or [check data](#) stripe are mapping boundaries.

Massive Array of Idle Disks (MAID)

[Storage System] A storage system comprising an [array](#) of disk drives that are powered down individually or in groups when not required.

MAID storage systems reduce the power consumed by a [storage array](#), at the cost of increased [Mean Time To Data](#).

Max TTFD

[Storage System] Shorthand for [Maximum Time to First Data](#).

Maximum Time to First Data (Max TTFD)

[Storage System] The maximum time required to start receiving data from a storage system to satisfy a read request for arbitrary data.

Max TTFD is used in the industry and in the *SNIA Emerald™ Power Efficiency Measurement Specification* to distinguish classes of storage systems.

M

Maximum Transfer Unit

[Network] The largest amount of data that it is permissible to transmit as one unit according to a [protocol](#) specification.

The [Ethernet MTU](#) is 1536 eight bit bytes. The [Fibre Channel](#) MTU is 2112 eight bit bytes.

MB**MByte**

[Computer System] Shorthand for [Megabyte](#).

Mb**Mbit**

[Computer System] Abbreviations for [Megabit](#).

MBps

[Computer System] Shorthand for Megabytes per second, a measure of [bandwidth](#) or [data transfer rate](#).

Mbps

[Computer System] Shorthand for megabits per second, a measure of [bandwidth](#) or [data transfer rate](#).

MD5

[Data Security] A message-[digest](#) algorithm producing a 128-bit digest.

This algorithm is obsolete.

Mean Time Between Failures (MTBF)

[General] The expected time between consecutive failures in a system or component. [ISO/IEC/IEEE 24765]

Mean Time To Data (MTTD)

[storage system] The average time required to stage a data stream from storage and make it available for reading by a [client](#).

mean time to data loss

[Storage System] The average time from startup until a component failure causes a permanent loss of user data in a large population of storage elements.

[Mean time to data](#) loss is similar to [MTBF](#) for disks and tapes, but is likely to differ in [RAID](#) arrays, where [redundancy](#) can protect against data loss due to component failures.

Mean Time To (first) Failure (MTTF)

[General] The average time from start of use to first failure in a large population of identical systems, components, or devices.

mean time to loss of data availability

[Storage System] The average time from startup until a component failure causes a loss of timely user data access in a large population of storage elements.

Loss of [availability](#) does not necessarily imply loss of data; for some classes of failures, (e.g., failure of non-[redundant](#) intelligent storage controllers), data remains intact, and can again be accessed after the failed component is replaced.

Mean Time To Repair (MTTR)

[General] The average time between a failure and completion of repair in a large population of identical systems, components, or devices.

Mean time to repair comprises all elements of repair time, from the occurrence of the failure to [restoration](#) of complete functionality of the failed component. This includes time to notice and respond to the failure, time to repair or replace the failed component, and time to make the replaced component fully [operational](#). In mirrored and [RAID](#) arrays, for example, the mean time to repair a disk failure includes the time required to reconstruct user data and [check data](#) from the failed disk on the [replacement disk](#).

M

meaningful (control field)

[Standards] In a standard, a control field or bit that must be correctly interpreted by a [receiver](#).

Control fields are either meaningful or “not meaningful.” In the latter case they must be ignored.

measured service

[Services] Metered dispensation of resources appropriate to a given type of service (e.g., storage, processing, [bandwidth](#), and active user accounts), such that usage can be monitored, controlled, reported and billed.

Mebibit (Mibit)

[General] Shorthand for 1,048,576 (2^{20}) bits.

Binary notation is most commonly used for semiconductor memory sizes.

See also [Megabit](#).

Mebibyte (MiB)

[General] Shorthand for 1,048,576 (2^{20}) bytes.

Binary notation is most commonly used for semiconductor memory sizes.

See also [Megabyte](#).

media

1. [Storage System] Synonym for [storage media](#).
2. [Network] A physical link on which data is transmitted between two points.

Media Access Control (MAC)

1. [Network] Algorithms that control access to physical [media](#), especially in shared media networks.
2. [Network] The MAC layer in the [Ethernet protocol](#).

media changer

[SCSI] Deprecated [SCSI](#) term for [library](#).

media ID

[Data Recovery] A machine-readable identifier written on a removable storage [volume](#) that remains constant throughout the volume's life.

See [external volume serial number](#), [label](#).

media manager

[Data Recovery] A [backup](#) software component responsible for tracking the location, contents, and state of removable storage volumes.

media robot

[Storage System] Synonym for [robotic media handler](#).

media sanitization

[Data Security] A general term referring to the actions taken to render data written on media unrecoverable by both ordinary and extraordinary means. [NIST SP 800-88]

Making data unrecoverable by extraordinary means usually involves total destruction of the [media](#).

media stacker

[Storage System] A [robotic media handler](#) in which media must be moved sequentially by the [robot](#).

medium

[Storage System] See [media](#).

Medium Auxiliary Memory (MAM)

[Storage System] A non-volatile memory (other than the recording [medium](#)) residing in a [storage element](#) (e.g., a tape cartridge) that is accessible to the [storage device](#).

medium transport element

[SCSI] Synonym for [robotic media handler](#).

M

megabaud

[Data Communication] One million [baud](#) (elements of transmitted information) per second, including data, signaling and overhead.

Megabit (Mb)

[Computer System] 1,000,000 (10^6) bits.

The SNIA uses the base 10 convention commonly found in I/O-related and scientific literature rather than the base 2 convention (1,048,576, i.e., 2^{20}) common in computer system and software literature.

See also [Mebibit](#).

Megabyte (MB)

[Computer System] 1,000,000 (10^6) bytes.

The SNIA uses the base 10 convention commonly found in I/O-related and scientific literature rather than the base 2 convention (1,048,576, i.e., 2^{20}) common in computer system and software literature.

See also [Mebibyte](#).

megatransfer

[SCSI] The transfer of one million data units per second.

The term is used to describe the characteristics of [parallel](#) I/O interconnects like SCSI, for which the [data transfer rate](#) depends upon the amount of data transferred in each data cycle. See [SCSI](#), [fast SCSI](#), [Ultra SCSI](#), [Ultra2 SCSI](#), [wide SCSI](#).

melting

[Data Security] A method of sanitization that uses extreme heat to cause a device or component to change state, from solid to liquid and/or gas, in an approved facility. [ISO/IEC 27040]

member**member disk**

[Storage System] A disk that is in use as a member of a [disk array](#).

Message Authentication Code (MAC)

[Data Security] A cryptographic hash appended to a message to allow a [receiver](#) to ensure that the contents have not been changed in transit.

message digest

[Data Security] Synonym for [hash value](#).

message digest algorithm

[Data Security] An algorithm that produces a [secure hash](#).

metadata

[Data Management] Data associated with other data.

metering

[Services] Providing a measuring capability appropriate to the type of service (e.g., storage, processing, [bandwidth](#), and active user accounts).

Metropolitan Area Network (MAN)

[Network] A network that connects nodes distributed over a metropolitan (city-wide) area as opposed to a local area (campus) or wide area (national or global).

From a storage perspective, MANs are of interest because there are MANs over which [block](#) storage protocols (e.g., [ESCON](#), [Fibre Channel](#)) can be carried natively, whereas most WANs that extend beyond a single metropolitan area do not currently support such protocols.

MIB

[Management] Acronym for [Management Information Base](#).

Mibit

[General] Shorthand for [Mebibit](#).

MiB**MiByte**

[General] Shorthand for [Mebibyte](#).

migration

[Data Management] A movement of data or information between information systems, formats, or [media](#).

Migration is performed for reasons such as possible decay of [storage media](#), obsolete hardware or software (including obsolete data formats), changing performance requirements (see [tiered storage](#)), the need for cost efficiencies etc.

MIME

[Network] Acronym for [Multipurpose Internet Mail Extensions](#).

mirror

[Storage System] A [replica](#) of a storage [volume](#), consisting of separate components with identical contents to the original volume, that can be accessed independently by the storage system.

mirror resynchronization

[Data Recovery] The process of making the contents of a split [mirror](#) identical with the contents of the storage devices from which the mirror was split.

Mirror resynchronization may entail copying the entire contents of the storage devices, or when [fast mirror resynchronization](#) is used, only the data items changed in the original since the instant of splitting.

mirrored array

[Storage System] Common term for a [disk array](#) that implements [RAID Level 1](#), or [mirroring](#).

mirroring

[Storage System] A [configuration](#) of storage in which two or more identical copies of data are maintained on separate [media](#);

also known as [RAID Level 1](#), [disk shadowing](#), real-time copy, and [T1 copy](#).

mirrors

mirrored disks

[Storage System] The disks of a [mirrored array](#).

MMA

[Management] Acronym for [Multipath Management API](#).

modal dispersion

[Network] Distortion in the optical signal transmitted through a [multimode](#) fiber caused by different time delays for the various modes of propagation, resulting in a smearing of the signal edges that increases with the length of the fiber, thereby limiting the maximum length as a function of the data rate.

mode of operation

[Data Security] An algorithm for the cryptographic [transformation](#) of data that applies a symmetric key [block cipher](#) algorithm to one or more blocks of data.

model

[Management] A set of entities and the relationships between them that define the semantics, behavior and state of that set.

modeling language

[Management] A language for describing the concepts of an information or [data model](#).

A popular modeling language in use today is [UML](#) ([Unified Modeling Language](#)).

MOF

[Management] Acronym for [Managed Object Format](#).

monitor (program)

[Computer System] A program that executes in an [operating environment](#) and keeps track of system resource utilization.

M

Monitors typically record CPU utilization, [I/O request](#) rates, data transfer rates, RAM utilization, and similar statistics. A monitor program, which may be an integral part of an operating system, a separate software product, or a part of a related component, such as a [database management system](#), is a necessary prerequisite to manual [I/O load balancing](#).

mount

[Storage System] In the [Network File System \(NFS\)](#), a [protocol](#) and set of procedures to specify a remote host and file system or [directory](#) to be accessed, and their location in the local directory hierarchy.

MTBF

[Computer System] Acronym for [Mean Time Between Failures](#).

MTDL

[Computer System] Acronym for [Mean Time to Data Loss](#).

MTTD

[General] Acronym for [Mean Time To Data](#).

MTTF

[General] Abbreviation for [Mean Time to \(first\) Failure](#).

MTTR

[General] Acronym for [Mean Time To Repair](#).

MTU

[Network] Acronym for [Maximum Transfer Unit](#).

multicast

[Fibre Channel] [Network] The simultaneous transmission of a message to multiple, but not all, of the ports connected to a communication facility.

In a [Fibre Channel](#) context, multi-cast specifically refers to the sending of a message to multiple N_Ports connected to a fabric.

multicast group

[Fibre Channel] [Network] A set of ports associated with an address or identifier that serves as the destination for [multicast](#) packets or frames that are to be delivered to all ports in the set.

multi-factor authentication

[Data Security] Verification of an individual's identity using more than one factor pertaining to knowledge, possession or biometrics.

A knowledge factor is something an individual knows; a possession factor is something an individual has, and a biometric factor is something an individual is or is able to do.

multi-level disk array

[Storage System] A [disk array](#) with multiple levels of data [mapping](#), in which the virtual disks created by one mapping level become the members of the next level.

The most frequently encountered multi-level disk arrays use [mirroring](#) at the first level, and [stripe](#) data across the resulting mirrored arrays at the second level.

multilevel security

[Data Security] A security system that allows users and resources of different sensitivity levels to access a system concurrently, while ensuring that only information for which the user or resource has [authorization](#) is made available.

multimode (fiber optic cable)

[Fibre Channel] [Network] Designed to carry multiple light rays or modes concurrently.

In optical fiber, each mode is transmitted at a slightly different reflection angle within the optical fiber core. Multimode fiber transmission is used for relatively short distances.

Multi-Path I/O (MPIO)

[Storage System] The facility for a host to direct I/O requests to a [storage device](#) on more than one [access path](#).

M

This requires that devices be uniquely identifiable by some means other than by bus address.

Multipath Management API (MMA)

[Management] A SNIA specification for discovery and management of the multipath devices on a host system and the associated local and device ports.

multiplexer

[Fibre Channel] A [Fibre Channel](#) architectural object that provides the functions of the [FC-2M](#) sublevel, multiplexing and demultiplexing frames between a set of physical ports and a set of virtual ports.

Multiplexers are components of both nodes and switches.

multi-protocol storage

[Storage System] Synonym for [unified storage](#).

Multipurpose Internet Mail Extensions (MIME)

[Network] A specification that defines the mechanisms for specifying and describing the format of Internet message bodies.

An [HTTP](#) response containing a [MIME](#) Content-Type header allows the HTTP [client](#) to invoke the appropriate application for processing the received data.

multi-tenancy

[Data Security] Allocation of physical and virtual resources such that multiple tenants and their computations and data are isolated from and inaccessible to one another. [ISO/IEC 17788]

multi-threaded

[Computer System] Having multiple concurrent or pseudo-concurrent execution sequences.

Multi-threaded processes are one means by which [I/O request](#)-intensive applications can make maximum use of disk arrays to increase I/O performance.

mutual authentication

[Data Security] A process that verifies the [identity](#) of both entities prior to establishing communication.

N

N_Port

[Fibre Channel] A "[Node](#)" port that connects via a point-to-point link to either a single N_Port or a single [F_Port](#).

N_Ports handle creation, detection, and flow of message units to and from the connected systems. N_Ports are end ports in virtual point-to-point links through a fabric, for example the N_Port on an end node to F_Port on a [switch](#) to F_Port in that switch to the N_Port on the other end node using a single [Fibre Channel](#) fabric switch. An N_Port is assumed to always refer to an [Nx_Port](#) in a direct Fabric-attached [PN_Port](#), and does not include NL_Ports

N_Port_ID Virtualization (NPIV)

[Fibre Channel] The ability for a single physical [Fibre Channel node](#) or [switch](#) to support more than one [Nx_Port](#) on a single point-to-point link.

N_Port_Name

[Fibre Channel] A [Name Identifier](#) associated with an [N_Port](#).

NAA

[Network] [Standards] Acronym for [Network Address Authority](#).

N

Name_Identifier

[Fibre Channel] A 64-bit identifier, with a 60-bit value preceded by a 4-bit Network_Address_Authority Identifier, used to identify entities in [Fibre Channel](#) (e.g., [Nx_Port](#), [node](#), [F_Port](#), or Fabric).

name server

1. [Fibre Channel] A distributed service provided by the fabric to register and discover the attributes of [Fibre Channel](#) N_Ports. Once registered, the attributes may be viewed by requesting N_ports.
2. [Network] A [server](#), such as a [DNS](#) server, that resolves textual names to machine addresses and vice versa.

namespace

1. [File System] The set of valid names recognized by a [file system](#).
2. [General] In [XML](#), a document at a specific Web address (URL) that lists the names of data elements and attributes that are used in other XML files.
3. [Management] In [CIM](#) and [WBEM](#), a collection of object definitions and instances that are logically consistent.

naming

[Computer System] The [mapping](#) of address space to a set of objects.

Naming is typically used either for human convenience (e.g., symbolic names attached to files or storage devices), or to establish a level of independence between two system components (e.g., [identification](#) of files by [inode](#) names or identification of computers by [IP](#) addresses).

NAS

[Network] [Storage System] Acronym for [Network Attached Storage](#).

National Institute of Standards and Technology (NIST)

[Standards] [Data Security] A non-regulatory federal agency within the U.S. Commerce Department's Technology Administration.

NIST's mission is to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life. Specifically, the [Computer Security](#) Division within NIST's [Information Technology](#) Laboratory managed the [Advanced Encryption Standard](#) (AES) program.

native data format

[Legal] The original, non-derived format and structure of data, together with its associated [metadata](#).

Where data is unstructured, native file format means the original format of a file. While structured or [unstructured data](#) may be read by other programs, native data format means data whose state and [integrity](#) are unchanged since generation by its instantiating application.

Native Fabric

[Fibre Channel] In [inter-fabric routing](#) (IFR), the local fabric where the [Native Nx_Port](#) resides.

Native Nx_Port

[Fibre Channel] A role of an [Nx_Port](#) in an IFR environment.

A Native Nx_Port is physically attached to the local fabric.

NDMP

[Management] [Network] Acronym for [Network Data Management Protocol](#).

near-online data

[Data Management] Data that is accessible within some moderate length of time, usually some number of seconds.

See [active data](#), [offline data](#).

near-online storage

[Energy] Storage systems with first data access times > 80 ms and less than several seconds, as specified in the *SNIA Emerald™ Power Efficiency Measurement Specification*.

network

[Network] An [interconnect](#) that enables communication among a collection of attached nodes, consisting of optical or electrical transmission [media](#), infrastructure in the form of hubs and/or switches, and protocols that make message sequences meaningful.

In comparison to I/O interconnects, networks are typically characterized by large numbers of nodes that act as peers, large inter-node separation, and flexible configurability. See [channel](#), [I/O interconnect](#), [local area network](#), [storage area network](#).

network adapter

[Network] An [adapter](#) that connects an [intelligent device](#) to a network, also called a [network interface card](#), or NIC.

See [Ethernet adapter](#), [NIC](#).

Network Address Authority (NAA)

[Fibre Channel] A 4-bit field used to identify the controlling authority for guaranteeing uniqueness of World Wide Names (WWNs).

In a [Fibre Channel](#) environment, several [Naming](#) Authorities can be active at the same time, therefore Fibre Channel prepends the NAA field to World Wide Names to guarantee global uniqueness. An NAA =1, for example, indicates IEEE 48-bit Identifiers. The NAA also identifies one of several WWN formats, for example Format 1, Format 2 and Format 5.

Network Attached Storage (NAS)

1. [Storage System] A term used to refer to storage devices that connect to a network and provide file access services to computer systems.

These devices generally consist of an engine that implements the file services, and one or more devices, on which data is stored.

2. [Network] A class of systems that provide file services to host computers using file access protocols such as [NFS](#) or [CIFS](#).

See [storage area network](#).

network backup

[Data Recovery] A [backup](#) methodology that copies data over a [LAN](#) to a Backup [Server](#).

Network Data Management Protocol (NDMP)

[Data Recovery] A communications [protocol](#) that allows data storage devices, robotic [library](#) devices, and [backup](#) applications to intercommunicate for the purpose of performing backups.

NDMP is an open standard protocol for network-based backup of [NAS](#) devices. It allows a [network backup](#) application to control the retrieval of data from, and backup of, a [server](#) without third-party software. The control and data transfer components of backup and restore are separated. NDMP is intended to support tape drives, but can be extended to address other devices and [media](#) in the future. The SNIA has developed a v4 reference implementation, based on donation to it of the original code from NetApp and PDC.

Network File System (protocol) (NFS)

[File System] [Standards] A distributed [file system](#) and its associated network [protocol](#), commonly implemented in UNIX systems.

The [IETF](#) maintains the [NFS](#) standard. NFS clients and/or servers are available for all major platforms at this point.

Network Interface Card (NIC)

[Network] An [I/O adapter](#) that connects a computer or other type of [node](#) to a network.

A NIC is commonly a plug-in [circuit](#) board, however, the term is also used to denote an [ASIC](#) or set of ASICs on a computer

N

[system board](#) that perform the network I/O adapter function. The term *NIC* is universally used in [Ethernet](#) and [token ring](#) contexts. In [Fibre Channel](#) contexts, the terms host bus adapter, HBA and *adapter* are used in preference to *NIC*. See [host bus adapter](#), [I/O adapter](#).

nexus

[SCSI] A temporary relationship between two [SCSI](#) devices, consisting of at least a target identifier and initiator identifier.

A full working nexus, known as an I_T_L_Q nexus, also contains a Logical Unit Number (LUN) and a Queue tag.

NFS

[File System] [Standards] Acronym for [Network File System](#).

NIC

[Network] Acronym for [Network Interface Card](#).

NIST

[Data Security] Shorthand for [National Institute of Standards and Technology](#).

NL_Port

[Fibre Channel] A “[Node](#) Loop” port, i.e., an [Nx_Port](#) that is communicating via an [Arbitrated Loop](#).

NL_Ports are end points for [Fibre Channel](#) communication via Arbitrated Loop topologies that are attached to a Fabric, for example NL_Port to FL_Port to F_Port to N_Port using a single Fibre Channel Fabric [switch](#). See [F_Port](#), [FL_Port](#), [Nx_Port](#), [L_Port](#).

node

[Network] [Storage System] An addressable entity connected to an [I/O interconnect](#) or network.

The term *node* is used to refer to computers, storage devices, storage subsystems and network interconnection devices such as

switches, routers and gateways. The component of a node that connects to the bus or network is a port.

Node_Name

[Fibre Channel] A [Name Identifier](#) that is associated with a [Fibre Channel node](#).

non-erasable content

[Data Management] Content that cannot be deleted except in accordance with a [retention policy](#).

non-linear mapping

[Storage System] Any form of [tabular mapping](#) in which there is not a fixed size correspondence between the two mapped address spaces.

Non-linear mapping is required in disk arrays that compress data, since the space required to store a given range of virtual blocks depends on the degree to which the contents of those blocks can be compressed, and therefore changes as [block](#) contents change. See [algorithmic mapping](#), [dynamic mapping](#), [tabular mapping](#).

nonrepudiation

[Data Security] [Assurance](#) that a [subject](#) cannot later deny having performed some action.

For communication, this may involve providing the sender of data with proof of delivery and the recipient with proof of the sender's [identity](#), so neither can later deny having participated in the communication. Digital signatures are often used as a non-[repudiation](#) mechanism for stored information in combination with timestamps.

non-transparent failover

[Computer System] A [failover](#) from one component of a [redundant](#) system to another that is visible to the external environment.

An example is a [controller](#) failover in a redundant [disk subsystem](#) if the surviving controller exports the other's virtual disks at

N

different [host I/O interconnect](#) addresses or on a different host I/O interconnect. See [transparent failover](#).

Non-Uniform Memory Architecture (NUMA)

[Computer System] A computer architecture that enables memory to be shared by multiple processors, but with different processors having different access speeds to different parts of the memory.

non-volatile cache

[Storage System] A cache that retains data through power cycles.

non-volatile memory (NVM)

[Computer System] Synonym for [NVRAM](#).

Non-Volatile Random Access Memory (NVRAM)

[Computer System] Computer system random access memory that has been made impervious to data loss due to power failure through the use of [UPS](#), batteries, or implementation technology such as flash memory.

Non-Volatile Dual Inline Memory Module (NVDIMM)

[Hardware] A [dual inline memory module](#) that operates as standard RAM while also having persistence across power cycles.

non-volatility

[Storage System] The property of an electronic device that data is preserved even when electrical power is removed.

normal operation

normal mode

[Computer System] A state of a system in which the system is functioning within its prescribed [operational](#) bounds.

For example, a [disk array subsystem](#) is operating in normal mode when all disks are up, no extraordinary actions (e.g., [reconstruction](#)) are being performed, and environmental

conditions are within operational range. Sometimes called optimal mode.

not operational (receiver, transmitter)

[Fibre Channel] A [receiver](#) or [transmitter](#) that is not capable of receiving or transmitting an encoded bit stream based on rules defined by [FC-FS-2](#) for error control.

NPIV

[Fibre Channel] Acronym for [N_Port ID Virtualization](#).

NQN

[NVMe] Shorthand for NVMe Qualified Name.

NUMA

[Computer System] Shorthand for [Non-Uniform Memory Architecture](#).

NVDIMM

[Hardware] Acronym for [Non-Volatile Dual Inline Memory Module](#).

NVDIMM-F

[Hardware] A [dual in-line memory module](#) that is accessed using a block access protocol.

This appears in a separate address space from DRAM and may provide different performance than [DRAM](#).

NVDIMM-N

[Hardware] A dual in-line memory module that operates as persistent [DRAM](#).

The DRAM access methods are either byte- or block-oriented. This may not provide the same performance as volatile DRAM.

NVDIMM-P

[Hardware] A [dual in-line memory module](#) that operates as persistent [DRAM](#) (NVDIMM-N) and also as a block-accessed drive (NVDIMM-F) using non-volatile memory media.

N

NVM

[Computer System] Shorthand for [non-volatile memory](#).

NVM Express (NVMe)

[Storage System] A host [controller](#) interface with a register interface and command set designed for [PCI Express®](#)-based SSDs.

NVM Express over Fibre Channel (NVMeoFC)

[Fibre Channel] Protocol defined by [FC-NVMe](#).

NVM Subsystem

[NVMe] An integrated collection of one or more NVMe controllers and one or more ports.

NVMe

[NVMe] An acronym for NVM Express.

NVMe_DATA IUs

[Fibre channel] The [NVMeoFC Information Unit](#) for data frame(s) transfers.

NVMe-oF

[NVMe] Shorthand for [NVMe over Fabrics](#).

NVMe_Port

[Fibre Channel] [Nx_Port](#) that supports the FC-NVMe standard.

NVMe command

[Fibre Channel] A command issued by an NVMe host to a controller.

NVMe Completion Queue (CQ)

[NVMe] a circular buffer used to post status for completed NVMe commands

NVMe host

[NVMe] An entity that submits [NVMe](#) commands to a controller for processing and receives NVMe command completions from the same controller.

NVMe host port

[Fibre Channel] [VN_Port](#) that acts as an interface between an NVMe host and an [NVMe-oF](#) fabric.

NVMe over fabrics (NVMe-oF)

[NVMe] An interface to support message-based [NVMe](#) operations over a network fabric.

Example network fabrics include [Ethernet](#), [Fibre Channel](#), and [InfiniBand](#).

NVMe Submission Queue (SQ)

[NVMe] a circular buffer that NVMe host software uses to submit commands for processing by the NVMe controller

NVMeoFC

[Fibre Channel] Shorthand for [NVMe Express over Fibre Channel](#).

NVMeoFC association

[Fibre Channel] An [NVMeoFC](#) layer abstraction for an exclusive communication relationship between a particular [NVMe host](#), connected via a particular initiator [NVMe_Port](#), and a particular controller in an [NVM subsystem](#) connected via a particular target [NVMe_Port](#).

NVMeoFC connection

[Fibre Channel] An [NVMeoFC](#) layer abstraction representing an [NVMe Submission Queue](#) and [NVMe Completion Queue](#) pair for an NVMe controller.

NVMeoFC I/O operation

[Fibre Channel] A Fibre Channel exchange that is uniquely associated with an NVMe command.

NVMeoFC port

[Fibre Channel] An [NVMe Port](#) connecting one or more [NVMe hosts](#) or NVM subsystems to an FC Fabric.

NVRAM

[Computer System] Shorthand for [Non-Volatile Random Access Memory](#).

NVRAM cache

[Storage System] A quantity of [NVRAM](#) used as a [cache](#).

NVRAM cache is particularly useful in [RAID array](#) subsystems, filers, database servers, and other intelligent devices that must keep track of the state of multi-step I/O operations even if power fails during the execution of the steps. It also allows arrays to reply to writes before they are committed to disk, as the NVRAM becomes the non-volatile store for the writes.

NVRAM card

[Computer System] A printed [circuit](#) module containing [NVRAM](#).

Nx_Port

[Fibre Channel] An end point for [Fibre Channel frame](#) communication, having a distinct [address identifier](#) and [Name Identifier](#), providing an independent set of Fibre Channel functions to applications, and having the ability to act as an [Originator](#), a [Responder](#), or both, for Exchanges and Sequences.

O

OASIS

[General] Short name for the Organization for the Advancement of Structured Information Standards (OASIS), a consortium for developing standards (e.g., [KMIP](#)).

object

1. [General] An instantiated instance of a class in an [Object Oriented](#) system.
2. [Data Security] In the context of [access control](#), an entity such as an [information system](#) resource to which access is controlled and/or usage of which is restricted to authorized subjects.
3. [Data Management] The encapsulation of data and associated [metadata](#).

object drive

[Storage System] A storage element that directly provides [object services](#).

Object Oriented (methodology) (OO)

[General] A methodology for decomposing an entity or problem by its key abstractions, versus by its procedures or steps.

The key abstractions become classes in an information or [data model](#), and embody well-defined behaviors called *methods*, with

a unique set of data attributes. Instances of a class are called objects.

object service

[Storage System] Object-level access to storage.

object storage

[Storage System] A storage device that provides object services.

Object storage includes [DSaaS](#).

Object Storage Device (OSD)

[Storage System] An object-based storage standard defined by SNIA and [INCITS T10](#).

OC-n

[Network] A data rate that is a multiple of the fundamental [SONET](#) rate of 51.84 Mbits/sec.

OC-3 (155 Mbits/sec), OC-12 (622 Mbits/sec), OC-48 (2488 Mbits/sec) and OC-192 (9953 Mbits/sec) are currently in common use. See [Asynchronous Transfer Mode](#).

OData

[Management] The Open Data Protocol.

OData is an [OASIS](#) standard protocol that enables the creation and consumption of RESTful APIs.

OData service

[Management] A service conforming to the [OData](#) standard.

OData allows resources, identified using [Uniform Resource Locators](#) (URLs) and defined in a model, to be published and edited by Web clients using simple HTTP messages.

offline backup

[Data Recovery] A form of [backup](#) in which the data being backed up is not accessed by applications for the duration of the backup.

offline data

[Data Management] Data that may not be accessible for an extended period of time, for example data on removable [media](#) at a remote site.

See [near-online data](#).

offline data deduplication

[Capacity Optimization] Deprecated synonym for [post-process data deduplication](#).

OM1

[Fibre Channel] A designation for a [multimode](#) optical fiber with a 62.5 micrometer core diameter and a [bandwidth](#)-distance product of 200 MHz*km for 850 nm optical signals.

This fiber is typical of [FDDI](#) installations. Specified by ISO 11801 second edition.

OM2

[Fibre Channel] A designation for a [multimode](#) optical fiber with a 50 micrometer core diameter and a [bandwidth](#)-distance product of 500 MHz*km for 850 nm optical signals.

This fiber is typical of 1 [Gb/s Ethernet](#) and [Fibre Channel](#) installations. Specified by ISO 11801 second edition.

OM3

[Fibre Channel] A designation for a [multimode](#) optical fiber with a 50 micrometer core diameter and a [bandwidth-length product](#) of 2000 MHz*km for 850 nm optical signals.

Optical fiber is available with considerably higher bandwidth-distance products. Specified by ISO 11801 second edition.

online backup

[Data Recovery] A form of [backup](#) in which the data being backed up may be accessed by applications during the backup.

Online backup of a set of data is usually accomplished through the use of a [frozen image](#) of the data.

oo

[General] Acronym for [Object Oriented](#).

open

1. [General] Any system or aspect of a system whose function is governed by a readily accessible standard rather than by a privately owned specification.
2. [General] Not electrically terminated, as an unplugged cable.
3. [Fibre Channel] A period of time that begins when a [sequence](#) or [exchange](#) is initiated and ends when the sequence or exchange is normally or abnormally terminated.

Open Group, the

[General] A cross-industry consortium for open systems standards and their certification.

UNIX, management and security standards are developed within the Open Group, homed at www.opengroup.org.

open interconnect

[Computer System] Synonym for [standard interconnect](#).

operating environment

[Computer System] A collective term for the hardware architecture and operating system of a computer system.

operational (state)

[Fibre Channel] The condition of a [receiver](#) that is capable of receiving an encoded bit stream based on the rules defined by [FC-FS-2](#) for the FC receiver state machine.

Operational Recovery (OR)

[Data Recovery] [Recovery](#) of one or more applications and associated data to correct [operational](#) problems such as a corrupt database, user error or hardware failure.

OR may use a [point in time copy](#) or other techniques that create a consistent set of recoverable data.

Operation

[Storage] Any protocol command that is delivered from a client to a storage system, including I/O operations.

See also [OPS](#).

OPS**ops****Op/s****OPs**

[Storage] Shorthand for operations per second.

This is similar to *IOPS*, but includes non-read and non-write operations (e.g., NFS SETATTR call, SCSI TEST UNIT READY).

OPs is also used as the plural for operations, thus, Op/s is preferred to OPs.

See also [IOPS](#) and [operation](#).

optical fall time

[Network] The time interval required for the falling edge of an optical pulse to transition between specified percentages of the signal amplitude.

For lasers the transitions are measured between the 80% and 20% points. For [LED media](#) the specification points are 90% and 10%.

optional (characteristics)

[Standards] Characteristics of a standard that are specified by the standard but not required for [compliance](#), but which must be implemented as defined in the standard if they are implemented at all.

OR

[Data Recovery] Acronym for [Operational Recovery](#).

ordered set

[Fibre Channel] A [transmission word](#) ([sequence](#) of four 10-bit code bytes) with a [special character](#) in its most significant (first

on the link) position and data characters in the remaining three positions.

An ordered set is identified by the combination of special codes and data bytes that, when encoded, result in the generation of the transmission characters specified for the ordered set.

Ordered sets are used for low-level [Fibre Channel](#) link functions such as [frame](#) demarcation, signaling between the ends of a link, [initialization](#) after power on, and some basic [recovery](#) actions.

originator

1. [General] In a negotiation, the party that initiates the negotiation.
2. [Fibre Channel] With reference to an [Exchange](#), the [Nx_Port](#) that sent the [frame](#) that caused the Exchange to become open.

Originator Exchange_Identifier (OX_ID)

[Fibre Channel] An identifier assigned by an [Exchange Originator](#) to identify an Exchange.

An OX_ID is used by both the Exchange Originator and the Exchange [Responder](#) to identify the Exchange with respect to the Exchange Originator.

OSD

[Storage System] Acronym for [Object Storage Device](#).

out-of-band (transmission)

[Network] [Fibre Channel] Transmission of a separate data stream, such as management information, over a different medium than the primary data stream, e.g., transmission of [Fibre Channel](#) management information to a Fibre Channel component over an [Ethernet](#) network.

See [in-band](#).

out-of-band data deduplication

[Storage System] Deprecated synonym for [post-process data deduplication](#).

out-of-band virtualization

[Computer System] [Virtualization](#) functions or services that are not in the data path.

Examples are the management of data or storage, security management, [backup](#) of data, etc.

over provisioning

[Storage System] [Management] Purposely allocating more capacity than strictly required.

E.g., to avoid future out-of-capacity events.

E.g., in flash storage, extra capacity is reserved for controller use, is not addressable by the user, and is used to improve performance and device life.

overwrite procedure

[Data Security] A process of writing patterns of data on a magnetic [medium](#) for the purpose of obliterating data that was formerly stored there.

OX_ID

[Fibre Channel] Acronym for [Originator Exchange Identifier](#).

P

PaaS

[Services] Acronym for [Platform as a Service](#).

panic

[Computer System] A colloquial term describing a software program's reaction to an incomprehensible state.

In an operating system context, a panic is usually a system call, triggered by an unexpected state, that causes the system to abruptly stop executing. This is intended to reduce the possibility that the cause of the panic will cause further damage to the system, applications, or data and hopefully to preserve the system in a viable enough state that it can store debugging information in a safe place for analysis once it has come back up.

parallel access array

[Storage System] A [disk array](#) model in which data transfer and [data protection](#) algorithms assume that all [member](#) disks operate in unison, with each participating in the execution of every [application I/O request](#).

A [parallel](#) access array is only capable of executing one I/O request at a time. True parallel access would require that an array's disks be rotationally synchronized. In actual practice, arrays approximate parallel access behavior. Ideal [RAID Level 2](#) and [RAID Level 3](#) arrays are parallel access arrays. See [Independent access array](#).

parallel (transmission)

[Network] Simultaneous transmission of multiple data bits over multiple physical lines.

parity data

[Storage System] In a [RAID array](#), data stored on [member](#) disks that can be used for regenerating any user data that becomes inaccessible.

Parity data is usually calculated by taking the XOR of the data on the member disks.

parity disk

[Storage System] In a [RAID Level 3](#) or 4 [array](#) and some Level 6 arrays, a dedicated disk on which parity [check data](#) is stored.

parity RAID

[Storage System] A collective term used to refer to [Berkeley RAID Levels](#) 3, 4, 5 and 6.

parity RAID array

[Storage System] A [RAID array](#) whose [data protection](#) mechanism is one of [Berkeley RAID Levels](#) 3, 4, 5 or 6.

partition

1. [Storage System] A subdivision of the capacity of a physical or [virtual disk](#).

2. [Storage System] A contiguously addressed range of logical blocks on a physical [media](#) that is identifiable by an operating system.

Partitions are consecutively numbered ranges of blocks that are created and used by MS-[DOS](#), Windows, and most UNIX operating systems.

partitioning

[Storage System] Presentation of the usable storage capacity of a disk or [array](#) to an [operating environment](#) in the form of several virtual disks whose aggregate capacity approximates that of the underlying physical or [virtual disk](#).

Partitioning is common in MS-[DOS](#), Windows, and UNIX environments. Partitioning is useful with hosts that cannot support the full capacity of a large disk or array as one device. It can also be useful administratively, for example, to create hard subdivisions of a large virtual disk.

passphrase

[Data Security] A [sequence](#) of characters longer than the acceptable length of a [password](#) that is transformed by a password system into a virtual password of acceptable length.

password

[Data Security] A private alphanumeric string used to authenticate an [identity](#).

password digest

[Data Security] The hashed form of a [cleartext password](#).

path

1. [Storage System] The [access path](#) from a [host computer](#) to a [storage device](#).
2. [File System] The combination of device address and [file system directory](#) elements used to locate a file within a file system.
3. [Network] Any route through an [interconnect](#) that allows two devices to communicate.
4. [Computer System] A [sequence](#) of computer instructions that performs a given function, such as [I/O request](#) execution.
5. [Cloud] The access path from an internet-connected computer to a cloud service endpoint, typically in the form of a URI or URL.

path length

1. [Computer System] The number of instructions (a rough measure of the amount of time) required by a computer to perform a specific activity, such as [I/O request](#) execution.
2. [Data Recovery] [File System] The number of characters in a [path name](#).

path name

[File System] The complete list of nested sub-directories through which a file is reached.

payload

[Fibre Channel] [Network] Contents of the data field of a communications [frame](#) or packet.

In [Fibre Channel](#), the payload excludes [optional](#) headers and fill bytes, if they are present.

PB**PByte**

[Computer System] Shorthand for [Petabyte](#) (10^{15} bytes).

Pbit

[General] Shorthand for [Petabit](#).

PBC

[Fibre Channel] Acronym for [Port Bypass Circuit](#).

PCI

[Computer System] Acronym for [Peripheral Component Interconnect](#).

PCI Express Queuing Interface (PQI)

[SCSI] A circular queue interface for transferring information between a host and a device on a PCI Express bus or fabric.

pcnfsd

[File System] A [daemon](#) that permits personal computers to access file systems via the [NFS protocol](#).

PDU

1. [Network] [iSCSI] Acronym for [Protocol Data Unit](#).
2. [Computer System] Acronym for [Power Distribution Unit](#).

Pebibit (Pibit)

[General] Shorthand for 1,125,899,906,842,624 (2^{50}) bits.

Binary notation is most commonly used for semiconductor memory sizes.

See also [Petabit](#).

Pebibyte (PiB)

[General] Shorthand for 1,125,899,906,842,624 (2^{50}) bytes.

Binary notation is most commonly used for semiconductor memory sizes.

See also [Petabyte](#).

peer

[Computer System] One of two complimentary but physically separate systems.

For example, when user data is copied from a local system to a remote system, the remote system is considered the “peer” of the local system, and vice versa.

penetration

[Data Security] An unauthorized bypassing of the security mechanisms of a system.

penetration testing

[Data Security] A test methodology that attempts to circumvent or defeat the security features of an [information system](#).

performance audit

[Computer System] Systematic evaluation of a system by assessing how well it conforms to a set of established performance criteria.

Peripheral Component Interconnect (PCI)

[Computer System] A bus for connecting interface modules to a computer system.

Older variations of PCI support 32 and 64 bit [parallel](#) data transfers at 33 and 66 MHz cycle times. The newer PCIe interface supports one bit wide [serial](#) “lanes” operating at 250MB/sec or 500MB/sec.

permanent deletion

[Data Management] The process of reliably and provably eliminating the ability, to a given level of [assurance](#), to discover, recover, and read from digital [media](#).

This process has two phases. The first phase is identifying all of the instances (including the physical locations) of the data to be deleted regardless of where it is located; the second phase is permanently destroying all traces of the data. Depending on the level of assurance required, complete physical destruction of the media may be necessary. See [data shredding](#).

Legal considerations may also require maintenance of an [audit trail](#) of the above steps.

Permanent Port Name

[Fibre Channel] The [Name Identifier](#) common among all N_Ports that are associated with the same physical interface, and is set to the F_Port_Name of the [F_Port](#) that is attached to the physical interface.

persistence

[Computer System] A synonym for [non-volatility](#), usually used to distinguish between data and [metadata](#) held in DRAM, which is lost when electrical power is lost, and data held on non-volatile storage (disk, tape, battery-backed DRAM, etc.) that survives, or *persists* across power outages.

persistent memory access model

[Computer System] Semantic definition of how software accesses persistent memory hardware

persistent memory hardware

[Computer System] [NVRAM](#) that is byte addressable.

Personally Identifiable Information (PII)

[Data Security] Information associated with a person, as defined in ISO/IEC 29100.

Petabit (Pbit)

[General] Shorthand for 1,000,000,000,000,000 (10^{15}) bits.

The SNIA uses the base 10 convention commonly found in I/O-related and scientific literature rather than the base 2 convention (1,125,899,906,842,624, i.e., 2^{50}) common in computer system and software literature.

See also [Pebibit](#).

Petabyte (PB)

[Computer System] Shorthand for 1,000,000,000,000,000 (10^{15}) bytes.

The SNIA uses the base 10 convention commonly found in I/O-related and scientific literature rather than the base 2 convention (1,125,899,906,842,624, i.e., 2^{50}) common in computer system and software literature.

See also [Pebibyte](#).

phy

[SCSI] A transceiver used to set up physical links between [SCSI](#) devices.

There are different transceivers for each transport protocol. SAS, for example, uses four wires that comprise two differential signal pairs. Some other fabrics use an optical cable.

physical block

[Storage System] A physical area on a recording [media](#) at which data is stored, as distinguished from the logical and [virtual block](#) views typically presented to the [operating environment](#) by storage devices.

physical block address

[Storage System] The address of a [physical block](#), i.e., a number that can be algorithmically converted to a physical location on [storage media](#).

physical configuration

[General] The installation, removal, or re-installation of disks, cables, HBAs, and other components required for a system or subsystem to function.

Physical configuration is typically understood to include address assignments, such as [PCI](#) slot number, [SCSI target](#) ID and [Logical Unit Number](#), etc. See [array configuration](#), [configuration](#).

physical disk

1. [Storage System] A disk that is not virtual.
2. [Operating System] A host operating system's view of an online [storage device](#).

physical extent

[Storage System] A number of consecutively addressed blocks on a [physical disk](#).

Physical extents are created by [control software](#) as building blocks from which [redundancy](#) groups and [volume](#) sets are created. Called a p_extent by [ANSI](#).

physical extent block number

[Storage System] The relative position of a [block](#) within a [physical extent](#).

Physical extent block numbers are used to develop higher-level constructs in [RAID array](#) striped data [mapping](#), not for application or data [addressing](#).

Pibit

[General] Shorthand for [Pebibit](#).

PiB

PiByte

[General] Shorthand for [Pebibyte](#).

PII

[Data Security] Acronym for [Personally Identifiable Information](#).

PKCS

[Data Security] Acronym for [Public Key Cryptography](#) Standards.

PKI

[Data Security] Acronym for [Public Key Infrastructure](#).

plaintext

[Data Security] Unencrypted information.

platform

[Fibre Channel] A physical entity that contains nodes.

Platforms include all end devices that are attached to a Fabric, for example, hosts and storage subsystems. Platforms communicate with other platforms in the [storage area network](#) using the facilities of a Fabric or other [topology](#)

Platform as a Service (PaaS)

[Services] Delivery over a network of a virtualized programming environment, consisting of an application deployment stack based on a virtual computing environment.

Typically, PaaS is based on [IaaS](#), is either self-provisioned or provisionless, and is billed based on consumption.

PLDA

[Fibre Channel] Acronym for [Private Loop](#) Direct Attach.

PLOGI

[Fibre Channel] Shorthand for [Port Login](#).

PN_Port

[Fibre Channel] A [Fibre Channel](#) Link Control Facility (that is, a Fibre Channel physical port) in a [node](#)

point of encryption

[Data Security] Location within the Information and Communications Technology (ICT) infrastructure where data are encrypted on its way to storage (3.43) and, conversely, where data are [decrypted](#) when accessed from storage.

[ISO/IEC 27040]

The point of [encryption](#) is only applicable for data at rest.

Point In Time copy (PIT copy)

[Data Recovery] A fully usable copy of a defined collection of data that contains an image of the data as it appeared at a single instant in time.

A PIT copy is considered to have logically occurred at that point in time, but implementations may perform part or all of the copy at other times (e.g., via database log replay or rollback) as long as the result is a consistent copy of the data as it appeared at that point in time. Implementations may restrict point in time copies to be read-only or may permit subsequent writes to the copy. Three important classes of point in time copies are split [mirror](#), changed [block](#), and concurrent. [Pointer remapping](#) and [copy on write](#) are implementation techniques often used for the latter two classes. See [snapshot](#).

pointer copy

[Data Recovery] A [point in time copy](#) made using the [pointer remapping](#) technique.

pointer remapping

[Data Recovery] A technique for maintaining a [point in time copy](#) in which pointers to all of the source data and copy data are maintained.

When data is overwritten, a new location is chosen for the updated data, and the pointer for that data is remapped to point to it. If the copy is read-only, pointers to its data are never modified. See [Copy on Write](#).

policy (from RFC 3198)

1. [General] A definite goal, course or method of action to guide and determine present and future decisions.
2. [Management] Policies as a set of rules to administer, manage, and control access to network resources [RFC 3060].

Policies are implemented or executed within a particular context, such as policies defined within a business unit. See [policy goal](#) and [policy rule](#).

policy goal (from RFC 3198)

[Management] Goals are the objectives or desired state intended to be maintained by a [policy](#) system.

As the highest level of abstraction of policy, these goals are most directly described in business rather than technical terms. For example, a goal might state that a particular application operate on a network as though it had its own dedicated network, despite using a shared infrastructure. 'Policy goals' can include the objectives of a [service level agreement](#), as well as the assignment of resources to applications or individuals. A policy system may be created that automatically strives to achieve a goal through feedback regarding whether the goal (such as a service level) is being met.

policy processor

[Computer System] In an [intelligent device](#), the processor that schedules the overall activities.

[Policy](#) processors are usually augmented by additional processors, state machines, or sequencers that perform the lower-level functions required to implement overall policy.

policy rule (from RFC 3198)

[Management] A basic building block of a policy-based system; the binding of a set of actions to a set of conditions, where the conditions are evaluated to determine whether the actions are performed [RFC 3060].

port

1. [Network] An entrance to or exit from a storage network.
2. [Network] A [connection](#) point for a peripheral device or an application program.

Ports can be logical, physical or both. Examples include [Fibre Channel](#) Ports, [Internet Protocol](#) Suite Ports and [SCSI](#) Ports.

Port_ID

[Fibre Channel] Formally referenced as [N_Port_ID](#), a unique 24 bit address used for [frame](#) routing and assigned to an N_Port or [NL_Port](#).

The Port_ID hierarchy includes an 8-bit [Domain](#) ID (typically a [switch](#) number), an 8-bit Area ID (a port or group of switch ports) and an 8-bit Device ID (typically 00 for N_Ports or for NL_Ports, the [Loop Initialization](#) assigned [Arbitrated Loop Physical Address](#) (ALPA). The Port_ID of the Source Port ([S_ID](#)) and the Port_ID of the Destination Port ([D_ID](#)) is used in the [Fibre Channel](#) frame header for routing.

Port_Name

[Fibre Channel] A [Name Identifier](#) that is associated with a [Fibre Channel](#) port.

port bypass circuit

[Fibre Channel] A [circuit](#) that automatically opens and closes a [Fibre Channel arbitrated loop](#) so that nodes can be added to or removed from the loop with minimal disruption of operations.

Port bypass circuits are typically found in Fibre Channel hubs and disk enclosures.

port login

[Fibre Channel] The port-to-port login process by which [Fibre Channel](#) initiators establish sessions with targets.

Port_VF_ID

[Fibre Channel] A configurable [VF_ID](#) that is associated with any untagged [frame](#) received by a VF capable [Multiplexer](#).

POST

[Computer System] Acronym for [Power On Self Test](#).

post-process data deduplication

[Storage System] [Data deduplication](#) performed after the data to be deduplicated has been initially stored.

See [inline data deduplication](#).

power conditioning

[General] The regulation of power supplied to a system so that acceptable ranges of voltage and frequency are maintained.

Power [conditioning](#) is sometimes done by a [storage subsystem](#), but may also be an environmental requirement.

Power Distribution Unit (PDU)

[Computer System] An element or device which distributes power to and possibly monitors the power consumption of other devices in a system.

power efficiency

[Computer System] Synonym for [electrical efficiency](#).

Power On Self Test (POST)

[Computer System] A set of internally stored diagnostic programs run by intelligent devices when powered on, that verify the basic [integrity](#) of hardware before software is permitted to run on it.

power supply

[Computer System] A component which converts an AC or DC voltage input to one or more DC voltage outputs for the purpose of powering a system or subsystem.

Power supplies may be [redundant](#) and hot swappable.

power supply efficiency

[Storage System] The [electrical efficiency](#) of a [power supply](#), not including the fan power required to cool it.

In a perfect world, any power required to keep the power supply within specified operating temperature limits would be included in the calculation. In this one, the convention to measure efficiency without it saves much work and controversy.

Power Supply Unit (PSU)

[Computer System] Synonym for [power supply](#).

PP

[Data Security] Acronym for [Protection Profile](#).

PQI

[SCSI] Shorthand for [PCI Express Queuing Interface](#).

present

[Storage System] To cause to appear or to make available.

[RAID control software](#) and [volume](#) managers *present* virtual disks to host environments. Synonym for [export](#).

preservation

[Data Management] The processes and operations involved in ensuring the ability to read, interpret, authenticate, secure and protect against the loss of data or information throughout its lifecycle.

preservation object

[Long Term Retention] The basic unit of data or information that is preserved by a [preservation system](#).

The Archival Information Package (AIP) defined in Open Archival [Information System](#) (OAIS) is an example of a preservation object.

preservation system

[Long Term Retention] A repository that, either as its sole responsibility or as one of multiple responsibilities, undertakes all necessary actions for the [long-term preservation](#) of the data or information in its custody.

Primary storage

[Data Management] Data storage device, system, or service used to store data that is accessed frequently by applications.

primitive sequence

[Fibre Channel] In a data stream using [8B/10B encoding](#), an [ordered set](#) transmitted repeatedly and continuously until a specified response is received.

primitive signal

[Fibre Channel] In a data stream using [8B/10B encoding](#), an [ordered set](#) with a special meaning such as an [idle](#) or Receiver_Ready (R_RDY).

principal

[Management] [Data Security] Short for [security principal](#).

Priority-based Flow Control (PFC)

[Network] A [DCB](#) component that provides a mechanism for link level flow control on a per-priority basis for full-duplex links.

privacy breach

[Data Security] An event that exploits a [vulnerability](#) to reveal [PII](#), or creates a loss of control over PII.

private cloud

[Services] Delivery of [SaaS](#), [PaaS](#), [IaaS](#) and/or [DaaS](#) to a restricted set of customers, usually within a single organization.

Private Clouds are created due to issues of [trust](#).

private key

[Data Security] The cryptographic key in an [asymmetric cryptosystem](#) that is not made public.

private key cryptography

[Data Security] An [encryption](#) methodology in which the encryptor and decryptor use the same key, which must be kept secret. See [symmetric cryptosystem](#).

private loop

[Fibre Channel] A [Fibre Channel arbitrated loop](#) with no fabric attachment.

private loop device

[Fibre Channel] A [Fibre Channel arbitrated loop](#) device that does not support [fabric login](#).

privilege

[Data Security] A right granted to an individual, a program, or a process. [CNSSI-4009]

privileged user

[Data Security] A user who, by virtue of function or seniority, has been allocated powers within a system that are significantly greater than those available to the majority of users.

Such persons will include, for example, the system [administrator](#)(s), storage administrator(s), and network administrator(s) who are responsible for keeping the system available and may need powers to create new user profiles as well as add to or amend the powers and access rights of existing users.

process policy

[Fibre Channel] An error handling [policy](#) that allows an [N_Port](#) to continue processing data frames following detection of one or more missing frames in a [sequence](#).

Process_Associator

[Fibre Channel] A value in the Association_Header that identifies a process or a group of processes within a [node](#).

Communicating processes in different nodes use Process_Associators to address each other. Originating processes have [Originator](#) Process_Associators; responding processes have [Responder](#) Process_Associators.

profile

[Standards] A proper subset of a standard that supports [interoperability](#) across a set of products or in a specific application.

A profile is a vertical slice through a standard containing physical, logical and behavioral elements required for interoperability.

proprietary interconnect

proprietary I/O interconnect

[Storage System] An [I/O interconnect](#) (either a [host I/O interconnect](#) or a device I/O interconnect) whose transmission characteristics and protocols are the intellectual property of a single vendor, and require the permission of that vendor to be implemented in the products of other vendors.

See [open interconnect](#).

protected space

protected space extent

[Storage System] The storage space available for application data in a [physical extent](#) that belongs to a [redundancy group](#).

Protection Profile (PP)

[Data Security] An implementation-independent set of security functional and [assurance](#) requirements for a category of IT products that meet specific consumer needs.

PPs are most commonly associated with ISO 15408.

protocol

[General] A set of rules that control an interaction between two or more entities in communication with one another, e.g., [TCP](#) ports, [Fibre Channel FC-4](#) processes and polite humans.

Rules may specify the formats of a set of communication messages, and in what sequences they are expected to occur.

Protocol Data Unit (PDU)

1. [Network] A single message between two network nodes used for communication.
2. [iSCSI] The term used to describe one [iSCSI](#) message sent by either a [target](#) or an [initiator](#) in an iSCSI [connection](#).

provenance

[General] Information regarding an item's source, origin, custody and ownership.

provisioning

[Computer System] The process of initializing and equipping a system to prepare it to provide services.

Proxy Fabric

[Fibre Channel] In an IFR environment, the remote fabric associated with a [Proxy Nx_Port](#).

Proxy Nx_Port

[Fibre Channel] A role of an [Nx_Port](#) in an IFR environment.

From the perspective of a remote (Proxy) Fabric, an Nx_Port assumes the role of a Proxy Nx_Port.

PSU

[Computer System] Acronym for [Power Supply Unit](#).

public cloud

[Services] Delivery of [SaaS](#), [PaaS](#), [IaaS](#) and/or [DaaS](#) to a relatively unrestricted set of customers.

public key

[Data Security] A cryptographic key that is made public for purposes of using [asymmetric encryption](#) with an entity that has the [private key](#).

public key cryptography

[Data Security] Synonym for asymmetric [cryptography](#).

Public Key Infrastructure (PKI)

[Data Security] A collection of software, hardware, people and procedures that facilitate secure creation and management of digital certificates.

public loop

[Fibre Channel] A [Fibre Channel arbitrated loop](#) with an attachment to a fabric.

public loop device

[Fibre Channel] A [Fibre Channel arbitrated loop](#) device that supports [fabric login](#) and services.

pull technology

[Computer System] The transmission of information in response to a request for that information.

An example of a pull technology is polling. See [push technology](#).

pulverization

[Data Security] A method of sanitization that reduces devices or components to fine particles of a specified size.

Pulverization is related to shredding, but usually uses a grinding process as opposed to a cutting process. [ISO/IEC 27040]

purge

1. [Data Security] A class of sanitization that makes recovery infeasible using state of the art laboratory techniques, but which preserves the storage media in a potentially reusable state. [ISO/IEC 27040]
2. [Storage System] The process of returning a solid state storage device to a state in which subsequent writes execute, as closely as possible, as if the device had never been used and does not contain any valid data. See [FOB](#).

push technology

[Computer System] The transmission of information from a source or [initiator](#) without a request to the source to send that information.

An example of a push technology is an [SNMP trap](#). See [pull technology](#).

Q

QoS

[Management] Acronym for [Quality of Service](#).

Quality of Service (QoS)

[Management] A technique for managing computer system resources such as [bandwidth](#) by specifying user visible parameters such as message delivery time.

[Policy](#) rules are used to describe the operation of network elements to make QoS guarantees. Relevant standards for QoS in the [IETF](#) are the RSVP (Resource Reservation [Protocol](#)) and COPS (Common Open Policy Service) protocols. RSVP allows for the reservation of bandwidth in advance, while COPS allows routers and switches to obtain policy rules from a [server](#).

quiesce

[Data Recovery] To bring a device or an application to a [quiescent state](#).

quiescent state

[Data Recovery] An application or device state in which (a.) the application or device is able to operate, (b.) all of its data is consistent and stored on non-volatile storage, and (c.) processing has been suspended and there are no tasks in progress; i.e., all tasks have either been completed or not started.

quota

[File System] A limit that restricts the amount of a resource, such as disk space, that a user, group or [directory](#) structure may consume.

R

R

RADIUS

[Data Security] Acronym for [Remote Authentication Dial In User Service](#).

RAID

[Storage System] Acronym for [Redundant Array of Independent Disks](#).

The phrase Redundant Array of Independent Disks is adapted from the 1988 SIGMOD paper A Case for Redundant Arrays of Inexpensive Disks. In modern systems, RAID techniques are often applied to storage devices or technologies other than disk.

RAID 0

RAID Level 0

[Storage System] Synonym for [data striping](#).

RAID 1

RAID Level 1

[Storage System] Synonym for [mirroring](#).

RAID 2

RAID Level 2

[Storage System] A form of [RAID](#) in which an error detecting code computed on stripes of data on some of a RAID array's disks is stored on the remaining [disks](#) and serves as check data.

RAID 3

RAID Level 3

[Storage System] A form of [parity RAID](#) in which all [disks](#) are assumed to be rotationally synchronized, and in which the data [stripe size](#) is no larger than the exported [block](#) size.

RAID 4

RAID Level 4

[Storage System] A form of [parity RAID](#) in which the [disks](#) operate independently, the data [stripe size](#) is no smaller than the exported [block](#) size, and all parity [check data](#) is stored on one disk.

RAID 5

RAID Level 5

[Storage System] A form of [parity RAID](#) in which the [disks](#) operate independently, the data [stripe size](#) is no smaller than the exported [block](#) size, and parity [check data](#) is distributed across the [RAID array](#)'s disks.

RAID 6

RAID Level 6

[Storage System] Any form of [RAID](#) that can continue to execute read and write requests to all of a [RAID array](#)'s virtual [disks](#) in the presence of any two concurrent disk failures.

Several methods, including dual [check data](#) computations (parity and Reed Solomon), orthogonal [dual parity](#) check data and diagonal parity have been used to implement RAID Level 6.

RAID 10

[Storage System] [RAID](#) 10 uses both striping and mirroring.

RAID 10 may be implemented in two different ways with different properties. One stripes sets of mirrored [disk](#) drives, which is often called "RAID 1+0". The other mirrors sets of striped drives, which is often called "RAID 0+1".

RAID array

[Storage System] Shorthand for [Redundant Array of Independent Disks](#).

RAID-Z

[Storage System] A form of [RAID](#) implemented in the open source ZFS project.

RAIN

[Storage] Acronym for [Redundant Array of Independent Nodes](#).

raised floor

[General] An elevated floor providing space for cable runs between equipment cabinets and cold air flow for cooling.

Many mainframe systems are designed to intake cool air from the bottom and exhaust heat from the top of a closed cabinet system.

RAMdisk

[Storage System] A quantity of host system random access memory (RAM) managed by software and presented to applications as a high-performance disk.

RAMdisks generally emulate disk I/O functional characteristics, but unless augmented by special hardware to make their contents non-volatile, they cannot tolerate loss of power without losing data. See [solid state disk](#).

random I/O**random I/O load****random reads****random writes**

[Storage System] Any [I/O load](#) whose consecutively issued read and/or write requests do not specify adjacently addressed data.

The term random I/O is commonly used to denote any I/O load that is not sequential, whether or not the distribution of data locations is indeed random. Random I/O is characteristic of [I/O request-intensive](#) applications. See [sequential I/O](#).

random number

[General] A number having properties of randomness or unpredictability.

There are three basic classes of random number. Deterministic or pseudorandom numbers are generated by an algorithm that produces a predictable [sequence](#) of values from an initial value called a seed. Cryptographically secure random numbers are produced in a sequence that, while deterministic, cannot be feasibly discovered or computed by examination of previous numbers in the sequence. Nondeterministic generators incorporate input from some unpredictable physical source that is outside human control.

random relative offset

[Fibre Channel] A transmission control algorithm in which the frames containing the subblocks that comprise a [block](#) of information may be transmitted in any order.

rank

1. [Storage System] A set of [physical disk](#) positions in an enclosure, usually denoting the disks that are or can be members of a single [array](#).
2. [Storage System] The set of corresponding [target](#) identifiers on all of a [controller](#)'s device I/O interconnects.
3. [Storage System] Synonym for a [stripe](#) in a [redundancy group](#).

Because of the diversity of meanings attached to this term by [disk subsystem](#) developers, SNIA publications make minimal use of it.

rapid elasticity

[Computer System] Quick scaling of resources and capabilities to meet expansion and contraction of demand.

To the consumer, the capabilities available for [provisioning](#) often appear to be unlimited and available for purchase in any quantity at any time.

rapid provisioning

[Computer System] Quickly and automatically deploying services in response to requests.

RAS

1. [Computer System] Acronym for Reliability, [Availability](#), and Serviceability.
2. [Windows] Acronym for Remote Access [Server](#) (Windows NT dialup networking server).

raw capacity

[Storage System] The sum total amount of addressable capacity of the storage devices in a storage system.

The addressable capacity of a storage device is commonly understood to be the number of bytes available to be written via [SCSI](#) or equivalent [protocol](#). It does not include unaddressable space, ECC ([error correcting code](#)) data, remap areas, inter-[sector](#) gaps and so on. See [theoretical capacity](#).

raw partition

[Storage System] A disk [partition](#) not managed by a [volume manager](#).

The term raw partition is frequently encountered when discussing database systems because some database system vendors recommend volumes or files for underlying database storage, while others recommend direct storage on raw partitions.

raw partition backup

[Data Recovery] A bit-by-bit copy of a [partition](#) image.

A [raw partition backup](#) incorporates no information about the objects contained on the partition, and hence cannot be used for individual object [restoration](#). See [disk image backup](#).

RBAC

[Data Security] Acronym for [Role-Based Access Control](#).

read/write head

[Storage System] The magnetic or optical recording device in a disk.

Read/write heads are used both to write data by altering the recording [media](#)'s state, and to read data by sensing the alterations. Disks typically have read/write heads, unlike tapes, in which reading and writing are often done using separate heads.

ready idle

[Storage System] Synonym for [idle](#).

real time copy

[Storage System] Deprecated synonym for [mirroring](#).

real time data deduplication

[Storage System] Synonym for [inline data deduplication](#).

rebuild

rebuilding

[Storage System] The [regeneration](#) and writing onto one or more replacement disks of all of the user data and [check data](#) from a failed disk in a mirrored or [RAID array](#).

In most arrays, a rebuild can occur while applications are accessing data on the array's virtual disks.

receiver

1. [General] An [interconnect](#) or network device that includes a detector and signal processing electronics.
2. [General] A [circuit](#) that converts an optical or electrical [media](#) signal to a (possibly retimed) electrical [serial](#) logic signal.

3. [Fibre Channel] The portion of a Link_Control_Facility dedicated to receiving an encoded bit stream, converting the stream into transmission characters, and [decoding](#) the characters using the rules specified by [FC-0](#).

receptacle

[Network] The stationary (female) half of the [interface connector](#) on a [transmitter](#) or [receiver](#).

reconstruction

[Storage System] Synonym for [rebuilding](#).

Recorded Volume Serial Number (RVSN)

[Data Recovery] Synonym for [media ID](#).

recovery

[Data Recovery] The recreation of a past [operational state](#) of an entire application or computing environment.

Recovery is required after an application or computing environment has been destroyed or otherwise rendered unusable. It may include [restoration](#) of application data, if that data had been destroyed as well.

Recovery Point Objective (RPO)

[Data Recovery] The maximum acceptable time period prior to a failure or disaster during which changes to data may be lost as a consequence of [recovery](#).

Data changes preceding the failure or disaster by at least this time period are preserved by recovery. Zero is a valid value and is equivalent to a "zero data loss" requirement.

Recovery Time Objective (RTO)

[Data Recovery] The maximum acceptable time period required to bring one or more applications and associated data back from an outage to a correct [operational state](#).

R

Redfish

[Management] A [DMTF](#) open standard specification and schema that specifies a RESTful interface that utilizes JSON and [OData](#) for managing scalable hardware platforms.

Redfish schema

[Management] The representation of [Redfish](#) resources and data model using CSDL.

Redfish service

[Management] An [OData service](#) that conforms to requirements of the Redfish specification.

Redfish service entry point

[Management] A [URI](#) through which a particular instance of a Redfish Service is accessed.

reduced mode

[Storage System] Synonym for [degraded mode](#).

reduction

[Storage System] The removal of a [member disk](#) from a [RAID array](#), placing the array in [degraded mode](#).

Reduction most often occurs because of member disk failure, however, some RAID implementations allow reduction for system management purposes.

redundancy

[General] The inclusion of extra components of a given type in a system (beyond those required by the system to carry out its function) for the purpose of enabling continued operation in the event of a component failure.

redundancy group

[Storage System] A collection of extents organized for the purpose of providing [data protection](#).

Within a [redundancy](#) group, a single type of data protection is employed. All of the usable storage capacity in a redundancy group is protected by [check data](#) stored within the group, and no

usable storage external to a redundancy group is protected by check data within it.

redundancy group stripe

[Storage System] A set of sequences (strips) of correspondingly numbered [physical extent](#) blocks in each of the physical extents comprising a [redundancy group](#).

The [check data](#) blocks in a redundancy group [stripe](#) protect the [protected space](#) in that stripe.

redundancy group stripe depth

[Storage System] The number of consecutively numbered [physical extent](#) blocks in one physical extent ([strip](#)) of a [redundancy group stripe](#).

In the conventional striped data [mapping](#) model, redundancy group [stripe depth](#) is the same for all stripes in a redundancy group.

redundant (components)

[Computer System] Components of a system that have the capability to substitute for each other when one of the components fails, so that the system can continue to perform its function.

In storage subsystems, power distribution units, power supplies, cooling devices, and controllers are often configured to be redundant. The disks comprising a [mirror](#) set are redundant. A [parity RAID array](#)'s [member](#) disks are redundant, since surviving disks can collectively replace the function of a failed disk.

redundant (configuration, system)

[Computer System] A system or [configuration](#) of a system in which [failure tolerance](#) is achieved by the presence of [redundant](#) instances of all components that are critical to the system's operation.

Redundant Array of Independent Disks (RAID)

[Storage System] A [disk array](#) in which part of the physical storage capacity is used to store [redundant](#) information about user data stored on the remainder of the storage capacity.

The redundant information enables [regeneration](#) of user data in the event that one of the array's [member](#) disks or the [access path](#) to it fails. Although it does not conform to this definition, [disk striping](#) is often referred to as RAID ([RAID Level 0](#)). See [Berkeley RAID levels](#).

Redundant Array of Independent Nodes

[Storage] A collection of networked [server](#) nodes with software that provides and maintains pools of highly available storage capacity.

reference data

[Data Management] Synonym for [fixed content](#).

reference information

[Data Management] Synonym for [fixed content](#).

refreshment

1. [General] Synonym for beer.
2. [Long Term Retention] A type of [migration](#) where the contents of some [media](#) are copied onto newer media of the same type.

regeneration

[Storage System] Recreation of user data from a failed disk in a [RAID array](#) using [check data](#) and user data from surviving members.

Regeneration may also be used to recover data from an unrecoverable [media](#) error. Data in a [parity RAID array](#) is regenerated by computing the exclusive OR of the contents of corresponding blocks from the array's remaining disks. Data in a [RAID Level 6](#) array is regenerated by choosing the more convenient of two parity algorithms and executing it.

registered state change notification

[Fibre Channel] A [Fibre Channel switch](#) function that allows notification to registered nodes if a change occurs to other specified nodes.

rejoin mirror

[Storage System] To bring a split [mirror](#) component back into the mirror.

When the [resilvering](#) process completes, the mirror component becomes identical to all mirror components in the mirror.

rekeying

[Data Security] The process of changing the key used for an ongoing communication session.

relative offset

[Fibre Channel] A displacement, expressed in bytes, used to divide a quantity of data into blocks and subblocks for transmission in separate frames.

Relative offsets are used to reassemble data at the [receiver](#) and verify that all data has arrived.

relative offset space

[Fibre Channel] A numerical range defined by a sending upper level [protocol](#) for an [information category](#).

The range starts at zero, representing the upper level-defined-origin, and extends to a highest value. [Relative offset](#) values are required to lie within the appropriate relative offset space.

Remote Authentication Dial In User Service (RADIUS)

[Data Security] An [authentication](#) and accounting [protocol](#) used by many Internet Service Providers (ISPs).

Information such as username and [password](#) is entered when a [connection](#) is made. This information is passed to a RADIUS [server](#) that verifies the information in order to authorize access to the system. RADIUS is defined in [RFC 2865](#).

removable media library

[Backup] Synonym for [library](#).

removable media storage device

[Storage System] A [storage device](#) designed so that its storage volumes can be readily removed and inserted.

Tapes, CD-ROMs, and optical disks are removable [media](#) devices.

replacement disk

[Storage System] A disk available for use as or used to replace a failed [member disk](#) in a [RAID array](#).

Replacement Unit (RU)

[General] A component or collection of components in a system that are always replaced (swapped) as a unit when any part of the collection fails.

Replacement units may be field replaceable, or they may require that the system of which they are part be returned to a factory or repair depot for replacement. Field replaceable units may be customer replaceable, or their replacement may require trained service personnel. Typical replacement units in a [disk subsystem](#) include disks, [controller](#) logic boards, power supplies, cooling devices, and cables. Replacement units may be cold swappable, warm swappable, or hot swappable.

replay attack

[Data Security] An [attack](#) in which a valid data transmission is maliciously or fraudulently repeated, either by the [originator](#) or by an adversary who intercepts the data and retransmits it.

replica

1. [Data Recovery] A general term for a copy of a collection of data. See [duplicate](#), [point in time copy](#), [snapshot](#).
2. [Data Recovery] An image of data usable by one or more applications without an intermediate restore process.
See [backup copy](#).

replicate

1. [Data Recovery] A general term for a copy of a collection of data. See [duplicate](#), [point in time copy](#), [snapshot](#).
2. [Data Recovery] The action of making a replicate as defined above.

replication link

[Storage System] A physical and logical [connection](#) that transports data and replication control commands between primary and secondary sites.

replication set

[Storage System] A pair of volumes that have a replication relationship.

A replication set consists of a primary volume and a secondary volume that are physically separated. The replication set also defines how the primary and secondary volumes are connected and how replication ought to proceed.

Representational State Transfer (REST)

[Services] A specific set of principles for defining, [addressing](#) and interacting with resources addressable by URIs.

Architectures that follow these principles are said to be RESTful. The principles include: abstraction of state into resources and a uniform set of representations and operations (e.g., [HTTP](#) verbs like GET and PUT as the only means to manipulate a resource). RESTful interfaces are contrasted with Web Services interfaces such as [WBEM](#), which tend to be RPC-like.

repudiation

[Data Security] The act of a [principal](#) in denying, disowning or disavowing an act, event or transaction.

Request For Comment (RFC)

[Data Security] Internet -related specifications, including standards, experimental definitions, informational documents and best practice definitions, produced by the [IETF](#).

request intensive (application)

[Computer System] A characterization of I/O intensive applications.

Request-intensive applications' I/O requests are usually randomly addressed and often specify a small amount of data for transfer.

reserved (field)

1. [General] In a standard, a field in a data structure set aside for future definition.

Some standards prescribe implementation behavior with respect to reserved fields (e.g., originators of data structures containing reserved fields must zero fill them; consumers of data structures containing reserved fields must ignore them, etc.); others do not.

2. [Fibre Channel] A field filled with binary zeros by a [source N_Port](#) and ignored by a destination N_Port.

Each bit in a reserved field is denoted by "r" in the [Fibre Channel](#) standards. Future enhancements to Fibre Channel Standards may define usages for reserved fields.

Implementations should not check or interpret reserved fields. Violation of this guideline may result in loss of compatibility with future implementations that comply with future enhancements to Fibre Channel Standards.

resiliency

[Storage] The ability of a [storage element](#) to preserve [data integrity](#) and [availability](#) of access despite the unavailability of one or more of its storage devices.

resilvering

[Data Recovery] [Storage Systems] Synonym for [mirror resynchronization](#).

resource pooling

[Computer System] [Aggregation](#) of a provider's computing resources to serve multiple consumers using a multitenant

model, with physical and virtual resources dynamically assigned and reassigned on demand.

responder

1. [General] [iSCSI] In a negotiation or [exchange](#), the party that responds to the [originator](#) of the negotiation or exchange.
2. [Fibre Channel] With reference to an Exchange, the [Nx_Port](#) that receives the [frame](#) that caused the Exchange to become open.

Responder Exchange Identifier (RX_ID)

[Fibre Channel] An identifier assigned by a [responder](#) to identify an [exchange](#).

An RX_ID is meaningful only to the responder that originates it.

REST

[Services] Abbreviation for [Representational State Transfer](#).

restoration

[Data Recovery] Synonym for [recovery](#).

retention period

1. [Data Recovery] The length of time that a [backup](#) image should be kept.
2. [File System] In some file systems, such as that shipped with IBM Corporation's OS/390 operating system, a property of a file that can be used to implement backup and data [migration](#) policies.
3. [Data Management] The length of time a [compliance volume](#) or file must be maintained undeleted and unchanged.

retention policy

[Data Management] A [policy](#) governing when and for how long a record must be retained by a storage system.

This may be a rule that applies to groups or categories of records, or may be specified for individual records. The policy may be time or event based.

retimer

[Computer System] A [circuit](#) that uses a clock independent of the incoming signal to generate an outbound signal.

return loss

[Data Communication] The ratio of the strength of a returned signal to that of the [incident](#) signal that caused it.

In electrical circuits, return loss is caused by impedance discontinuities. Optical return loss is caused by index of refraction differences.

reverse rejoin mirror

[Storage System] An operation performed on a split [mirror](#) component, in order to use its data as the basis for the mirror as a whole.

When a component is reverse rejoined, all mirror components in the mirror become identical to the previously split mirror component as a result of the resilver process.

RFC

[Data Security] Acronym for [Request For Comment](#).

risk

[Data Security] The potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss or damage to the assets [IEEE 13335-1:1996].

risk acceptance

[Data Security] Decision to accept a risk.

[ISO/IEC 27000]

risk analysis

[Data Security] The process of identifying security risks, determining their magnitude, and identifying areas needing safeguards [IEEE 13335-1:1996].

risk management

[Data Security] The process of assessing and quantifying risk and establishing an acceptable level of risk for the organization [IEEE 13335-1:1996].

risk treatment

[Data Security] Process of selection and implementation of measures to modify risk.

[ISO/IEC 27000]

robot**robotic media handler**

[Storage System] The mechanical component of a [library](#) which moves removable volumes among drives and entry/exit slots.

Role-based Access Control (RBAC)

[Data Security] An [access control](#) method that assigns permissions to roles that [mirror](#) the organization and policies of an organization.

rollback to snapshot

1. [System] The process of resetting a [volume](#)'s data to become identical to a [snapshot](#) taken of that volume.
2. [File System] In [LTFS](#), the process of modifying the index to match a previous version of the index.

rotational latency

[Storage System] The interval between the end of a disk seek and the time at which the starting [block](#) address specified in the [I/O request](#) passes the disk head.

Exact rotational latencies for specific sequences of I/O operations can only be obtained by detailed [disk drive](#) simulation or measurement. The simplifying assumption that on average, requests wait for half a disk revolution time of rotational [latency](#) works well in practice. Half of a disk revolution time is therefore defined to be the average rotational latency.

routing function

[Fibre Channel] An entity that resides in an [Inter-Fabric Router](#) and is responsible for the forwarding of frames between independent Fabrics including the translation of N_Port_ID's to present the Proxy N_Ports to the local Fabrics.

row

[Storage System] The set of blocks with corresponding [physical extent block](#) addresses in each of an [array's member](#) physical extents.

The concept of rows is useful for [locking](#) the minimal amount of data during a [RAID array](#) update so as to maximize the potential for [parallel](#) execution.

RPO

[Data Recovery] Acronym for [Recovery Point Objective](#).

RSA

[Data Security] Acronym for both a [public key](#) algorithm and a corporation in the business of algorithm design, derived from the names of its founders (Rivest, Shamir & Adelman).

RSCN

[Fibre Channel] Acronym for [Registered State Change Notification](#).

RTO

[Data Recovery] Acronym for [Recovery Time Objective](#).

RU

[General] Acronym for Replaceable Unit.

See [CRU](#), [FRU](#).

run length

[Data Communication] The number of consecutive identical bits in a transmitted signal. For example, the pattern 0011111010 has run lengths of 2, 5, 1, 1, and 1.

running disparity

[Fibre Channel] In a data stream using [8B/10B encoding](#), the cumulative [disparity](#) (positive or negative) of all previously issued transmission characters.

RVSN

[Data Recovery] Acronym for [Recorded Volume Serial Number](#).

R

S

S

S_ID

[Fibre Channel] The Source_ID, a three-byte field that contains the [address identifier](#) of the source [Nx_Port](#).

SA

[Data Security] Acronym for [Security Association](#).

SaaS

[Services] Acronym for [Software as a Service](#).

SAM

[SCSI] Acronym for [SCSI Architecture Model](#).

The SCSI Architecture Model is developed and owned by the [T10](#) working group of [ANSI](#). SAM has undergone numerous revisions, each being consecutively named as SAM-2, SAM-3 and so on, the latest revision being SAM-5.

SAN

1. [Fibre Channel] [iSCSI] [Network] [Storage Area Network](#).
This is the normal meaning in SNIA documents.
2. [Computer System] Acronym for [Server](#) Area Network, which connects one or more servers.
3. [Computer System] Acronym for System Area Network, an interconnected set of system elements.

sanitization

[Data Security] A process or method to sanitize.
[ISO/IEC 27040]

sanitize

[Data Security] Render access to target data on storage media infeasible for a given level of effort. [ISO/IEC 27040]

Clear, purge, and destruct are actions that can be taken to sanitize storage media. See [media sanitization](#).

SAS

[SCSI] Acronym for [Serial Attached SCSI](#).

SAS Expander

[SCSI] Short for [Serial Attached SCSI Expander](#).

SAS Protocol Layer (SPL)

[SCSI] The layer of the [SAS interconnect](#) that comprises the [Serial SCSI Protocol](#) (SSP), the Serial [ATA](#) Tunneled Protocol (STP) and the Serial Management Protocol (SMP).

SATA

[Storage System] Acronym for [Serial Advanced Technology Attachment](#).

saturated disk

[Storage System] A disk whose instantaneous [I/O load](#) is as great as or greater than its capability to satisfy the requests comprising the load.

Mathematically, a saturated disk's I/O queue eventually becomes indefinitely long. In practice, however, user reaction or other system factors generally reduce the rate of new request arrivals for a saturated disk.

scale

[Computer System] To grow or support growth in such a way that all capabilities of the system remain in constant ratio to each other.

A [storage subsystem](#) whose [data transfer capacity](#) increases by the addition of buses as its storage capacity increases by the addition of disks is said to scale.

schema

1. [Management] A collection of information models or data models.
2. [Data Management] Data that describes the organization and format of other data.

scrambling

[Data Communication] Modifying data by XORing each bit with a pattern generated by a linear feedback shift register to minimize repetitive character patterns.

script

1. [Storage System] A parameterized list of primitive [I/O interconnect](#) operations intended to be executed in [sequence](#). Often used with respect to ports, most of which are able to execute scripts of I/O commands autonomously (without [policy processor](#) assistance).
2. [Computer System] A sequence of instructions intended to be parsed and carried out by a command line interpreter or other scripting language.
Perl, VBScript, JavaScript and Tcl are all scripting languages.
See [Command Line Interface](#).

SCSI

[SCSI] Acronym for [Small Computer System Interface](#).

SCSI adapter

[SCSI] An [adapter](#) that connects an [intelligent device](#) to a [SCSI interconnect](#).

See [HBA](#), [host bus adapter](#).

SCSI address

[SCSI] The full address used by a computer to communicate with a [SCSI device](#), including an [adapter](#) number (required with computers configured with multiple SCSI adapters), and the [target](#) ID of the device.

SCSI addresses do not include [logical unit number](#), because those are not used for communication.

SCSI Architecture Model (SAM)

[SCSI] An [ANSI](#) standard that defines the generic requirements and overall framework in which other [SCSI](#) standards are defined.

New generations of this standard are identified by a numeric suffix; for example the second generation standard is SAM2.

SCSI bus

[SCSI] Deprecated synonym for [SCSI interconnect](#).

SCSI Device

[SCSI] The [SAM-2](#) term for an entity that contains other [SCSI](#) entities.

For example, a SCSI [Initiator](#) Device contains one or more SCSI Initiator Ports and zero or more application clients.

SCSI Enclosure Services (SES)

[SCSI] A standard for management of environmental factors such as temperature, power, voltage, etc.

SCSI Initiator Port

[SCSI] The [initiator](#) endpoint of an [I_T nexus](#).

SCSI interconnect

[SCSI] A [serial](#) or [parallel interconnect](#) that implements a [SCSI](#) transport standard.

The number of SCSI initiator ports and SCSI target ports which may be connected on a [SCSI bus](#) is dependent upon the particular transport standard. See [initiator](#), [target](#).

SCSI Media Changer Commands (SMC)

[SCSI] A standard for [media changer](#) devices (i.e., libraries).

SCSI Over PCI Express (SOP)

[SCSI] A protocol to transport [SCSI](#) operations over PCI Express.

SCSI Parallel Interface (SPI)

[SCSI] The family of [SCSI](#) standards that define the characteristics of the [parallel](#) version of the SCSI interface.

Several versions of SPI, known as SPI, SPI2, SPI3, etc., have been developed. Each version provides for greater performance and functionality than preceding ones.

SCSI port

[SCSI] The [SCSI](#) term for an entity in a [SCSI Device](#) that provides the SCSI functionality to interface with a service delivery subsystem or transport.

SCSI Stream Commands (SSC)

[SCSI] A standard for sequential-access devices (i.e., tape drives).

SCSI target port

[SCSI] The [target](#) endpoint of an [I T nexus](#).

SCSI Trade Association (STA)

[General] A trade association incorporated in 1996 to promote all forms of [SCSI](#) technology in the market.

See <http://www.scsita.org/>.

SDDC

[Management] Acronym for [Software Defined Data Center](#).

SDH

[Network] Acronym for [Synchronous Digital Hierarchy](#).

SDS

[Storage] Shorthand for [software-defined storage](#).

secret key

[Data Security] A key used in a [symmetric cryptosystem](#) to both encrypt and decrypt data.

The key must remain confidential to the using parties to ensure the security of the cryptosystem.

sector

[Storage System] The unit in which data is physically stored and protected against errors on a [fixed block architecture](#) disk.

A sector typically consists of a [synchronization](#) pattern, a header field containing the block's address, data, a [checksum](#) or [error correcting code](#), and a trailer. Adjacent sectors are often separated by information used to assist in track centering. Most often, each sector holds a block of data. See [disk block](#).

secure hash

[Data Security] An algorithm that generates a fixed-size [digest](#) from its input (e.g., a message).

The algorithm has the properties that different inputs are extraordinarily unlikely to yield the same digest, small changes in its input lead to large changes in its output, and it is computationally intractable to generate an input that yields the same digest as another given input.

secure multi-tenancy

A type of [multi-tenancy](#) that employs security controls to explicitly guard against data breaches and provides validation of these controls for proper governance. [ISO/IEC 27040]

Secure multi-tenancy exists when the risk profile of an individual tenant is no greater than it would be in a dedicated, single-tenant environment. In very secure environments even the identity of the tenants is kept secret. See [multi-tenancy](#).

Secure Remote Password (SRP)

[Data Security] An [authentication](#) and [key exchange](#) system.

SRP is standardized by the [Internet Engineering Task Force](#) and described in [RFC 2945](#).

Secure Sockets Layer (SSL)

[Data Security] A suite of cryptographic algorithms, protocols and procedures used to provide security for communications used to access the world wide web.

The characters "https:" at the front of a URL cause SSL to be used to enhance [communications security](#). More recent versions of SSL are known as [TLS](#) (Transport Level Security) and are standardized by the [Internet Engineering Task Force](#) (IETF).

SSL is a predecessor of TLS and is considered a vulnerability if it is supported in a product.

See also [SSL](#).

Security Association (SA)

[Data Security] A simplex "[connection](#)" that affords security services to the traffic carried by it.

To secure typical, bi-directional communication between two hosts, or between two security gateways, two Security Associations (one in each direction) are required. In [IPsec](#), a security association is uniquely identified by a triple consisting of a [Security Parameters Index](#) (SPI), an [IP](#) Destination Address, and a security [protocol](#) identifier ([Authentication Header](#) or [Encapsulating Security Payload](#)).

security domain

[Data Security] A collection of people and systems under the control of a single authority, often with a single security [policy](#).

security incident

[Data Security] A single or a series of unwanted or unexpected events that have a significant probability of compromising business operations and threatening [information security](#).

security principal

[Data Security] A securely identified and verified entity.

security safeguards

[Data Security] The protective measures and controls that are prescribed to meet the security requirements specified for a system.

Safeguards may include but are not necessarily limited to: hardware and software security features, operating procedures, [accountability](#) procedures, access and distribution controls, management constraints, personnel security, and physical structures, areas, and devices. Also called safeguards (without the adjective).

security strength

[Data Security] A measure of the computational complexity associated with defeating the protection conveyed by a given [cryptographic algorithm](#).

Security strength is often expressed as a number of bits.

Security Target (ST)

[Data Security] A set of security functional and [assurance](#) requirements and specifications to be used as the basis for evaluation of an identified product or system, most commonly associated with ISO 15408.

Self-contained Information Retention Format (SIRF)

[Long Term Retention] A self-describing container format, developed by the SNIA, appropriate for the long-term storage of digital information.

self encrypting drive

[Storage System] A type of [self encrypting storage device](#).

self encrypting storage device

[Storage System] A [storage device](#) that has the native ability to encrypt all user data written to and decrypt the same data read from it, and that prevents access until a credential is supplied.

Tape drives, disk drives and other types of storage devices may all be designed to be self encrypting storage devices.

self-signed certificate

[Data Security] A [public key certificate](#) whose [digital signature](#) may be verified by the public key contained within the certificate.

The signature on a self-signed certificate protects the integrity of the data, but does not guarantee authenticity of the information. The trust of self-signed certificates is based on the secure procedures used to distribute them. [NIST SP 800-57 Part 1]

sensitive information

[Data Security] Information that could adversely affect the interest or the conduct of an organization's business or activities, or the [privacy](#) to which individuals are entitled.

SEQ_ID**Sequence Identifier**

[Fibre Channel] A number transmitted with each [data frame](#) in a [sequence](#) that identifies the frame as part of the sequence.

sequence

[Fibre Channel] A set of [Fibre Channel](#) data frames with a common Sequence_ID ([SEQ_ID](#)), corresponding to one message element, [block](#), or [Information Unit](#).

Sequences are transmitted from the [sequence initiator](#) to the [sequence recipient](#).

sequence initiative

[Fibre Channel] A [Fibre Channel](#) signaling feature that designates which end of an [exchange](#) has authority to send the next [sequence](#).

Sequence Initiator

[Fibre Channel] An [Nx_Port](#) that initiates a [sequence](#) and transmits data frames to a [destination Nx_Port](#).

Sequence Recipient

[Fibre Channel] An [N_Port](#) or [NL_Port](#) that receives Data frames from a [Sequence Initiator](#) and, if applicable, transmits responses (Link Control frames) to the Sequence Initiator.

Sequence Status Block

[Fibre Channel] A data structure that tracks the state of a [sequence](#).

Both Sequence Initiators and Sequence Recipients have Sequence Status Blocks for each active sequence.

sequential I/O

sequential I/O load

sequential reads

sequential writes

[Storage System] An [I/O load](#) consisting of consecutively issued read or write requests to adjacently addressed data.

Sequential I/O is characteristic of data transfer intensive applications. See [random I/O](#).

SERDES

[Computer System] Short for [Serializer Deserializer](#).

serial (transmission)

[General] The transmission of data bits one at a time over a single link.

serial adapter

[Computer System] An [adapter](#) that connects an [intelligent device](#) to an RS232 or RS425 [serial](#) communications link.

Serial adapters are sometimes used by storage subsystems, filers, and other intelligent devices to connect to serial consoles for management purposes. See [host adapter](#).

Serial Advanced Technology Attachment (SATA)

[Storage System] A version of the [ATA](#) interface that uses a [serial connection](#) architecture.

Serial Attached SCSI (SAS)

[SCSI] A [SCSI](#) interface standard that provides for attaching hosts to SCSI devices, including SAS and [SATA](#) disk and tape drives.

[INCITS](#) Technical Committee [T10](#) is responsible for the national ([ANSI](#)) and international ([ISO](#)) standards for SAS. See www.t10.org.

Serial Attached SCSI Expander

[SCSI] A switching device that uses [virtualization](#) to allow multiple [SAS](#) devices to be connected to each [initiator](#) port.

serial console

[Computer System] A real or emulated communication terminal used by humans to manage an [intelligent device](#).

[Serial](#) consoles connect to the devices' virtual or physical serial adapters.

S

Serializer Deserializer (SERDES)

[Computer System] A mechanism for converting data from [parallel](#) to [serial](#) form and from serial to parallel form.

server

1. [Computer System] An [intelligent device](#), usually a computer, that provides services to other intelligent devices, usually other computers or appliances. See [client](#).
2. [Computer System] An asymmetric relationship with a second party (a client) in which the client initiates requests and the server responds to those requests.

server based virtualization

[Computer System] Synonym for [host based virtualization](#).

Server Message Block (protocol) (SMB)

[Network] A [network file system](#) access [protocol](#) designed primarily used by Windows clients to communicate file access requests to Windows servers.

Current versions of the SMB protocol are referred to as [CIFS](#), the [Common Internet File System](#).

serverless backup

[Data Recovery] A [backup](#) methodology that utilizes a device other than the [server](#) to copy data without using the [LAN](#).

The copy may be performed by a network-attached [controller](#) (e.g., utilizing [SCSI](#) Extended Copy), by an [appliance](#) within the [SAN](#), or by a Backup Server.

Service Incident Standard (SIS)

[Management] A [DMTF](#) standard that defines how a support or help desk [incident](#) is processed.

Service Level Agreement (SLA)

[General] An agreement between a service provider, such as an IT department, an internet services provider, or an [intelligent device](#) acting as a [server](#), and a service consumer.

A service level agreement defines parameters for measuring the service, and states quantitative values for those parameters.

Service Level Objective (SLO)

[General] A [partition](#) of an [SLA](#) consisting of individual metrics and [operational](#) information to enforce and/or [monitor](#) the SLA.

Service Level Objectives may be defined as part of an SLA, an SLS, or in a separate document. Each is a set of parameters and their values. The actions of enforcing and reporting monitored [compliance](#) can be implemented as one or more policies. See [Service Level Agreement](#).

Service Location Protocol (SLP)

[Management] An [IETF](#) standards track [protocol](#) that provides a framework to allow networking applications to dynamically discover the existence, location, and [configuration](#) of networked services in enterprise networks.

service root

[Management] A particular resource that is directly accessed via the [Redfish service entry point](#).

This resource serves as a starting point for locating and accessing the other resources and associated metadata that together make up an instance of a Redfish service.

SES

1. [SCSI] Acronym for [SCSI Enclosure Services](#).
2. [Standards] Acronym for [Solution Exchange Standard](#).

SF_ID

[Fibre Channel] Abbreviation for Source [Fabric Identifier](#).

SHA-x

[Data Security] Acronym for [Secure Hash](#).

share

[File System] A resource such as a data [volume](#) or a printer device made available for use by users on other computer systems.

For example, a printer or a collection of files stored in a single [directory tree](#) on a [file server](#) may be made available as a share. [CIFS](#) clients, which include most networked personal computers, typically map a share to a [drive letter](#).

shared secret

[Data Security] A pre-shared key that has been distributed to communicating parties prior to beginning of an encrypted communication.

shelf

[Storage System] A modular enclosure for storage devices such as disks and tapes.

Storage shelves usually contain power supplies and cooling devices, and have pre-wired backplanes that carry power and [I/O interconnect](#) signals to the devices mounted in them. See [canister](#).

shielded enclosure

[Data Security] A room or container designed to attenuate electromagnetic radiation.

SIA

1. [General] Acronym for Semiconductor Industries Association.
2. [SCSI] Acronym for [SCSI](#) Industry Association.

Simple Network Management Protocol (SNMP)

[Network] [Standards] An [IETF protocol](#) for monitoring and managing systems and devices in a network.

The data being monitored and managed is defined by a [MIB](#). The functions supported by the protocol are the request and retrieval of data, the setting or writing of data, and *traps* that signal the occurrence of events.

single (component) configuration

[General] A [configuration](#) in which the referenced component is not redundant.

See [redundant](#) (component).

single ended (signaling)

[SCSI] An electrical signaling technique in which all control and data signals are represented by a voltage difference from a common ground.

See [differential](#).

single instance storage

[Storage System] A form of data deduplication that operates at a granularity of an entire file or data object.

See [data deduplication](#), [subfile data deduplication](#).

single mode (fiber optic cable)

[Fibre Channel] [Network] A fiber optic cabling specification that provides for up to 10 kilometer distance between devices.

single mode fibre

[Fibre Channel] Optical fiber that is designed for the transmission of a single ray or mode of light as a carrier.

[Single mode fibre](#) transmission is typically used for long-distance signal transmission.

Single Point Of Failure (SPOF)

[General] One component or path in a system, the failure of which would make the system inoperable.

Single Sign On (SSO)

[Data Security] A form of centralized [authentication](#) employing a single set of [credentials](#) that are used transparently to perform subsequent authentications on behalf of the users.

SIRF

[Long Term Retention] Acronym for [Self-contained Information Retention Format](#).

SIS

1. [Management] [Standards] Acronym for [Service Incident Standard](#).
2. [Storage System] Acronym for [Single Instance Storage](#).

SLA

[General] Acronym for [Service Level Agreement](#).

SLO

[General] Acronym for [Service Level Objective](#).

SLP

[Management] Acronym for [Service Location Protocol](#).

Small Computer System Interface (SCSI)

[SCSI] A collection of [ANSI](#) standards and proposed standards that define I/O interconnects primarily intended for connecting storage subsystems or devices to hosts through [host bus adapters](#).

Originally intended primarily for use with small (desktop and desk-side workstation) computers, SCSI has been extended to serve most computing needs, and is arguably the most widely implemented I/O interconnect in use today.

small read request**small write request****small I/O request**

[Storage System] An I/O, read, or write request that specifies the transfer of a relatively small amount of data.

‘Small’ usually depends on the context, but most often refers to 8 KBytes or fewer. See [large I/O request](#).

SMB

[File System] [Network] Acronym for [Server Message Block](#).

SMI

1. [Management] The [Storage Networking Industry Association](#)’s (SNIA) Storage Management Initiative (SMI).

SMI develops and standardizes interoperable storage management technologies, including providing conformance testing for products.

2. [Fibre Channel] [Management] [Network] Acronym for [Structure of Management Information](#).

SMI-S

[Standards] Acronym for *Storage Management Initiative Specification*.

SMPTE

[Standards] Acronym for [Society of Motion Picture and Television Engineers](#).

snapshot

[Data Management] A [point in time copy](#) of a defined collection of data.

Clones and snapshots are full copies. See [delta snapshot](#).

Depending on the system, snapshots may be of files, LUNs, file

systems, or any other type of container supported by the system.

SNIA

[Network] [Standards] [Storage System]

Acronym for [Storage Networking Industry Association](#).

sniffer

[Data Security] A software tool for auditing and identifying network traffic packets.

SNMP

[Network] [Management] Acronym for [Simple Network Management Protocol](#).

SNS

[Network] Acronym for Simple [Name Server](#).

social engineering

[Data Security] Use of social rather than technical methods to obtain [sensitive information](#) or perform privileged actions.

Examples include tricking people into downloading and executing files that appear to be benign but are actually malicious, revealing passwords, etc.

Society of Motion Picture and Television Engineers (SMPTE)

[Standards] An industry association whose goal is to standardize television and motion picture industry information interchange protocols.

SOF

[Fibre Channel] Acronym for [Start Of Frame](#).

soft link

[File System] Synonym for [symbolic link](#).

S

soft zone

[Fibre Channel] A [zone](#) consisting of zone members that are permitted to communicate with each other via the fabric.

Soft zones are typically implemented through a combination of [name server](#) and [Fibre Channel protocol](#) — when a port contacts the name server, the name server returns information only about Fibre Channel ports in the same zone(s) as the requesting port. This prevents ports outside the zone(s) from being discovered and hence the Fibre Channel protocol will not attempt to communicate with such ports. In contrast to hard zones, soft zones are not enforced by hardware; e.g., a [frame](#) that is erroneously addressed to a port that should not receive it will nonetheless be delivered. Well-known addresses are implicitly included in every zone. See [zone](#), [hard zone](#).

software appliance

[Computer System] An application combined with an [operating environment](#) designed to run on industry standard hardware.

If a vendor installs the software [appliance](#) on hardware prior to customer delivery, the offering is considered an appliance.

Software as a Service (SaaS)

[Services] Delivery over a network, on demand, of the use of an application.

Software Defined Data Center (SDDC)

[Management] A virtualized data center with a service management interface.

Application requirements determine the service levels provided.

software-defined storage (SDS)

[Storage] Virtualized storage with a service management interface.

SDS includes pools of storage with data service characteristics that may be applied to meet the requirements specified through the service management interface.

solicited control

[Fibre Channel] An [information category](#) indicated in a [Fibre Channel frame](#) header.

solicited data

[Fibre Channel] An [information category](#) indicated in a [Fibre Channel frame](#) header.

solid state array

[Storage System] Synonym for [solid state storage array](#).

Solid State Disk

[Storage System] Synonym for [Solid State Drive](#).

Solid State Storage (SSS)

[Storage System] A storage capability built from solid state electronics.

solid state storage array

[Storage System] A storage [array](#) that uses solid state storage and may contain other storage media.

Solid State Drive (SSD)

[Storage System] A [disk drive](#) whose storage capability is provided by [solid state storage](#).

Form factors and interfaces for solid state drives are typically the same as for traditional disk drives.

Solution Exchange Standard

[Management] A [DMTF](#) standard that defines the [exchange](#) of support or help desk information.

solution under test

[Computer System] All hardware and software components that are exercised during a test to verify functional behavior or determine performance characteristics.

The solution under test comprises the infrastructure including software components, application(s), test system(s), and the system(s) under test.

See also [system under test](#) and [test system](#).

SONET

[Network] Shorthand for [Synchronous Optical Network](#).

Source Identifier (S_ID)

[Fibre Channel] A number in a [Fibre Channel frame](#) that identifies the source of the frame.

See [D_ID](#).

source N_Port

[Fibre Channel] The [Nx_Port](#) from which a [frame](#) is transmitted.

space reduction

[Storage System] Deprecated synonym for capacity optimization.

spare (disk, extent)

[Storage System] An object [reserved](#) for the purpose of [substitution](#) for a like object in case of that object's failure.

sparse file

[File System] A file that has empty (unwritten and unallocated) data regions, which on reading back are implicitly filled with bytes containing the value zero (0x00).

On some file systems all files are implicitly sparse.

special character

[Fibre Channel] Any [transmission character](#) that is valid in the [transmission code](#) but does not correspond to a [valid data byte](#).

Special characters are used to denote special functions.

special code

[Fibre Channel] A code that, when encoded using the rules specified by the [transmission code](#), results in a [special character](#).

Special codes are typically associated with control signals related to [protocol](#) management (e.g., [K28.5](#)).

SPI

[SCSI] Acronym for [SCSI Parallel Interface](#).

spiral data transfer rate

[Storage System] Synonym for [full volume transfer rate](#).

split I/O request

1. [Storage System] An [I/O request](#) to a [virtual disk](#) that requires two or more I/O operations to satisfy, because the virtual data addresses in the request map to more than one extent on one or more disks.
2. [Storage System] An [application I/O request](#) that is divided into two or more sub-requests by a [file system](#) or other operating system component because the amount of data requested is too large for the [operating environment](#) to handle as a unit.

split mirror, split mirror copy**split mirror point in time copy**

1. [Storage System] Any of a class of [point in time copy](#) implementations or the resulting copies in which the storage for the copy is synchronized to the source of the copy and then split.

A split [mirror](#) copy occupies as much storage as the source of the copy.

2. [Data Recovery] A method for generating a [frozen image](#) of a set of data.

A split mirror frozen image contains a complete copy of data as of the moment of frozen image creation. When a split mirror frozen image has served its purpose, it may be resynchronized with the original data from which it was split, or discarded.

SPOF

[General] Acronym for [Single Point Of Failure](#).

spoliation of evidence

[Legal] The intentional or negligent destruction, hiding, alteration, withholding or concealment of withholding of evidence relevant to a legal action.

spoofing

[Data Security] Unauthorized use of legitimate [identification](#) and [authentication](#) data to mimic a [subject](#) different from the attacker.

Impersonating, masquerading, piggybacking and mimicking are forms of spoofing.

SR

[Fibre Channel] Acronym for [Sequence Recipient](#).

SRAM

[Hardware] Acronym for [Static Random Access Memory](#).

SRM

[Management] Acronym for [Storage Resource Management](#).

SRP

[Data Security] Acronym for [Secure Remote Password](#).

SSD

[Storage System] Acronym for [Solid State Drive](#).

SSID

[iSCSI] Shorthand for [iSCSI Session Identifier](#).

SSL

[Data Security] Acronym for [Secure Sockets Layer](#).

SSO

[Data Security] Acronym for [Single Sign On](#).

ST

[Data Security] Acronym for [Security Target](#).

STA

[SCSI] Acronym for [SCSI Trade Association](#).

stand alone drive

[Data Recovery] A removable [media drive](#) that is not associated with a [media stacker](#) or [robot](#).

standard interconnect

[Standards] An I/O or network [interconnect](#) whose specifications are readily available to the public, and that can therefore easily be implemented in a vendor's products without license or royalty payments.

Also called an [open interconnect](#).

star

[Network] A physical network [configuration](#) in which every [node](#) is connected directly to, and only to, a central point; all communications pass through the central point, which may be a [hub](#) or a [switch](#).

Start Of Frame (SOF)

[Fibre Channel] A group of ordered sets that delineates the beginning of a [frame](#).

Static Random Access Memory (SRAM)

[Hardware] Byte-addressable computer memory that maintains state indefinitely given continuous power.

storage

[General] A function that records data and supports retrieval.

Storage Area Network (SAN)

1. [Network] A network whose primary purpose is the transfer of data between computer systems and storage devices and among storage devices.

A SAN consists of a communication infrastructure, which provides physical connections, and a management layer, which organizes the connections, storage devices, and computer systems so that data transfer is secure and robust.

The term SAN is usually (but not necessarily) identified with [block](#) I/O services rather than file access services.

2. [Storage System] A storage system consisting of storage elements, storage devices, computer systems, and/or appliances, plus all [control software](#), communicating over a network.

The SNIA definition specifically does not identify the term *SAN* with [Fibre Channel](#) technology. When the term *SAN* is used in connection with Fibre Channel technology, use of a qualified phrase such as "Fibre Channel SAN" is encouraged. According to this definition, an [Ethernet](#)-based network whose primary purpose is to provide access to storage devices would be considered a SAN. SANs are sometimes also used for system interconnection in clusters.

storage array

[Storage System] A collection of storage devices from one or more commonly accessible storage subsystems, combined with a body of [control software](#).

storage controller

[Storage System] A device for handling storage requests that includes a processor or sequencer programmed to autonomously process a substantial portion of I/O requests directed to storage devices.

Aggregating [RAID](#) controllers and filers are examples of storage controllers.

storage device

[Storage System] Any [storage element](#) or [aggregation](#) of elements, designed and built for data storage and delivery.

storage device virtualization

[Storage System] [Virtualization](#) of storage elements and storage devices such as disks, tape drives, [RAID](#) arrays, LUNs, file systems, etc.

storage domain

[Storage System] A collection of storage resources and supporting software and interfaces that are managed as a unit.

storage efficiency

[Storage System] The ratio of a storage system's [effective capacity](#) to its [raw capacity](#).

An estimated efficiency calculation is permissible using estimated effective capacity.

The storage efficiency of a system is normally low when it is new. On a [capacity optimizing system](#) efficiency generally increases as the system is loaded with data. There is no way to precisely predict the storage efficiency of a loaded capacity optimizing system before data is loaded onto it.

storage element

[Storage System] Any component that is used to build storage devices and which contributes to persistent data storage and delivery, such as a disk drive, [flash memory](#), tape, [tape drive](#), or library.

Storage elements are components of storage devices.

storage extent

[Storage System] A contiguous [array](#) of bytes—real or virtual—as exposed by a storage container.

A storage extent instance may include data on either removable or nonremovable [media](#) storage devices. See [extent](#).

storage federation

[Storage System] Making multiple storage systems appear to a user as a single system.

Storage Interoperability

[Storage System] The ability of storage devices, products, or systems to work together in a correct, predictable and interchangeable fashion.

Storage Management Initiative-Specification (SMI-S)

[Management] [Standards] A storage management interface developed by SNIA, and standardized via [ANSI](#) and [ISO](#).

storage media

[Storage System] The material in a [storage device](#) on which data is recorded.

Storage [media](#) includes electrical (e.g., solid state), magnetic (hard disk, tape), and optical media.

storage medium

1. [General] An individual that makes prophesies regarding the storage industry.
2. [Storage System] See [storage media](#).

storage networking

[Storage System] [Network] The practice of creating, installing, administering, or using networks whose primary purpose is the transfer of data between computer systems and storage elements and among storage devices.

Storage Networking Industry Association (SNIA)

[Network] [Standards] [Storage System] A 501(c)(6) association of producers and consumers of [storage networking](#) products whose goal is to further storage networking technology and applications.

storage resource domain

[Management] The category of resources that encompasses storage services.

storage resource management

[Management] Management of physical and logical storage resources, including storage elements, storage devices, appliances, virtual devices, disk [volume](#) and file resources.

storage security

[Data Security] Application of physical, technical, and administrative controls to protect storage systems and infrastructure as well as the data stored (3.50) within them. [ISO/IEC 27040]

Storage security is focused on protecting data (and its storage infrastructure) against unauthorized disclosure, modification, or destruction while assuring its availability to authorized users. These controls may be preventive, detective, corrective, deterrent, recovery, or compensatory in nature.

storage service

[Management] A set of functions that provide storage.

storage subsystem

[Storage System] An integrated collection of (a.) storage controllers and/or [host bus adapters](#), (b.) storage devices, CD-ROM drives, tape drives, and libraries, and (c.) any required [control software](#), that provides storage services to one or more computers.

storage system power efficiency

[Storage System] The [power efficiency](#) of a storage system, where input power is measured at the wall socket and output power is measured at the power inputs to the disks, fans, robotics and electronics.

Measurement points of interest include the [idle](#) and maximum activity states.

storage taxonomy

[Standards] A hierarchical categorization of storage networking products based on capacity, availability, port count and other attributes.

The *SNIA Emerald™ Power Efficiency Measurement Specification* presents a storage taxonomy.

storage tier

[Storage System] Storage space that has [availability](#), performance, and cost characteristics that justify the movement of data between it and other storage tiers based on the requirements of the stored data.

storage virtualization

1. [Storage System] The act of abstracting, hiding, or isolating the internal function of a storage (sub) system or service from applications, compute servers or general network resources for the purpose of enabling application and network independent management of storage or data.
2. [Storage System] The application of [virtualization](#) to storage services or devices for the purpose of aggregating, hiding complexity or adding new capabilities to lower level storage resources.

Storage can be virtualized simultaneously in multiple layers of a system, for instance to create [HSM](#) like systems.

store and forward (switching)

[Fibre Channel] [Network] A switching technique that requires buffering an entire [frame](#) before it is routed.

stream

1. [Network] Continuous [media](#) content served over a specialized [protocol](#) in real-time.
2. [File System] A subfile in the [CIFS](#) protocol. NFSv4 provides equivalent functionality using Named Attributes.

streamed sequence

[Fibre Channel] A new [sequence](#) initiated by a [Sequence Initiator](#) in any [class of service](#) for an [exchange](#) while it already has sequences open for that exchange.

strip

[Storage System] The consecutively addressed blocks in a single extent.

A [disk array](#)'s [controller](#) uses strips to map [virtual disk](#) block addresses to [member disk](#) block addresses. Also known as [stripe element](#).

strip size

[Storage System] Synonym for [stripe depth](#).

stripe

[Storage System] The set of strips at corresponding locations of each [member](#) extent of a [disk array](#) that uses striped data [mapping](#).

The strips in a stripe are associated with each other in a way (e.g., relative extent [block](#) addresses) that allows membership in the stripe to be quickly and uniquely determined by a computational algorithm. [Parity RAID](#) uses stripes to map [virtual disk](#) block addresses to member extent block addresses.

S

stripe depth

1. [Storage System] The number of blocks in a [strip](#) in a [disk array](#) that uses striped data [mapping](#).
2. [Storage System] The number of consecutively addressed [virtual disk](#) blocks mapped to consecutively addressed blocks on a single [member](#) extent of a disk array.

stripe element

[Storage System] Synonym for [strip](#).

stripe size

[Storage System] The number of blocks in a [stripe](#).

A [striped array](#)'s stripe size is the [stripe depth](#) multiplied by the number of [member](#) extents. A [parity RAID array](#)'s stripe size is the stripe depth multiplied by the number of member extents less the number of parity extents.

striped array

striped disk array

[Storage System] A [disk array](#) with striped data [mapping](#) but no [redundancy](#) for failure protection.

Striped arrays are sometimes used to improve I/O performance on data that is of low value or easily replaced. Virtualizers may also use simple [striping](#) of the extents that they import, on the grounds that the underlying storage is responsible for [data protection](#).

stripeset

[Storage System] Synonym for [striped array](#).

striping

1. [Storage System] Short for [data striping](#).

Also known as [RAID Level 0](#) or [RAID 0](#), striping is a [mapping](#) technique in which fixed-size consecutive ranges of [virtual disk](#) data addresses are mapped to successive [array](#) members in a cyclic pattern.

2. [Storage System] A network technique for aggregating the [bandwidth](#) of several links between the same pair of nodes. A single data stream can be spread across the links for higher aggregate bandwidth. Sometimes called *port aggregation*.

Structure of Management Information (SMI)

[Fibre Channel] [Management] [Network] A notation for setting or retrieving management variables over [SNMP](#).

SNMP queries are in the form of GET requests for one or more Object [IDs](#) (OIDs), which take the form 1.3.1.1.4.6.123.1.1.0; an [encoding](#) called ASN.1 is used to transmit both request and reply. The SMI spec—not to be confused with the SNIA's Storage Management Initiative—specifies the [schema](#) used in the OID strings.

structured data

[Data Management] Data that is organized and formatted in a known and fixed way.

The format and organization are customarily defined in a [schema](#). The term structured data is usually taken to mean data generated and maintained by databases and business applications.

subdirectory

[File System] A [directory](#) in a hierarchical [directory tree](#) whose parent is a directory.

subfile data deduplication

[Storage System] A form of data deduplication that operates at a finer granularity than an entire file or data object.

See [data deduplication](#), [single instance storage](#).

S

subject

[Data Security] In the context of [access control](#) or [authorization](#), an entity whose access or usage is controlled.

substitution

[General] The assumption of a component's function in a system by a functionally equivalent component.

subtractive routing method

[SCSI] A method used by [SAS expanders](#) that forwards connection requests for unknown (i.e., not directly attached) devices via special designated [phy](#) links to another more authoritative expander.

The more authoritative expander is usually, but does not have to be, the "root" expander.

SUT

[Computer System] Shorthand for [solution under test](#).

SVC

[Network] Acronym for Switched Virtual [Circuit](#).

swap

[General] The installation of a [replacement unit](#) in place of a defective unit in a system.

Units are any parts of a system that may either be field replaceable (FRUs) by a vendor service representative or consumer replaceable (CRUs). A physical swap operation may be cold, warm, or hot, depending on the state in which the [disk subsystem](#) must be in order to perform it. A functional swap operation may be an auto swap or it may require human intervention.

switch

[Fibre Channel] [Network] A network infrastructure component to which multiple ports attach.

Unlike hubs, switches typically have internal [bandwidth](#) that is a multiple of link bandwidth, and the ability to rapidly switch port connections from one to another. A typical switch can accommodate several simultaneous full link bandwidth transmissions between different pairs of ports. See [hub](#).

switch-back

[Computer System] Synonym for [failback](#).

switch-over

[Computer System] Synonym for [failover](#).

Switch_Name

[Fibre Channel] A [Name Identifier](#) that is associated with a [Fibre Channel switch](#) or [bridge](#) name.

switched over (system)

[Computer System] Synonym for [failed over](#).

Swordfish

[Storage Management] A SNIA open standard for managing data and storage services.

Swordfish is an extension of the [Redfish](#) specification that enables simple, scalable, and interoperable management of storage resources, ranging from direct attached storage to complex enterprise class storage servers.

Swordfish service

[Storage Management] A [Redfish service](#) that conforms to requirements of the Swordfish specification.

Swordfish service entry point

[Storage Management] A [Redfish service entry point](#) through which a particular instance of a Swordfish Service is accessed.

symbolic link

[File System] A special type of file that can be used to redirect a file or [directory](#) path transparently to another file or directory that may be on another system.

Also known as [symlink](#) or [soft link](#). Symbolic links differ from hard links in that deletion of the underlying file causes them to be "broken", and subsequent attempts to traverse them fail.

symlink

[File System] Shorthand for a [symbolic link](#).

symmetric cryptography

[Data Security] [Cryptography](#) that uses a [symmetric cryptosystem](#).

symmetric cryptosystem

[Data Security] A [cryptographic algorithm](#) in which the same key is used to encrypt and decrypt a single message or [block](#) of stored information.

Keys used in a symmetric [cryptosystem](#) must be kept secret, yet are required on both ends of a [protocol exchange](#). They are commonly used on a per-session basis by layered protocols such as [TLS](#) and [SSL](#).

symmetric virtualization

[Computer System] Deprecated synonym for [in-band virtualization](#).

synchronization

1. [Fibre Channel] A [receiver's](#) [identification](#) of a [transmission word](#) boundary.

2. [General] The act of aligning or making two entities be equivalent at a specified point in time.

synchronize

[Data Management] In the context of [data replication](#), to establish an identical copy of the user data on the primary [volume](#) onto the secondary volume.

Synchronous Digital Hierarchy (SDH)

[Network] A common worldwide telecommunications methodology, standardized by [ISO](#) with 155, 622, 2048 and 9953 [Mbps serial](#) data rates in steps of 4.

An SDH uses a light scrambling of data to remove only the lowest frequency elements with the goal of achieving maximum digital [bandwidth](#) use.

synchronous mirroring

[Storage System] Deprecated synonym for [synchronous replication](#).

synchronous operations

[Computer System] Operations that have a fixed time relationship to each other.

Most commonly used to denote I/O operations that occur in time [sequence](#), i.e., a successor operation does not occur until its predecessor is complete.

Synchronous Optical Network (SONET)

[Network] A standard for optical network elements and transmission.

SONET provides modular building blocks, fixed overheads, integrated operations channels, and flexible [payload](#) mappings. Basic SONET provides a [bandwidth](#) of 51.840 megabits/second. This is known as OC-1. Higher bandwidths that are n times the basic rate are available (known as [OC-n](#)). OC-3, OC-12, OC-48, and OC-192 are currently in common use.

synchronous replication

[Storage System] A replication technique in which data must be committed to stable storage at both the primary site and the secondary site before the write is acknowledged to the host.

system board

[Computer System] A printed [circuit](#) module containing mounting devices for processor(s), memory, and [adapter](#) cards, and implementing basic computer functions such as memory access, processor and [I/O interconnect](#) clocking, and human interface device attachment.

system disk

[Computer System] The disk on which a computer system's operating software is stored.

The system disk is usually the disk from which the operating system is *bootstrapped* (initially loaded into memory). It frequently contains the computer system's [swap](#) and/or page files as well, and may also contain libraries of common software shared among several applications.

system portability

[Computer System] The ability of a service, application or system to run in more than one environment.

system under test

[General] An entity being tested to verify functional behavior or determine performance characteristics.

See also [solution under test](#) and [test system](#).

T

T

T1 copy

[Storage System] Synonym for [mirroring](#).

T10

[SCSI] Short name for the [ANSI INCITS T10](#) technical committee.

T11

[Fibre Channel] Short name for the [ANSI INCITS](#) TC T11 committee.

table routing method

[SCSI] A method used by [SAS expanders](#) for routing connection requests when multiple devices are accessible through a single SAS switch port.

tabular mapping

[Storage System] A form of [mapping](#) in which a lookup table contains the correspondence between the two address spaces being mapped to each other.

If a mapping between two address spaces is tabular, there is no mathematical formula that will convert addresses in one space to addresses in the other. See [algorithmic mapping](#), [dynamic mapping](#).

tampering

[Data Security] An unauthorized modification that alters the proper functioning of a device, system or communications path in a manner that degrades the security or functionality it provides.

tape

[Storage System] A removable [storage element](#) containing a tape substrate used as a [storage medium](#).

A tape cartridge may also contain other storage elements (e.g., a [medium auxiliary memory](#)). The data on a tape is accessed by a [tape drive](#).

tape autoloader

[Storage System] Deprecated synonym for [media stacker](#).

The term *autoloader* is typically used to indicate a low-cost [library](#).

tape drive

[Storage System] A [storage device](#) that reads and writes data on tapes.

Unlike disks, tapes use implicit data [addressing](#). See [disk](#).

tape eject slot

[Storage System] An [entry/exit slot](#) in a [tape library](#).

tape library

[Storage System] A [storage device](#) that provides automated access to multiple tape cartridges, typically via multiple tape drives.

A [robotic media handler](#) is used to move tape cartridges between the tape drives, tape slots (for storage), and tape eject slots if there are any.

tape slot

[Storage System] A physical location used to hold a tape cartridge when not in a [tape drive](#).

tape virtualization
tape drive virtualization
tape library virtualization

[Storage System] The act of creating abstracted tape devices by applying [virtualization](#) to tape drives, tape libraries or other storage devices.

target

[SCSI] The endpoint that receives a [SCSI](#) I/O command [sequence](#).

See [initiator](#), [LUN](#), [target port identifier](#).

target NVMe_Port

[Fibre Channel] [NVMe_Port](#) which is the NVM subsystem port for an [NVMeoFC association](#).

Target of Evaluation (TOE)

[Data Security] An IT product or system and its associated guidance documentation that is the [subject](#) of evaluation.

This term is most commonly associated with ISO 15408.

target port identifier

[SCSI] The [interconnect](#) address of a [target](#) or [controller](#).

Target Session Identifying Handle (TSIH)

[iSCSI] An identifier, assigned by the [iSCSI target](#), for a session with a specific named [initiator](#).

TB

TByte

[Computer System] Shorthand for [Terabyte](#).

Tbit

[General] Shorthand for [Terabit](#).

TCG

[Data Security] Acronym for [Trusted Computing Group](#).

T

TCO

[General] Acronym for [Total Cost of Ownership](#).

TCP

[Network] Acronym for [Transmission Control Protocol](#).

TCP Offload Engine (TOE)

[Network] A technology for improving [TCP/IP](#) performance by offloading TCP/IP processing to a [Network Interface Card](#).

TCP/IP

[Network] Shorthand for the suite of protocols that includes [TCP](#), [IP](#), [UDP](#), and [ICMP](#).

This is the basic set of communication protocols used on the Internet.

Tebibit (Tibit)

[General] Shorthand for 1,099,511,627,776 (2^{40}) bits.

Binary notation is most commonly used for semiconductor memory sizes.

See also [Terabit](#).

Tebibyte (TiB)

[General] Shorthand for 1,099,511,627,776 (2^{40}) bytes.

Binary notation is most commonly used for semiconductor memory sizes.

See also [Terabyte](#).

technical controls

[Data Security] Security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system. [NIST Special Pub 800-53]

Technical Working Group (TWG)

[Standards] A SNIA working group in which specific technical work is undertaken, protected by the SNIA IP Policy.

Within the SNIA, technical work for standards development is conducted by volunteer technologists from member companies. The TWGs report to the SNIA Technical Council, which in turn reports to the SNIA Board.

tenancy

[Fibre Channel] The possession of a [Fibre Channel Arbitrated Loop](#) by a device to conduct a transaction.

Terabit (Tbit)

[General] Shorthand for 1,000,000,000,000 (10^{12}) bits.

The SNIA uses the base 10 convention commonly found in I/O-related and scientific literature rather than the base 2 convention (1,099,511,627,776, i.e., 2^{40}) common in computer system and software literature.

See also [Tebibit](#).

Terabyte (TB)

[Computer System] Shorthand for 1,000,000,000,000 (10^{12}) bytes.

The SNIA uses the base 10 convention commonly found in I/O-related and scientific literature rather than the base 2 convention (1,099,511,627,776, i.e., 2^{40}) common in computer system and software literature.

See also [Tebibyte](#).

test system

[Storage System] A collection of equipment used to perform a test on a system under test.

See also [solution under test](#) and [system under test](#).

theoretical capacity

[Storage System] The area of the [storage media](#) on a device times its areal density.

This number is rarely published, as it does little to contribute to an understanding of the eventual [raw capacity](#) of the device.

thin provisioning

[Storage System] A technology that allocates the physical capacity of a [volume](#) or [file system](#) as applications write data, rather than preallocating all the physical capacity at the time of [provisioning](#).

third party authentication

[Data Security] Reliance on an [authentication](#) service, such as a [RADIUS server](#), that is separate from (or external to) the entities of an authentication transaction.

third party copy

[Data Recovery] [Management] [SCSI] A technique for performing backups using minimal host resources by copying data directly from the source to the destination without passing through a host.

threat

[Data Security] An avenue of [attack](#) that may result in adverse changes to a protected asset.

threat monitoring

[Data Security] Analysis, assessment, and review of [audit](#) trails and other information collected for the purpose of searching out system events that may constitute violations of system security.

throughput

[Computer System] A deprecated synonym for [IOPs](#) that is often incorrectly used to refer to data transfer capacity.

The traffic passing through an interface during a given time period is expressed in IOPS or in Bytes per Second.

TiB

TiByte

[General] Shorthand for [Tebibyte](#).

Tibit

[General] Shorthand for [Tebibit](#).

tiered storage

[Storage System] Storage that is physically partitioned into multiple distinct classes based on price, performance or other attributes.

Data may be dynamically moved among classes in a tiered storage implementation based on access activity or other considerations.

time server

[Network] An intelligent entity in a network that enables all nodes in the network to maintain a common time base within close tolerances.

TLS

[Data Security] Acronym for [Transport Layer Security](#).

TNC

[Network] Acronym for Threaded Neil Councilman, a type of [coaxial cable](#) connector.

Specifications for TNC style connectors are defined in MIL-C-39012 and MIL-C-23329.

TOE

1. [Network] Acronym for [TCP Offload Engine](#).
2. [Data Security] Acronym for [Target of Evaluation](#).

token ring (network)

1. [Network] A network in which each [node's transmitter](#) is connected to the [receiver](#) of the node to its logical right, forming a continuous ring.

Nodes on a token ring network gain the right to transmit data by retaining a token (a specific unique message) when they receive it. When a node holding the token has transmitted its allotment of data, it forwards the token to the next node in the ring.

2. [Network] A [LAN protocol](#) for token ring networks governed by IEEE Standard 802.3 that operates at speeds of 4 Mbits/second and 16 Mbits/second.

topology

1. [Network] The logical layout of the components of a computer system or network and their interconnections.
Topology deals with questions of what components are directly connected to other components from the standpoint of being able to communicate. It does not deal with questions of physical location of components or interconnecting cables.
2. [Fibre Channel] The communication infrastructure that provides [Fibre Channel](#) communication among a set of PN_Ports (e.g., a Fabric, an [Arbitrated Loop](#), or a combination of the two).

Total Cost of Ownership (TCO)

[General] The comprehensive cost over its lifetime of a particular capability such as data processing, storage access, file services, etc.

TCO includes acquisition, environment, operations, management, service, upgrade, loss of service, and residual value. See [inherent cost](#).

TPC

[Data Recovery] [Management] Acronym for [Third Party Copy](#).

transceiver

[Fibre Channel] A [transmitter](#) and [receiver](#) combined in one package.

transformation

[Long Term Retention] A type of [migration](#) in which a format or representation change occurs during the movement of data or information.

Transformation involves possible information loss, since newer formats may be incapable of capturing all the functionality of the

original format, or the migration system may be unable to interpret all the nuances of the original format.

Translate Domain

[Fibre Channel] A [domain](#) presented by a [Translate Domain switch](#).

Translate Domain switch

[Fibre Channel] A [switch](#) within an [Inter-Fabric Router](#) that is created for each set of Proxy N_Ports whose corresponding Native Nx_Ports exist within a set of Native Fabrics.

transmission character

[Fibre Channel] Any encoded [character](#) (valid or invalid) transmitted across the physical interface of a [Fibre Channel](#) or [Ethernet](#) link.

Valid transmission characters are specified by the standard defining the [transmission code](#) and include data characters and special characters.

transmission code

1. [General] A means of [encoding](#) data to enhance its transmission characteristics.
2. [Fibre Channel] A byte-oriented transmission code specified by [FC-FS-2](#) for 1/2/4/8 GFC, with valid data bytes and special codes encoded into 10-bit Transmission Characters according to the 8B10B encoding.
3. [Network] A word-oriented transmission code specified by 10GFC, with 64 bits of data and special codes encoded into a 66-bit transmission unit according to the 64/66 encoding.

Transmission Control Protocol (TCP)

[Network] The Internet [connection](#) oriented network transport [protocol](#), which provides a reliable delivery service.

transmission word

[Fibre Channel] A string of four contiguous transmission characters aligned on boundaries that are zero modulo 4 from a previously received or transmitted [special character](#).

[Fibre Channel](#) transmission and reception operates in transmission word units when using [8B/10B encoding](#).

transmitter

1. [Fibre Channel] The portion of a Link_Control_Facility that converts valid data bytes and special codes into transmission characters using the rules specified by the [transmission code](#), converting these transmission characters into a bit stream, and transmitting this bit stream on an optical or electrical transmission [medium](#).
2. [Fibre Channel] An electronic [circuit](#) that converts an electrical logic signal to a signal suitable for an optical or electrical communications [media](#).

transparent failover

[Computer System] A [failover](#) from one component of a system to another that is transparent to the external [operating environment](#).

Often used to refer to paired disk controllers, one of which exports the other's virtual disks at the same [host bus](#) addresses after a failure. See [non-transparent failover](#).

Transport Layer Security (TLS)

[Data Security] A [protocol](#) suite defined by the [IETF](#) that provides privacy and [data integrity](#) between two communicating applications, using higher-level protocols that can layer on top of the TLS protocol transparently.

There are multiple versions of TLS, which are not compatible with each other, and early versions are considered less secure and should not be used. Multiple SNIA specifications leverage TLS as an important security mechanism; to ensure both security and interoperability, SNIA has published the *SNIA TLS specification for storage systems* (also ISO/IEC 20648) to identify specific requirements and guidance for TLS when it is used in conjunction with these SNIA specifications.

trap

[Management] A type of [SNMP](#) message used to signal that an event has occurred.

Trap delivery to recipients uses [UDP](#) and is not completely reliable. See [best effort](#).

triaxial cable

[Network] An electrical transmission [medium](#) consisting of three concentric conductors separated by a dielectric material with the spacings and material arranged to give a specified electrical impedance.

See [coaxial cable](#).

trim

[Storage System] A method by which the host operating system may inform a storage device of blocks of data that are no longer in use and can be reclaimed.

Many storage protocols support this functionality via various names, e.g., ATA TRIM and SCSI UNMAP. See also [garbage collection](#).

Triple DES (3DES)

[Data Security] A variant of the [Data Encryption Standard](#) (DES) in which the algorithm is applied three times in succession using two or three different keys.

This algorithm is obsolete.

trojan horse

[Data Security] Hidden code in a computer program that allows the unauthorized collection, falsification, or destruction of information.

trust

[Data Security] Belief in the reliability, truth, ability, or strength of someone or something.

A [trusted system](#) is believed to have the ability to function as expected and to not misbehave.

Trusted Computing Group (TCG)

[Data Security] A not-for-profit organization formed to develop, define, and promote open standards for hardware-enabled trusted computing and security technologies, including hardware building blocks and software interfaces, across multiple platforms, peripherals, and devices.

trusted system

[Data Security] A system that may be used for processing of sensitive or [classified information](#), that employs sufficient hardware and software [integrity](#) measures to assure that it performs according to its documented specification and acts in a predictable manner.

Such a system is developed in accordance with security criteria and evaluated by these criteria.

TSIH

[iSCSI] Acronym for [Target Session Identifying Handle](#).

tunneling

[Data Security] A technology that enables one network [protocol](#) to send its data via another network protocol's connections.

Tunneling works by encapsulating the first network protocol within packets carried by the second protocol. A tunnel may also encapsulate a protocol within itself (e.g., an [IPsec](#) gateway operates in this fashion, encapsulating [IP](#) in IP and inserting additional IPsec information between the two IP headers).

TWG

[Standards] Acronym for [Technical Working Group](#).

U

U.2

[Hardware] The SFF-8639 connector used for a Quad (4x) PCIe bus.

U

UDP

[Network] Acronym for [User Datagram Protocol](#).

UID

[Management] [Data Security] Short for "[user identifier](#)" (User Identifier).

ULP

[Fibre Channel] Acronym for [Upper Layer Protocol](#).

Ultra SCSI

[SCSI] A form of [SCSI](#) capable of 20 megatransfers per second.

[Single ended](#) Ultra SCSI supports bus lengths of up to 1.5 meters. [Differential](#) Ultra SCSI supports bus lengths of up to 25 meters. Ultra SCSI specifications define both narrow (8 data bits) and wide (16 data bits) buses. A narrow Ultra [SCSI interconnect](#) transfers data at a maximum of 20 MBytes per second. A wide Ultra SCSI interconnect transfers data at a maximum of 40 MBytes per second.

Ultra2 SCSI

[SCSI] A form of [SCSI](#) capable of 40 megatransfers per second.

There is no [single ended](#) Ultra2 SCSI specification. Low voltage [differential](#) (LVD) Ultra2 SCSI supports bus lengths of up to 12 meters. High voltage differential Ultra2 SCSI supports bus lengths of up to 25 meters. Ultra2 SCSI specifications define both narrow (8 data bits) and wide (16 data bits) buses. A narrow Ultra [SCSI interconnect](#) transfers data at a maximum of 40 MBytes per second. A wide Ultra2 SCSI interconnect transfers data at a maximum of 80 MBytes per second.

Ultra3 SCSI

[SCSI] A form of [SCSI](#) capable of 80 megatransfers per second.

There is no [single ended](#) Ultra3 SCSI specification. Low voltage [differential](#) (LVD) [Ultra2 SCSI](#) supports bus lengths of up to 12 meters. There is no high voltage differential Ultra3 SCSI specification. Ultra3 SCSI specifications only define wide (16 data bits) buses. A wide Ultra3 [SCSI interconnect](#) transfers data at a maximum of 160 MBytes per second.

Ultrium

[Storage System] The half-inch, 'square' tape implementation of the [LTO](#) format, currently in its 4th generation, LTO-4 Ultrium.

UML

[Management] Acronym for [Unified Modeling Language](#).

unauthorized disclosure

[Data Security] The exposure of information to individuals not authorized to receive or access it.

unicast

[Network] The transmission of a message to a single [receiver](#).

Unicast is contrasted with [broadcast](#) (sending a message to all receivers on a network) and [multicast](#) (sending a message to a select subset of receivers).

Unicode

[General] A set of standards intended to allow representation of every [character](#) in each of the world's languages; usually understood to mean the 16-bit variant.

Sixteen-bit Unicode allows for up to 2^{16} , or 65,536 characters, each of which may have a unique representation. It accommodates numerous non-English character sets and symbols, and is therefore an aid to development of products with multilingual user interfaces. Sixteen bits are not enough, however, to represent all the several hundred thousand Asian ideograms. Other 32-bit variants are available for these, but the increased inefficiency in representation of Western text inherent in them has been a barrier to widespread adoption.

unidirectional authentication

[Data Security] [Authentication](#) that provides one party to a communication with [assurance](#) of another's [identity](#).

Unified Modeling Language (UML)

[Management] A visual approach that uses a variety of diagrams such as use case, class, interaction, state, activity and others to specify the objects of a model and their relationships.

Various tools exist for turning UML diagrams into program code.

unified storage

[Storage System] A storage system that provides consolidated [NAS](#), [SAN](#), and possibly other storage services.

Uniform Resource Identifier

URI

Compact sequence of characters that identifies an abstract or physical resource.

See RFC2396.

U

Uniform Resource Locator

URL

Compact sequence of characters that identifies an abstract or physical resource, including its location.

See RFC1738.

Uninterruptible Power Source (UPS)

[General] A source of electrical power that is not affected by outages in a building's external power source.

UPSs may generate their own power using generators, or they may consist of large banks of batteries. UPSs are typically installed to prevent service outages due to external power grid failure in computer applications deemed by their owners to be "mission critical."

unmap

[Storage System] See [trim](#).

[Operating System] Removal of the virtual addresses from a portion of a file (e.g., POSIX).

unsolicited control

[Fibre Channel] An [information category](#) indicated in a [Fibre Channel frame](#) header.

unsolicited data

[Fibre Channel] An [information category](#) indicated in a [Fibre Channel frame](#) header.

unstructured data

[Data Management] Data that cannot be easily described as [structured data](#).

In general any non-database filesystem content is considered to be unstructured.

Upper Layer Protocol (ULP)

[Fibre Channel] A [protocol](#) used on a [Fibre Channel](#) network at or above the [FC-4](#) level.

The [Fibre Channel Protocol](#) for [SCSI](#) and [IP](#) over Fibre Channel are examples of ULPs.

UPS

[General] Acronym for [Uninterruptible Power Source](#).

usable capacity

[Storage System] Synonym for [formatted capacity](#).

user data extent

[Storage System] The [protected space](#) in one or more contiguously located [redundancy group](#) stripes in a single redundancy group.

In [RAID](#) arrays, collections of user data extents comprise the *virtual disks* or [volume sets](#) presented to the [operating environment](#).

user data extent stripe depth

[Storage System] The number of consecutive blocks of [protected space](#) in a single [user data extent](#) that are mapped to consecutive [virtual disk block](#) addresses.

In principle, each user data extent that is part of a virtual disk may have a different user data extent [stripe depth](#). User data extent stripe depth may differ from the [redundancy group stripe depth](#) of the [protected space extent](#) in which it resides.

User Datagram Protocol (UDP)

[Network] An [Internet protocol](#) that provides connectionless [datagram](#) delivery service to applications.

UDP over [IP](#) adds the ability to address multiple endpoints within a single network [node](#).

User Identifier (UID)

[Management] [Data Security] A unique number that identifies an individual to a computer system.

UIDs are the result of [authentication](#) processes that use account names, passwords and possibly other data to verify that a user is actually who she represents herself to be. UIDs are input to

U

[authorization](#) processes that grant or deny access to resources based on the [identification](#) of the requesting user.

userid

[Management] [Data Security] Shorthand for [User Identifier](#).

UTF-8

[General] An [encoding](#) for multi-byte [character](#) schemes such as [Unicode](#), in which ASCII text encodes to itself and POSIX string manipulation routines work largely as expected.

A 16-bit Unicode string that encodes ASCII text will have every other [data byte](#) within it set to zero. The UTF-8 encoding of this text will have a zero only at the end.

utilized capacity power efficiency

[Storage System] The ratio of bytes stored on an [idle](#) storage system to the amount of power required to maintain the system in a [ready idle](#) state.

UUID

[Computer System] An identifier that is expected to be universally unique across systems, space and time.

**valid data byte**

[Fibre Channel] A string of eight contiguous bits within [FC-P1](#) that represents a value between 0 and 255.

valid frame

[Fibre Channel] A received [frame](#) containing a valid [Start of Frame](#) (SOF), a valid [End of Frame](#) (EOF), valid data characters, and proper [Cyclic Redundancy Check](#) (CRC) of the Frame Header and Data Field.

**validity control bit**

[Fibre Channel] A control bit that indicates whether a field is valid.

If a validity control bit indicates that a field is invalid, the value in the field is treated as invalid and ignored.

variable-length segmentation

[Storage System] [Partitioning](#) a byte stream into parts that are not a constant number of bytes when performing [compression](#) or [hash-based data deduplication](#).

See [fixed-length segmentation](#).

VBA

[Storage System] Acronym for [Virtual Block Address](#).

VCI

[Network] Acronym for [Virtual Channel Identifier](#).

VCSEL

[Fibre Channel] Acronym for [Vertical Cavity Surface Emitting Laser](#).

vendor unique

[Standards] Aspects related to a standard (e.g., functions, codes, etc.) not defined by the standard, but offered by a single vendor within the framework of the standard.

Functionality unique to a given vendor may be exposed using standard methods. For example, many vendors offer vendor-specific [SNMP](#) MIBs that users of the SNMP standard can use to obtain system information.

verify**verification**

[Data Recovery] The object-by-object comparison of the contents of a [backup](#) image with the online data objects from which it was made.

versioning

[Data Recovery] The maintenance of multiple point-in-time copies of a collection of data.

Versioning is used to minimize [recovery](#) time by increasing the number of intermediate checkpoints from which an application can be restarted.

Vertical Cavity Surface Emitting Laser (VCSEL)

[Fibre Channel] A surface emitting [laser](#) source fabricated on a planar wafer with emission perpendicular to the wafer.

VE_Port_Name

[Fibre Channel] [Network] The [Name Identifier](#) of a VE_Port.

VF

[Fibre Channel] Acronym for [Virtual Fabric](#).

VF_ID

[Fibre Channel] Shorthand for [Virtual Fabric Identifier](#).

VF_Port_Name

[Fibre Channel] [Network] The [Name Identifier](#) of a VF_Port.

VFT Tagging E_Port

[Fibre Channel] An [E_Port](#) that has enabled processing of [Virtual Fabric](#) Tagging Headers.

VFT Tagging F_Port

[Fibre Channel] An [F_Port](#) that has enabled processing of [Virtual Fabric](#) Tagging Headers.

VFT Tagging PN_Port

[Fibre Channel] A [PN_Port](#) that has enabled processing of [Virtual Fabric](#) Tagging Headers.

VFT_Header

[Fibre Channel] Short for [Virtual Fabric Tagging Header](#).

VIA

[Computer System] Acronym for [Virtual Interface Architecture](#).

virtual block

[Storage System] A [block](#) in the address space presented by a [virtual disk](#).

Virtual blocks are the atomic units in which a virtual disk's storage capacity is typically presented by [RAID](#) arrays to their operating environments.

virtual block address

[Storage System] The address of a [virtual block](#).

Virtual block addresses are typically used in hosts' I/O commands addressed to the virtual disks instantiated by [RAID](#) arrays. [SCSI](#) disk commands addressed to RAID arrays are actually using virtual block addresses in their [logical block address](#) fields.

V

Virtual Channel Identifier (VCI)

[Network] A unique numerical tag contained in an [ATM](#) cell header.

A VCI identifies an ATM virtual [channel](#) over which the cell containing it is to travel.

virtual device

[Storage System] A device presented to an [operating environment](#) by [control software](#) or by a [volume manager](#).

From an application standpoint, a virtual device is equivalent to a physical one. In some implementations, virtual devices may differ from physical ones at the operating system level. E.g., booting from a [host based disk array](#) may not be possible.

virtual disk

[Storage System] A set of disk blocks presented to an [operating environment](#) as a range of consecutively numbered logical blocks with disk-like storage and I/O semantics.

The virtual disk is the [disk array](#) object that most closely resembles a [physical disk](#) from the operating environment's viewpoint. See [logical disk](#).

Virtual E_Port (VE_Port)

[Fibre Channel] [Network] The data forwarding component of an [FC Entity](#) that emulates an [E_Port](#) and is dynamically instantiated on successful completion of an ELP [Exchange](#).

The term virtual indicates the use of a non [Fibre Channel](#) link connecting the VE_Ports.

Virtual F_Port (VF_Port)

[Fibre Channel] [Network] The data forwarding component of an [FC Entity](#) that emulates an [F_Port](#) and is dynamically instantiated on successful completion of an [FLOGI Exchange](#).

The term virtual indicates the use of a non [Fibre Channel](#) link connecting a VF_Port with a [VN_Port](#).

Virtual Fabric (VF)

[Fibre Channel] A Fabric identified by a [VF_ID](#) composed of partitions of switches and N_Ports having the properties of: 1) a single Fabric management, 2) independence from all other Virtual Fabrics, e.g., an independent address space.

virtual fabric identifier

[Fibre Channel] A value that uniquely identifies a [Virtual Fabric](#) among all the Virtual Fabrics that share a set of switches and N_Ports.

Virtual Fabric Tagging Header (VFT_Header)

[Fibre Channel] An [Extended Header](#) that contains information to associate a [frame](#) to a specific [Virtual Fabric](#).

Virtual Interface Architecture (VIA)

[Computer System] An [API](#) specification for direct communication among distributed applications developed by Intel, Compaq, and Microsoft.

VIA reduces interprocess communication [latency](#) by obviating the need for applications to use processor [interrupt](#) or operating system paths to intercommunicate, while maintaining security on the communications path. VIA is [interconnect](#) neutral. See [Fibre Channel Virtual Interface](#).

Virtual Link

[Fibre Channel] [Network] The logical link connecting two [FCoE_LEPs](#). over a [Lossless Ethernet network](#) and is identified by the pair of [MAC](#) addresses of the two link end-points.

Virtual Local Area Network (VLAN)

[Network] A logical network that behaves as if it is physically separate from other physical and virtual LANs supported by the same switches and/or routers.

Virtual N_Port (VN_Port)

[Fibre Channel] [Network] The data forwarding component of an [FC_Entity](#) that emulates an [N_Port](#) and is dynamically



instantiated on successful completion of an [FLOGI](#) or FDISC [Exchange](#).

The term virtual indicates the use of a non [Fibre Channel](#) link connecting a VN_Port to a VF_Port.

Virtual Path Identifier (VPI)

[Network] An eight-bit field in an [ATM](#) cell header that denotes the cell over which the cell should be routed.

Virtual Switch

[Fibre Channel] A Switching Construct that resides in a [Core Switch](#) and corresponds to a [Virtual Fabric](#).

Multiple Virtual Switches may reside within a Core Switch.

virtual tape

[Storage System] A [virtual device](#) with the characteristics of a tape.

Virtual Tape Library (VTL)

[Backup] A storage system that emulates a [library](#).

VTLs are usually classified as near-online devices, and provide faster Max TTFD than tape, but normally not as fast as online systems. They typically use slower drives with higher capacities than high-performance systems, and therefore offer a better energy footprint per unit of data.

virtualization

[Computer System] Software that enable a single hardware platform to support multiple concurrent instances of systems such as storage, networking, or computing facilities.

Examples of virtualization are [compute virtualization](#) and [storage virtualization](#).

virus

[Data Security] A type of programmed [threat](#); a code fragment (not an independent program) that replicates by attaching to

another program, and either damages information directly or causes [denial of service](#).

VLAN

[Network] Acronym for [Virtual Local Area Network](#).

VN_Port

[Fibre Channel] Synonym for [Nx_Port](#), used when it is desired to emphasize the support for Virtual Fabrics and/or [N_Port Identification Virtualization](#).

VN_Port_Name

[Fibre Channel] [Network] The [Name Identifier](#) of a [VN_Port](#).

VN_Port MAC address

[Fibre Channel] [Network] The [MAC](#) address used by an ENode for a particular [address identifier](#) during [FC](#) operation using [FCoE](#) frames.

vnode

[Computer System] Synonym for [node](#), used when it is desired to emphasize the support for multiple nodes within a [platform](#).

volatility

[Computer System] A property of data yielding the possibility that it will be obliterated if certain environmental conditions are not met.

For example, data held in DRAM is volatile, since if electrical power to DRAM is cut, the data in it is lost. See [non-volatility, persistence](#).

volume

1. [Storage System] Synonym for [virtual disk](#).
2. [Storage system] A [storage element](#) that has been prepared for use.

Examples include [Logical Unit](#), tape cartridge, [LTFS](#) Volume, and USB thumb drive.

V

volume group

[Data Recovery] A collection of removable [media](#) that reside in a single location, for example in a single [robot](#) or group of interconnected robots.

volume manager

[Storage System] Common term for host-based [control software](#).

volume pool

[Data Recovery] A logical collection of removable [media](#) designated for a given purpose, for example, for holding the copies of a single repetitive [backup](#) job, or for backing up data from a given [client](#) or set of clients.

A [volume](#) pool is an administrative entity, whereas a [volume group](#) is a physical one.

volume set

[Storage System] Synonym for [virtual disk](#).

VPI

[Network] Acronym for [Virtual Path Identifier](#).

VSAN

[Fibre Channel] A collection of ports from a set of connected storage networking switches, that form a virtual network.

Ports within a single switch can be partitioned into multiple VSANs, despite sharing hardware resources. Conversely, multiple switches can join a number of ports to form a single VSAN.

VTL

[Backup] Acronym for [Virtual Tape Library](#).

vulnerability

[Data Security] A defect in [data protection](#) mechanisms that could be exploited by a [threat](#).

W

WAN

[Network] Acronym for [Wide Area Network](#).

warm spare (disk)

[Storage System] A [spare](#) to which power is applied, and which is not operating, but which is otherwise usable as a [hot spare](#).

warm swap

[Computer System] The [substitution](#) of a [replacement unit](#) (RU) in a system for a defective one, where in order to perform the substitution, the system must be stopped (causing it to cease performing its function), but power need not be removed.

Warm swaps are manual operations performed by humans. See [automatic swap](#), [cold swap](#), [hot swap](#).

Wave Division Multiplexing (WDM)

[Network] The splitting of light into a series of “colors” from a few (sparse WDM) to many with a narrow wavelength separation (dense WDM) for the purpose of carrying simultaneous traffic over the same physical fiber (9 micron usually).

Each “color” carries a separate data stream.

WBEM

[Management] Acronym for [Web Based Enterprise Management](#).

W

WDM

1. [Network] Acronym for [Wave Division Multiplexing](#).
2. [Windows] Acronym for Windows [Driver](#) Model.

weak key

[Data Security] A [key](#) that interacts with some aspect of a particular cipher's definition in such a way that it weakens the security strength of the cipher. [ISO/IEC 27040]

wear leveling

[Storage System] A set of algorithms utilized by a flash [controller](#) to distribute writes and erases across the cells in a flash device.

Cells in flash devices have a limited ability to survive write cycles. The purpose of wear leveling is to delay cell wear out and prolong the useful life of the overall flash device.

Web Based Enterprise Management (WBEM)

[Management] An initiative in the [DMTF](#), comprising a set of technologies that enable interoperable management of an enterprise.

WBEM consists of [CIM](#), an [XML DTD](#) defining the tags (XML encodings) to describe the CIM [Schema](#) and its data, and a set of [HTTP](#) operations for exchanging the XML-based information. CIM joins the XML data description language and HTTP transport [protocol](#) with an underlying [information model](#) (the CIM schema) to create a conceptual view of the enterprise.

well-known address

[Fibre Channel] An [address identifier](#) used to access a service provided by a [Fibre Channel](#) fabric.

The service may be distributed in many elements throughout the fabric or it may be centralized in one or a few elements. A well-known address is not [subject](#) to [zone](#) restrictions; i.e., a well-known address is always accessible, irrespective of the current active [zone set](#).

Wide Area Network

[Network] A communications network that is geographically dispersed and that includes telecommunications links.

wide link

[SCSI] A group of physical links that attaches a wide port to another wide port.

wide port

[SCSI] A port that contains more than one [phy](#).

wide SCSI

[SCSI] Any form of [SCSI](#) using a 16-bit data path.

In a wide SCSI implementation, the [data transfer rate](#) in MBytes per second is twice the number of megatransfers per second because each transfer cycle transfers two bytes. See [fast SCSI](#), [Ultra SCSI](#), [Ultra2 SCSI](#), [Ultra3 SCSI](#).

Windows Internet Naming Service (WINS)

[Windows] A facility of the Windows operating system that translates between [IP](#) addresses and symbolic names for network nodes and resources.

W

Windows Management Instrumentation (WMI)

[Windows] The Microsoft framework that supports [CIM](#) and [WBEM](#); a set of Windows operating system facilities that enable operating system components to provide management information to management agents.

WINS

[Windows] Acronym for [Windows Internet Naming Service](#).

WMI

[Windows] Acronym for [Windows Management Instrumentation](#).

word

1. [General] An addressable unit of data in computer memory. The length is specified by the computer architecture and is typically 8, 16, 32, or 64 bits. Most processor architectures

include arithmetic and logical instructions that operate on words.

2. [Fibre Channel] The smallest [Fibre Channel](#) data element consisting of 40 [serial](#) bits representing either a flag ([K28.5](#)) plus three encoded data bytes (ten encoded bits each) or four ten bit encoded data bytes.
3. [Fibre Channel] A string of four contiguous bytes occurring on boundaries that are zero modulo four from a specified reference. See [transmission word](#).

workgroup

[Computer System] A group of UNIX or Windows computer system users and/or computers, usually with a common mission or project, that is created for administrative simplicity.

workload

[Computer System] Characterization of the operations comprising a load placed upon a system.

World Wide Node Name (WWNN)

[Fibre Channel] A [Node Name](#) that is worldwide unique

World Wide Port Name (WWPN)

[Fibre Channel] A [Port Name](#) that is worldwide unique.

Worldwide_Name (WWN)

[Fibre Channel] A [Name Identifier](#) that is worldwide unique, and represented by a 64-bit value.

WORM

[Storage System] Acronym for [Write Once Read Many](#).

worm

[Data Security] Malicious software capable of autonomous replication without the necessity for embedding itself in another entity (program, etc.).

Write Amplification

[Storage System] Increase in the number of write operations by the device beyond the number of write operations requested by hosts.

Examples: In flash storage this may happen because of [garbage collection](#). In filesystems this may happen because writes to data blocks generally also require writes to inode blocks.

See JEDEC JESD218A,2/11

write amplification factor

[Storage System] The ratio of the number of write operations on the device to the number of write operations requested by the host.

I.e., $WAF = \text{Device Write Ops} / \text{Host Write Ops}$.

write back cache

[Computer System] A caching technique in which the completion of a write request is signaled as soon as the data is in [cache](#), and actual writing to non-volatile [media](#) occurs at a later time.

Write-back cache includes an inherent [risk](#) that an application will take some action predicated on the write completion signal, and a system failure before the data is written to non-volatile media will cause media contents to be inconsistent with that subsequent action. For this reason, good write-back cache implementations include mechanisms to preserve cache contents across system failures (including power failures) and to flush the cache at system restart time. See [write through cache](#).

W

write consolidation

[Storage System] The process of accumulating the data for a number of sequential write requests in a [cache](#), and performing a smaller number of larger write requests to achieve more efficient device utilization.

write hole

[Storage System] A potential data corruption problem for [parity RAID](#) technology resulting from an [array](#) failure while application

I/O is outstanding, followed by an unrelated [member disk](#) failure (some time after the array has been returned to service).

Data corruption can occur if member data and parity become inconsistent due to the array failure, resulting in a false [regeneration](#) when data from the failed member disk is subsequently requested by an application. Parity RAID implementations typically include mechanisms to eliminate the possibility of write holes.

Write Once Read Many (WORM)

[Storage System] A type of storage, designed for [fixed content](#), that preserves what is written to it in an immutable fashion.

Optical disks are an example of WORM storage.

write penalty

[Storage System] Low apparent application write performance to [RAID](#) arrays' virtual disks.

The write penalty is inherent in RAID [data protection](#) techniques, which require multiple disk I/O requests for each application write request, and ranges from minimal (mirrored arrays) to substantial (RAID Levels 5 and 6). Many RAID array designs include features such as write-back [cache](#) specifically to minimize the write penalty.

write through cache

[Computer System] A caching technique in which the completion of a write request is not signaled until data is safely stored on non-volatile [media](#).

Write performance with a write-through [cache](#) is approximately that of a non-cached system, but if the data written is also held in cache, subsequent read performance may be dramatically improved. See [write back cache](#).

**X_ID**

[Fibre Channel] Acronym for [Exchange Identifier](#).

XAM

[Standards] Acronym for [eXtensible Access Method](#).

XAM API

[Standards] The methods that a [XAM](#) Application uses to communicate with XAM enabled storage, via the XAM [Library](#).

XAM Storage System

[Storage System] A storage system that provides [XAM](#)-compliant storage services.

Typically this type of storage system is used for data that is not expected to change during its lifetime (e.g., [fixed content](#), [reference information](#), archival data). The contents of a XAM Storage System are exposed to applications via one or more [XSystem](#) objects in the [XAM API](#).

XML

[General] Acronym for [eXtensible Markup Language](#).



XSet

[Storage System] The primary stored object abstraction in [XAM](#).

An XSet binds data and [metadata](#) into a single entity that is stored and retrieved as a unit. [MIME](#) types are used to specify data and metadata formats.

XSystem

[Storage System] A logical container of XSets independent of the means (e.g., communication) used to access [XSet](#) contents.

An XSystem is visible to [XAM](#) applications as an abstraction in the [XAM API](#).

XTS-AES

[Data Security] An [encryption](#) mode developed for [data at rest](#) protection, specified in the IEEE Std 1619-2007 "Cryptographic Protection of Data on [Block](#)-Oriented Storage Devices."

**YB****YByte**

[General] Shorthand for [Yottabyte](#).

Ybit

[General] Shorthand for [Yottabit](#).

Yibit

[General] Shorthand for [Yobibit](#).

YiB**YiByte**

[General] Shorthand for [Yobibyte](#).

Yobibit (Yibit)

[General] Shorthand for 1,208,925,819,614,629,174,706,176 (2^{80}) bits.

Binary notation is most commonly used for semiconductor memory sizes.

See also [Yottabit](#).

Yobibyte (YiB)

[General] Shorthand for 1,208,925,819,614,629,174,706,176 (2^{80}) bytes.

Binary notation is most commonly used for semiconductor memory sizes.

See also [Yottabyte](#).

Yottabit (Ybit)

[General] Shorthand for 1,000,000,000,000,000,000,000 (10^{24}) bits.

The SNIA uses the base 10 convention commonly found in I/O-related and scientific literature rather than the base 2 convention (1,208,925,819,614,629,174,706,176, i.e., 2^{80}) common in computer system and software literature.

See also [Yobibit](#).

Yottabyte (YB)

[General] Shorthand for 1,000,000,000,000,000,000,000 (10^{24}) bytes.

The SNIA uses the base 10 convention commonly found in I/O-related and scientific literature rather than the base 2 convention (1,208,925,819,614,629,174,706,176, i.e., 2^{80}) common in computer system and software literature.

See also [Yobibyte](#).

Z

ZB

ZByte

[General] Shorthand for [Zettabyte](#).

Zbit

[General] Shorthand for [Zettabit](#).

Zebibit (Zibit)

[General] Shorthand for 1,180,591,620,717,411,303,424 (2^{70}) bits.

Binary notation is most commonly used for semiconductor memory sizes.

See also [Zettabit](#).

Zebibyte (ZiB)

[General] Shorthand for 1,180,591,620,717,411,303,424 (2^{70}) bytes.

Binary notation is most commonly used for semiconductor memory sizes.

See also [Zettabyte](#).

Z

zero filling

[Data Security] The process of filling unused storage locations in an [information system](#) with the representation of the [character](#) denoting "0".

zero-day event

[Data Security] First release of [malware](#) exploiting a previously undisclosed [vulnerability](#).

zeroing

[File System] The process of writing zeroes (0x00) to all the bytes in a [block](#) or an entire disk before delivering it for use, or upon its release from use.

Zeroing renders any data formerly stored on the block or device inaccessible except by forensic means such as magnetic force microscopy and other techniques that physically scan the [storage media](#).

zeroization

[Data Security] The process of removing or eliminating keys from a cryptographic program or device to prevent their use in the event of capture.

The term stems from the original practice of overwriting the keys with zeroes; arbitrary bit patterns unrelated to the keys themselves are also sometimes used.

Zettabit (Zbit)

[General] Shorthand for 1,000,000,000,000,000,000,000 (10²¹) bits.

The SNIA uses the base 10 convention commonly found in I/O-related and scientific literature rather than the base 2 convention (1,180,591,620,717,411,303,424, i.e., 2⁷⁰) common in computer system and software literature.

See also [Zebibit](#).

Zettabyte (ZB)

[General] Shorthand for 1,000,000,000,000,000,000,000 (10²¹) bytes.

The SNIA uses the base 10 convention commonly found in I/O-related and scientific literature rather than the base 2 convention (1,180,591,620,717,411,303,424, i.e., 2⁷⁰) common in computer system and software literature.

See also [Zebibyte](#).

ZiB

ZiByte

[General] Shorthand for [Zebibyte](#).

Zibit

[General] Shorthand for [Zebibit](#).

zone

[Fibre Channel] A collection of [Fibre Channel](#) N_Ports and/or NL_Ports (i.e., device ports) that are permitted to communicate with each other via the fabric.

Any two N_Ports and/or NL_Ports that are not members of at least one common zone are not permitted to communicate via the fabric. Zone membership may be specified by: 1) port location on a [switch](#), (i.e., Domain_ID and port number); or, 2) the device's [N_Port_Name](#); or, 3) the device's [address identifier](#); or, 4) the device's [Node_Name](#). Well-known addresses are implicitly included in every zone.

zone set

[Fibre Channel] A set of [zone](#) definitions for a fabric.

Zones in a zone set may overlap (i.e., a port may be a [member](#) of more than one zone). Fabric management may support switching between zone sets to enforce different access restrictions (e.g., at different times of day).

zoning

[Fibre Channel] A method of subdividing a [storage area network](#) into disjoint *zones*, or subsets of nodes on the network.

Storage area network nodes outside a zone—except those with well-known addresses—are invisible to nodes within the zone. Moreover, with switched SANs, traffic within each zone may be physically isolated from traffic outside the zone.