ISO/IEC 24775-1

Edition 1.0 2014-10

INTERNATIONAL STANDARD

colour inside

Information technology – Storage management – Part 1: Overview

ISO/IEC 24775-1:2014-10(en)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
www.iec.ch

About the IEC
The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications
The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

IEC Catalogue - webstore.iec.ch/catalogue
The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

IEC publications search - www.iec.ch/searchpub
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and also once a month by email.

Electropedia - www.electropedia.org
The world's leading online dictionary of electronic and electrical terms containing more than 30 000 terms and definitions in English and French, with equivalent terms in 14 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
More than 55 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

IEC Customer Service Centre - webstore.iec.ch/csc
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: csc@iec.ch.

ISO/IEC 24775-1

Edition 1.0 2014-10

INTERNATIONAL STANDARD

Information technology – Storage management – Part 1: Overview

INTERNATIONAL ELECTROTECHNICAL COMMISSION

PRICE CODE D

ICS 35.200

ISBN 978-2-8322-1892-1

CONTENTS

INFORMATION TECHNOLOGY – STORAGE MANAGEMENT –

Part 1: Overview

FOREWORD

1) ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

2) The formal decisions or agreements of IEC and ISO on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees and ISO member bodies.

3) IEC, ISO and ISO/IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees and ISO member bodies in that sense. While all reasonable efforts are made to ensure that the technical content of IEC, ISO and ISO/IEC publications is accurate, IEC or ISO cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.

4) In order to promote international uniformity, IEC National Committees and ISO member bodies undertake to apply IEC, ISO and ISO/IEC publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any ISO, IEC or ISO/IEC publication and the corresponding national or regional publication should be clearly indicated in the latter.

5) ISO and IEC do not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. ISO or IEC are not responsible for any services carried out by independent certification bodies.

6) All users should ensure that they have the latest edition of this publication.

7) No liability shall attach to IEC or ISO or its directors, employees, servants or agents including individual experts and members of their technical committees and IEC National Committees or ISO member bodies for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication of, use of, or reliance upon, this ISO/IEC publication or any other IEC, ISO or ISO/IEC publications.

8) Attention is drawn to the normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.

9) Attention is drawn to the possibility that some of the elements of this ISO/IEC publication may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

International Standard ISO/IEC 24775-1 was prepared by subcommittee 25: Interconnection of information technology equipment, of ISO/IEC joint technical committee 1: Information technology.

This International Standard, together with ISO/IEC 24775-2 to ISO/IEC 24775-8, replaces ISO/IEC 24775, second edition, published in 2011, and constitutes a technical revision.

The significant technical changes with respect to the previous edition are listed in the INTRODUCTION.

The list of all currently available parts of the ISO/IEC 24775 series, under the general title *Information technology – Storage management*, can be found on the IEC web site.

This International Standard is to be used in conjunction with all other parts of this series of standards.

This International Standard has been approved by vote of the member bodies, and the voting results may be obtained from the address given on the second title page.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

IMPORTANT – The "colour inside" logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this publication using a colour printer.

INTRODUCTION

The Overview part of the Storage Management International Standard contains informative clauses that provide an overview of how SMI-S works. It is a useful base for understanding the details of the standard. While the normative information of the ISO/IEC 24775 series of standards is contained in other parts, ISO/IEC 24775-1 provides high-level introductory material on key concepts.

ISO/IEC 24775 is subdivided into the following parts:

- *Information technology – Storage management – Part 1: Overview*
- *Information technology – Storage management – Part 2: Common architecture*
- *Information technology – Storage management – Part 3: Common profiles*
- *Information technology – Storage management – Part 4: Block devices*
- *Information technology – Storage management – Part 5: Filesystems*
- *Information technology – Storage management – Part 6: Fabric*
- *Information technology – Storage management – Part 7: Host elements*
- *Information technology – Storage management – Part 8: Media libraries*

The significant changes with respect to the second edition of ISO/IEC 24775 are listed below.

- **Improved organization**. The International Standard has been reorganized into eight parts to provide more information more easily. The parts are:
  - *Part 1 Overview*: The overview book provides a high level overview of the ISO/IEC 24775 series of standards.
  - *Part 2 Common Architecture*: This part covers general information about the interface, such as security and protocols.
  - *Part 3 Common Profiles*: This part covers component profiles that extend profiles in other books, such as target ports and job control.
  - *Part 4 Block Devices*: This part covers storage profiles that support various forms of disk storage.
  - *Part 5 Filesystems*: This part covers profiles that support filesystems, such as NAS (Network Attached Storage).
  - *Part 6 Fabric*: This part covers profiles that deal with interconnection of host servers and storage devices, such as switches.
  - *Part 7 Host Elements*: This part covers profiles for storage software on host servers, such as disk partitioning and Host Hardware RAID controllers.
  - *Part 8 Media Libraries*: This part covers profiles that deal with removable media such as tape libraries.
- **Maturity identification.** As material is added to the standard it goes through various stages of maturity. The initial stage is *Experimental*, which is material that has not yet been implemented and is subject to change. The other stages indicate the degree of implementations. The stages are:
  - **Experimental**: Full design review, no commercial implementations.
  - **Implemented**: Initial implementations available, may be removed at minor revision.
  - **Stable**: Three or more vendors have implemented the identified material, backward compatibility assured, removed only at major revision.
  - **Finalized**: Relies solely on Finalized content, deprecated only at major revision.

- **Deprecated**: Obsolete material, may be removed in future revisions.

  For a more detailed explanation of each maturity level and its typographical indication, see Clause 4 Typographical conventions.

- **Expanded scope.** The range of SAN components modeled by the profiles defined in the parts has been greatly expanded.
  - New profiles include:
    - *Part 3 Common Profiles:* Serial Attached SCSI (SAS) Target Port, Serial ATA (SATA) Target Ports, SB Target Port, SAS Initiator Ports, ATA Initiator Ports, FC-SB-x Initiator Ports, FCoE Initiator Ports, Power Supply, Fan, Sensors, Base Server, Media Access Device, Storage Enclosure, Software Inventory, Profile Registration, Proxy Server System Management, Operational Power.
    - *Part 4 Block Devices:* Block Storage Views, CKD Block Services, Erasure, Storage Server Asymmetry, Volume Composition, Storage Element Protection, Replication Services, Pools from Volumes, Group Masking and Mapping, Thin Provisioning.
    - *Part 5 Filesystems:* File Export, File Server Manipulation, File Storage, Filesystem, Filesystem Copy Services, Filesystem Performance, Filesystem Quotas, NAS Network Port, Host Filesystem, Filesystem Remote Copy Services.
    - *Part 6 Fabric:* Fibre Channel Security, Fabric Views, Virtual Fabrics, Switch Partitioning, SAS Expander, N Port Virtualizer, Inter Fabric Routing.
    - *Part 7 Host Elements:* Storage HBA, Host Hardware RAID Controller.
    - *Part 8 Media Libraries:* Partitioned Tape Library, Virtual Tape Library, Virtual Tape Library Copy and Library Views.
  - The following experimental profiles were removed from the International Standard:
    - *Part 3 Common Profiles:* Security, 3rd Party Authentication, Authorization, Credential Management, Identity Management, Security Role Based Access Control and Security Resource Ownership.
    - *Part 4 Block Devices:* Pool Management Policy.
  - The following profiles are deprecated:
    - *Part 3 Common Profiles:* Cascading (replaced by direct use of cascading classes).
    - *Part 4 Block Devices:* Volume Management (not replaced).
    - *Part 6 Fabric:* Router (not replaced).
    - *Part 7 Host Elements:* FC HBA (replaced by Storage HBA), SB Multipath Management (not replaced).
    - *Part 8 Media Libraries:* InterLibraryPort Connection (not replaced).
  - In addition, many of the existing profiles have been enhanced.

This International Standard was prepared by the SNIA (Storage Networking Industry Association)[1]. The standard is often referred to as ***SMI-S*** (*Storage Management Initiative Specification*).

1. Storage Networking Industry Association, 425 Market Street, Suite 1020, San Francisco, CA 94105, U.S.A., http://www.snia.org

INFORMATION TECHNOLOGY – STORAGE MANAGEMENT –

Part 1: Overview

1 Scope

This part of ISO/IEC 24775 defines an interface for the secure, extensible, and interoperable management of a distributed and heterogeneous storage system. This interface uses an object-oriented, XML-based, messaging-based protocol designed to support the specific requirements of managing devices and subsystems in this storage environment. Using this protocol, this part of ISO/IEC 24775 describes the information available to a WBEM Client from an Information Technology – Storage Management compliant CIM WBEM Server.

2 Normative references

The following documents, in whole or in part, are normatively referenced in the document and are indispensible for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document, including any amendments, applies.

ISO/IEC 24775-2, *Information technology – Storage management – Part 2: Common architecture*

ISO/IEC 24775-3, *Information technology – Storage management – Part 3: Common profile*

3 Terms, definitions, symbols, abbreviations, and conventions

For the purposes of this document, the terms, definitions, symbols, abbreviations, and conventions given in ISO/IEC 24775-2:2014 apply.

4 Typographical conventions

4.1 Maturity model

In addition to informative and normative content, this International Standard includes guidance about the maturity of emerging material that has completed a rigorous design review but has limited implementation in commercial products. This material is clearly delineated as described in Clause 4. The typographical convention is intended to provide a sense of the maturity of the affected material, without altering its normative content. By recognizing the relative maturity of different sections of the International Standard, an implementer should be able to make more informed decisions about the adoption and deployment of different portions of the International Standard in a commercial product.

This International Standard has been structured to convey both the formal requirements and assumptions of the Information Technology – Storage Management API and its emerging implementation and deployment lifecycle. Over time, the intent is that all content in the International Standard will represent a mature and stable design, be verified by extensive implementation experience, assure consistent support for backward compatibility, and rely solely on content material that has reached a similar level of maturity. Unless explicitly labeled with one of the subordinate maturity levels defined for this International Standard, content is assumed to satisfy these requirements and is referred to as “Finalized”. Since much of the evolving International Standard content in any given release will not have matured to that level, this International Standard defines three subordinate levels of implementation maturity that identify important aspects of the content’s increasing maturity and stability. Each subordinate maturity level is defined by its level of implementation experience, its stability and its reliance on other emerging standards. Each subordinate maturity level is identified by a unique typographical tagging convention that clearly distinguishes content at one maturity model from content at another level.

4.2 Experimental maturity level

No material is included in this International Standard unless its initial architecture has been completed and reviewed. Some content included in this International Standard has complete and reviewed design, but lacks implementation experience and the maturity gained through implementation experience. This content is included in order to gain wider review and to gain implementation experience. This material is referred to as “Experimental”. It is presented here as an aid to implementers who are interested in likely future developments within the SMI International Standards. The contents of an Experimental profile may change as implementation experience is gained. There is a high likelihood that the changed content will be included in an upcoming revision of the International Standard. Experimental material can advance to a higher maturity level as soon as implementations are available. Figure 1 is a sample of the typographical convention for Experimental content.

EXPERIMENTAL

Experimental content appears here.

EXPERIMENTAL

Figure 1 – Experimental maturity level tag

4.3 Implemented maturity level

Profiles for which initial implementations have been completed are classified as “Implemented”. This indicates that at least two different vendors have implemented the profile, including at least one provider implementation. At this maturity level, the underlying architecture and modeling are stable, and changes in future revisions will be limited to the correction of deficiencies identified through additional implementation experience. Should the

material become obsolete in the future, it shall be deprecated in a minor revision of the International Standard prior to its removal from subsequent releases. Figure 2 is a sample of the typographical convention for Implemented content.

IMPLEMENTED

Implemented content appears here.

IMPLEMENTED

Figure 2 – Implemented maturity level tag

4.4 Stable maturity level

Once content at the Implemented maturity level has garnered additional implementation experience, it can be tagged at the Stable maturity level. Material at this maturity level has been implemented by three different vendors, including both a provider and a client. Should material that has reached this maturity level become obsolete, it may only be deprecated as part of a minor revision to the International Standard. Material at this maturity level that has been deprecated may only be removed from the International Standard as part of a major revision. A profile that has reached this maturity level is guaranteed to preserve backward compatibility from one minor International Standard revision to the next. As a result, Profiles at or above the Stable maturity level shall not rely on any content that is Experimental. Figure 3 is a sample of the typographical convention for Implemented content.

STABLE

Stable content appears here.

STABLE

Figure 3 – Stable maturity level tag

4.5 Finalized maturity level

Content that has reached the highest maturity level is referred to as “Finalized.” In addition to satisfying the requirements for the Stable maturity level, content at the Finalized maturity level shall solely depend upon or refine material that has also reached the Finalized level. If International Standard content depends upon material that is not under the control of the SNIA, and therefore not subject to its maturity level definitions, then the external content is evaluated by the SNIA to assure that it has achieved a comparable level of completion, stability, and implementation experience. Should material that has reached this maturity level become obsolete, it may only be deprecated as part of a major revision to the International Standard. A profile that has reached this maturity level is guaranteed to preserve backward compatibility from one minor International Standard revision to the next. Over time, it is hoped that all International Standard content will attain this maturity level. Accordingly, there is no special typographical convention, as there is with the other, subordinate maturity levels. Unless content in the International Standard is marked with one of the typographical conventions defined for the subordinate maturity levels, it should be assumed to have reached the Finalized maturity level.

4.6 Deprecated material

Non-Experimental material can be deprecated in a subsequent revision of the International Standard. Sections identified as “Deprecated” contain material that is obsolete and not recommended for use in new development efforts. Existing and new implementations may still

use this material, but shall move to the newer approach as soon as possible. The maturity level of the material being deprecated determines how long it will continue to appear in the International Standard. Implemented content shall be retained at least until the next revision of the specialization, while Stable and Finalized material shall be retained until the next major revision of the International Standard. Providers shall implement the deprecated elements as long as it appears in the International Standard in order to achieve backward compatibility. Clients may rely on deprecated elements, but are encouraged to use non-deprecated alternatives when possible.

Deprecated sections are documented with a reference to the last published version to include the deprecated section as normative material and to the section in the current International Standard with the replacement. Figure 4 contains a sample of the typographical convention for deprecated content.

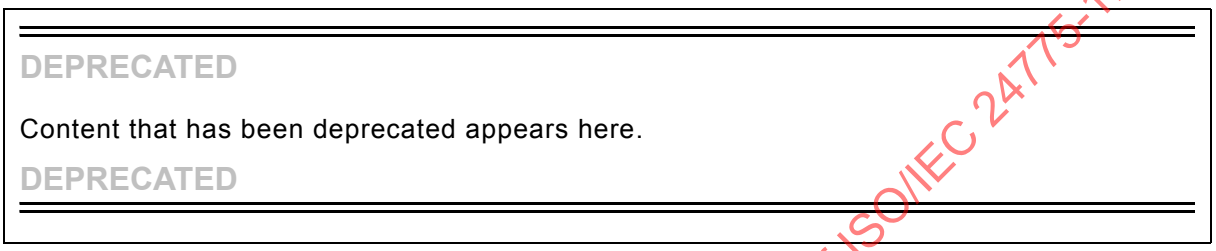

Figure 4 – Deprecated tag

5 Storage management introduction

5.1 Preamble

Large Storage Systems and Storage Area Networks (SANs) are emerging as a prominent and independent layer of IT infrastructure in enterprise class and midrange computing environments. Examples of applications and functions driving the emergence of new storage technology include:

- Sharing of vast storage resources between multiple systems via networks,
- LAN free backup,
- Remote, disaster tolerant, on-line mirroring of mission critical data,
- Clustering of fault tolerant applications and related systems around a single copy of data.
- Archiving requirements for sensitive business information.
- Distributed database and file systems.

To accelerate the emergence of more functional and sophisticated storage systems in the market, the industry requires a standard management interface that allows different classes of hardware and software products supplied by multiple vendors to reliably and seamlessly interoperate for the purpose of monitoring and controlling resources. The SNIA Storage Management Initiative (SMI) was created to develop this standard (SMI-Specification or SMI-S), the definition of that interface. This standard provides for heterogeneous, functionally rich, reliable, and secure monitoring/control of mission critical global resources in complex and potentially broadly-distributed, multi-vendor storage topologies like SANs. As such, this interface overcomes the deficiencies associated with legacy management systems that deter customer uptake of more advanced storage management systems.

5.2 Business rationale

This interface is targeted at creating broad multi-vendor management interoperability and thus increasing customer satisfaction. To that end, this standard defines an “open” and extensible interface that allows subsystems and devices within the global context of a large storage system to be reliably and securely managed by overlying presentation frameworks and management systems in the context of the rapidly evolving multi-vendor market. In specific, SAN integrators (like end-users, VARs, and SSPs) can, via this standardized management interface, more flexibly select between multiple vendors when building the hierarchy of software systems required to manage a large storage system independent of the underlying hardware systems. Additionally, storage integrators can more flexibly select between alternate hardware vendors when constructing storage configurations. Broad adoption of the standards defined and extended in this standard will provide increased customer satisfaction and will:

- more rapidly expand the acceptance of new storage management technology like SANs and iSCSI;
- accelerate customer acquisition of new storage management technology;
- expand the total market.

Additionally, a single common management interface allows SAN vendors and integrators to decrease the time required to bring new more functional technology, products, and solutions to market.

5.3 Interface definition

This management interface allows storage management systems to reliably identify, classify, monitor, and control physical and logical resources in a storage system. The fundamental relationship of this interface to storage management software, presentation frameworks, user

applications, SAN physical entities (i.e., devices), SAN discovery systems, and SAN logical entities is illustrated in Figure 5.

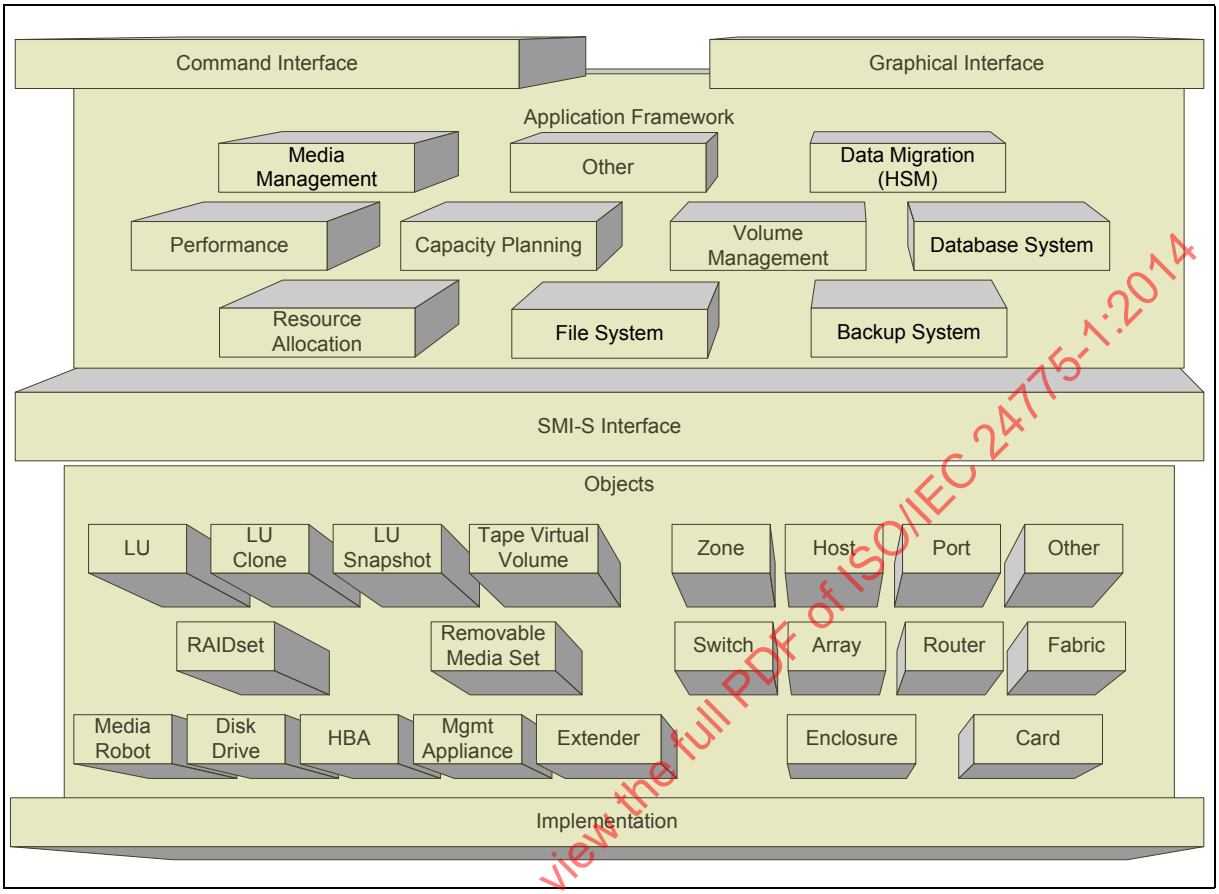

Figure 5 – Interface functions

Figure 5 illustrates that functions of the interface can be distributed across multiple devices (i.e., Switches or Array Controllers) and/or software systems (i.e., Discovery Systems). While the functionality of the interface is distributed within or across a storage environment, to insure that monitoring and control operations by clients are consistent and reliable, the state of a given resource is not certain to be valid if it is simultaneously available to clients from multiple unsynchronized sources.

EXAMPLE A request by an SRM application and a backup engine for the bandwidth available on a given Fibre Channel path should be coordinated by a single monitoring entity to insure information consistency. If the SRM application and Backup engine obtain different available bandwidth information for a given Fibre Channel path from multiple unsynchronized sources they could function in conflict and degrade the efficiency of the environment.

Addressing this concern is the responsibility of parties configuring Storage and Network management clients that rely on the primitives defined in the standard.

NOTE 1 Within this architecture (as depicted by Figure 5) entities like an appliance-based volume manager may potentially act as both a client and a server to the interface.

EXAMPLE A Host-based volume manager wants to construct a large storage pool from multiple SAN appliance based volumes, as well as volumes/LUNs originating from array controllers. In this case, the host based volume manager needs to inspect the characteristics of the volumes on both the SAN appliance and array controller prior to allocation. Additionally, the SAN appliance (which runs a volume manager) needs to inspect the properties of storage devices when building its volumes. As such, the SAN appliance in this case is both a client and server in the management environment, depending on the action being performed.

Figure 5 includes a number of strategic functional requirements for the interface. These capabilities will be introduced to the interface implementation over time, and may not be

present in this version of the interface. The functionalities required to fully satisfy the needs of clients using a storage management interface include:

a) clients need to be able to obtain sufficient information to discern the topology of the SAN or complex storage system;

b) clients need to be able to reliably identify resources that have experienced an error/fault condition that has resulted in degraded/disabled operation;

c) clients need to be able to construct a zone of allocation around a select group of host and storage resources;

d) clients need to be able to identify nonvolatile storage resources available to a storage management system, to allow them to construct a storage pool of a consistent level of performance and availability;

e) clients need to be able to identify third-party copy engines (and associated media libraries/ robots) available to a cooperating backup engine, allowing it to allocate an engine/library/ robot to a given backup task;

f) clients need to be able to dynamically allocate non-volatile storage resources;

g) each volume to be utilized is subject to strict availability and performance requirements. As a result, the file system needs to inspect the properties of each volume prior to allocation.

h) clients need to be able to access sufficient topology and component information to allow a Storage Resource Management (SRM) application like a performance monitor to examine topology and line utilization, such that performance bottlenecks can be exposed and capacity planning performed;

i) clients need to be able to employ appropriate data reporting and tracking to allow capacity planning system to identify each storage pool in the SAN and then interact with the manager of each pool to assess utilization statistics;

j) clients need to be provided with adequate controls for a privileged, user-written application to restrict the use of a volume to a specific host, set of hosts, or set of controller communications ports;

k) clients need to be assured of timely propagation of data concerning the health and performance of the devices and subsystems in the SAN to fault isolation and analysis systems.

Example non-goals for this interface include:

a) the ability to select a logical communications port over which to send/receive data;

b) the ability to read or write data to a volume;

c) the ability to identify and recover from data communications errors and failures;

d) the ability to log a new communications device into a network.

5.4 Technology trends

To be broadly embraced and long lived this management interface should respect and leverage key technology trends evolving within the industry. These include:

a) *Improved Connectivity*: Whether available In-band (i.e., over Fibre Channel/iSCSI) or available out-of-band (i.e., over a LAN/MAN/WAN), or available over a mix of both, virtually all devices in a storage management environment have (or soon will have), access to a common communications transport suitable for carrying management information content (e.g., TCP/IP), that is used to transmit a standardized encoding (e.g., a WBEM Protocol) of recognized semantics (e.g., CIM).

b) *Increased Device Manageability*: Through a common, general-purpose network transport, provide the option to provide proxy services to provide access to (e.g., general purpose computer system) devices via this standardized management interface.

EXAMPLE A legacy array controller is incapable of running the software necessary to implement a management server for this interface and uses a proxy server on a SAN appliance to communicate within the management environment.

EXAMPLE An HBA is incapable of running the software necessary to implement a management server for this interface and uses a proxy server on its host system to communicate within the management environment.

c) *XML Standardization:* XML is providing the ability to create management protocols with an extensible, platform independent, human readable, content describable communication language. This streamlines the task of developing infrastructure to support his interface and debug systems around the interface.

d) *Object Independent Protocols*: These protocols provide appropriate abstraction – separating the definition of the object model from the semantics/syntax of the protocol. Additionally, the transport-independent, content-description (i.e., markup) nature of XML allows it to be utilized by both web-enabled application and appliances.

e) *Increased SAN Complexity*: SANs are being configured with diverse classes of components and widely distributed topologies. Management clients and servers in the environment need to anticipate being widely distributed on systems, appliances and devices throughout large SAN topologies, while maintaining real-time distributed state for logical entities. Figure 6 provides an example of a single SAN built from multiple classes of components spanning three physical locations (i.e., Sites A, B and C).

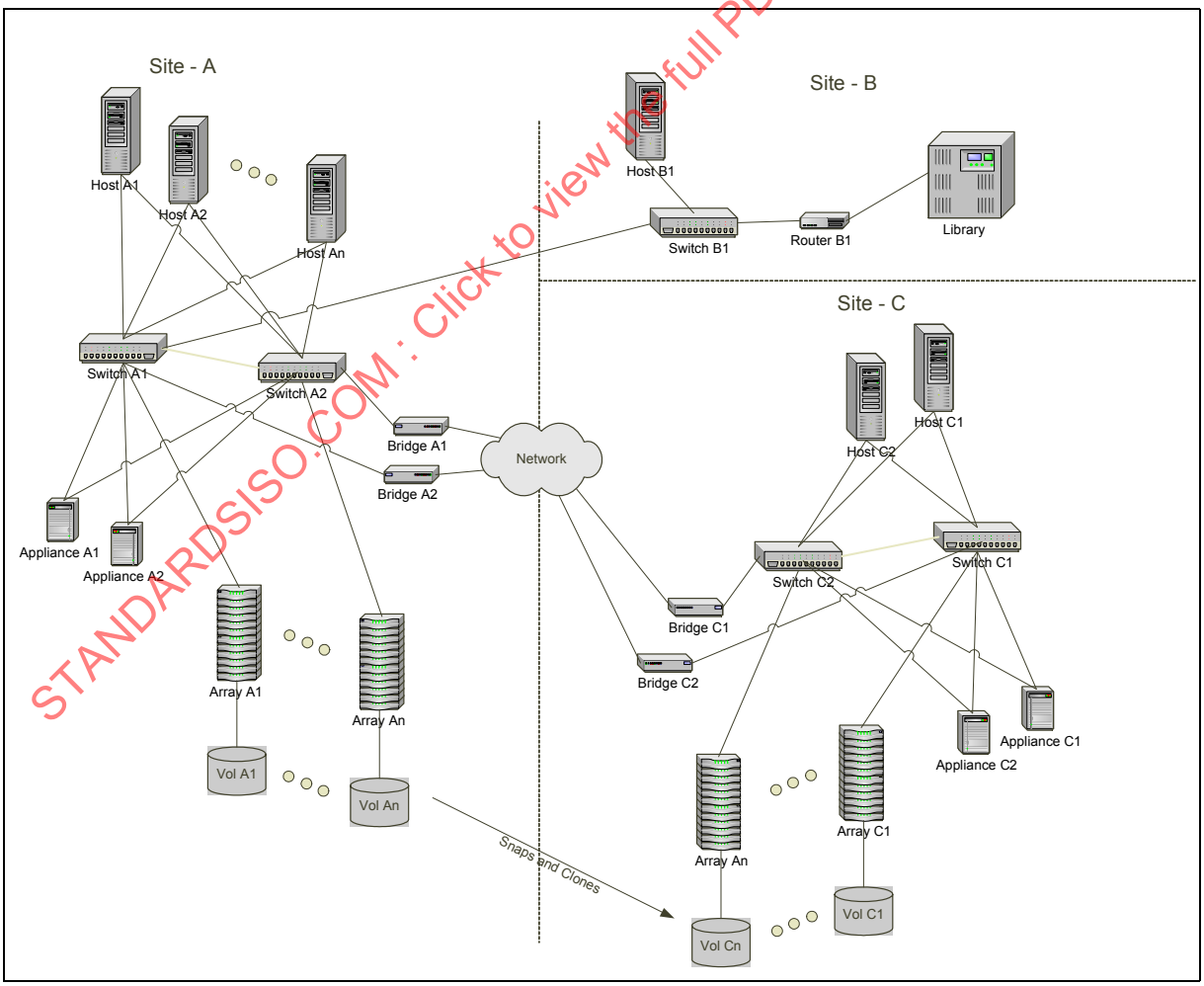

Figure 6 – Large SAN topology

5.5 Management environment

Clients and Servers of this interface can be widely distributed on systems, appliances, and devices across a network that includes one or more large SAN topologies.

The configuration in Figure 7 provides an example client/server distribution using in-band TCP/IP communications, out of band TCP/IP communications, or employing proxy services to bridge legacy and/or proprietary communication interfaces. The device “Old Array Controller” is incapable of appropriate communication with clients and servers in the management environment to provide management access (i.e., a CIM Server). Access to the communications transport that clients and servers share for communication is achieved via a proxy service on the host computer in the upper right hand corner of Figure 7. All other clients and servers communicate via direct access to a common communications transport.

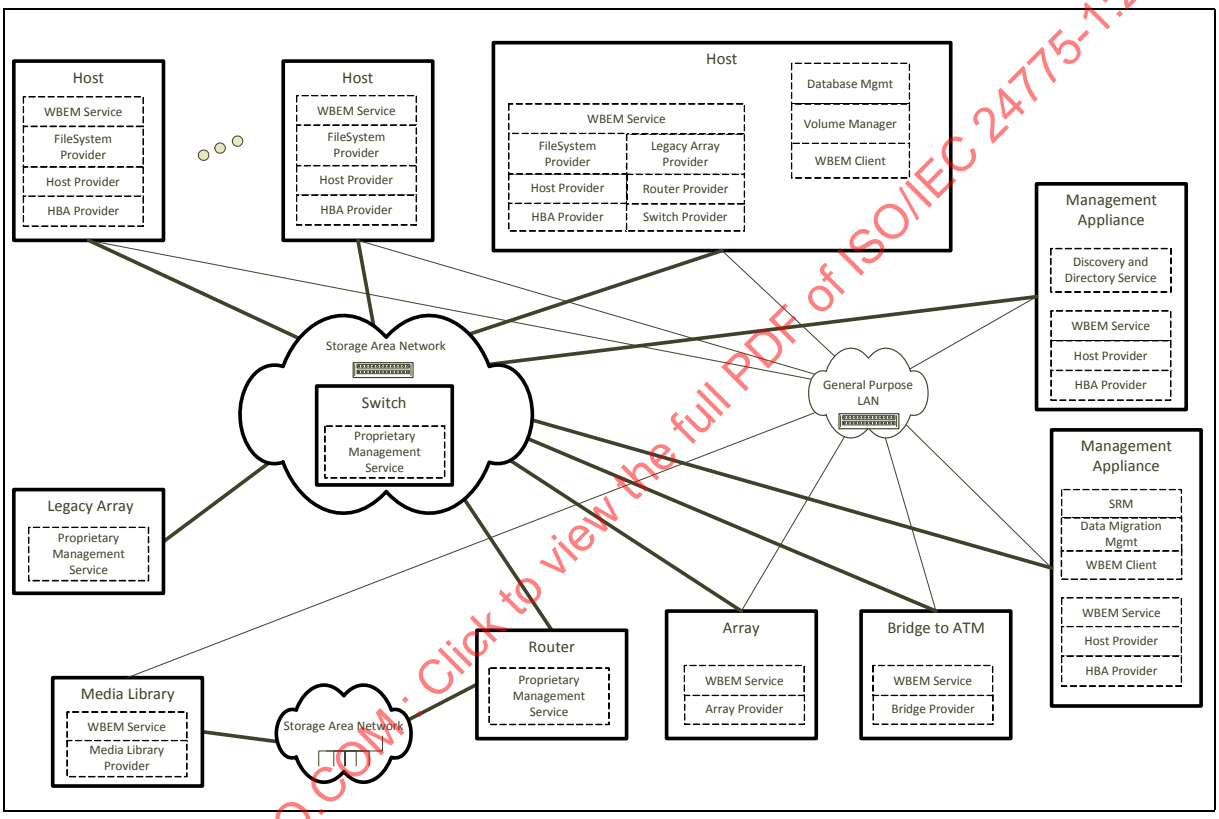

Figure 7 – Example Client Server Distribution in a SAN

5.6 Architectural objectives

The following reflect architectural objectives of the interface. Some of these capabilities are not present in the initial release of the interface, but are inherent in its architecture and intended extensibility. They are intended to provide guidance concerning the present and future direction of development of the Information Technology – Storage Management.

a) Consistency: State within a managed object and between objects remains consistent independent of the number of clients simultaneously exerting control, the distribution of objects in the environment, or the management action being performed.

b) Isolation: A client that needs to execute an atomic set of management actions against one or more managed objects is able to do so in isolation of other clients, who are simultaneously executing management actions against those same objects.

c) Durability: Consistency, and isolation are preserved independent of the failure of any entity or communications path in the management environment.

d) Consistent Name Space: Managed objects in a single management domain adhere to a consistent naming convention independent of state or reliability of any object, device, or subsystem in the SAN.

e) Distributed Security: Monitoring and control operations are secure. The architecture supports:

   1) Client authentication;

   2) Privacy (encryption) of the content of the messages in this protocol;

   3) Client authorization.

f) Physical Interconnect Independence: The interface will function independent of any particular physical interconnect between components, any supplier, or any topology.

g) Multi-vendor Interoperability: Clients and servers should use a common communication transport and message/transfer syntax to promote seamless plug compatibility between heterogeneous multi-vendor components that implement the interface.

h) Scalability: The size, physical distribution, or heterogeneity of the storage system does not degrade the quality or function of the management interface.

i) Vendor Unique Extension: The interface allows vendors to implement proprietary functionality above and beyond the definitions here-in to distinguish their products and services in the market independent of the release of a new version of the interface.

j) Volatility of State: This interface does not assume that objects are preserved in non-volatile repositories. Clients and servers may preserve object state across failures, but object preservation is not mandatory.

k) Replication: This interface provides no support for the automatic replication of object state within the management environment.

l) Functional Layering Independence: The design of this interface is independent of any functional layering a vendor chooses to employ in constructing the storage management systems (hardware and software) necessary to manage a storage environment.

m) Asynchronous or Synchronous execution: Management actions may execute either asynchronously or synchronously.

n) Events: This interface provides for the reliable asynchronous delivery of events to one or more registered clients.

o) Cancelable Management Actions: Long running synchronous or asynchronous directives need to be capable of being cancelled by the client. Cancellation needs to result in the termination of work by the server and resource consumed being released.

p) Durable Reference: Object classes that persist across power cycles and need to be monitored and controlled independent of SAN reconfiguration (i.e., logical volumes) need be identified via “Durable Names” to insure consistent reference by clients..

q) Dynamic installation and reconfiguration: New clients and servers need to be capable of being added to or removed from a Information Technology – Storage Management management environment without disrupting the operation of other clients or servers. In most cases, clients should be capable of dynamically managing new servers that have been added to a Information Technology – Storage Management environment.

r) Automatic discovery of new servers: When new management servers are added to the management system they should automatically become available to management clients without the need for manual configuration by administrations staff.

6 Storage management overview

6.1 Base capabilities

To achieve the architectural objectives and support the key technological trends in Clause 5, this clause describes an extensible, secure, auto-discoverable, object-oriented, XML-based messaging based interface designed to support the specific requirements of managing devices in and through storage systems. The top level protocol that implements this messaging based interface in this revision of the standard is called Web Based Enterprise Management (WBEM) and more specifically CIM/XML over http. To quickly become ubiquitous, Information Technology – Storage Management seeks to the greatest extent possible to leverage a number of existing enterprise management standards through this interface, such as:

- the Distributed Management Task Force (DMTF) authored Common Information Model (CIM) and Web Based Enterprise Management (WBEM) standards,
- the standards written by ANSI on Fibre Channel and SCSI,
- the World Wide Web Consortium (W3C) for standards on XML,
- the Internet Engineering Task Force (IETF) for standards on HTTP, SLP, and iSCSI.

6.2 Object oriented classes

A hierarchy of object classes with properties (a.k.a. attributes) and methods (a.k.a. directives) linked via the Universal Modeling Language (UML) modeling constructs of inheritance and associations defines most of the capabilities of the Information Technology – Storage Management. The SMI-S object model (which constitutes the bulk of this standard) is integrated with and part of the Common Information Model (CIM) at the DMTF. Implementers of this standard are encouraged to consult one of the many publicly available texts on UML or the uml.org web site (www.uml.org) to develop an understanding of UML. A brief tutorial on UML is provided in the introduction material *Information Technology – Storage Management, Part 2 Common Architecture* 7 Object Model General Information in this standard.

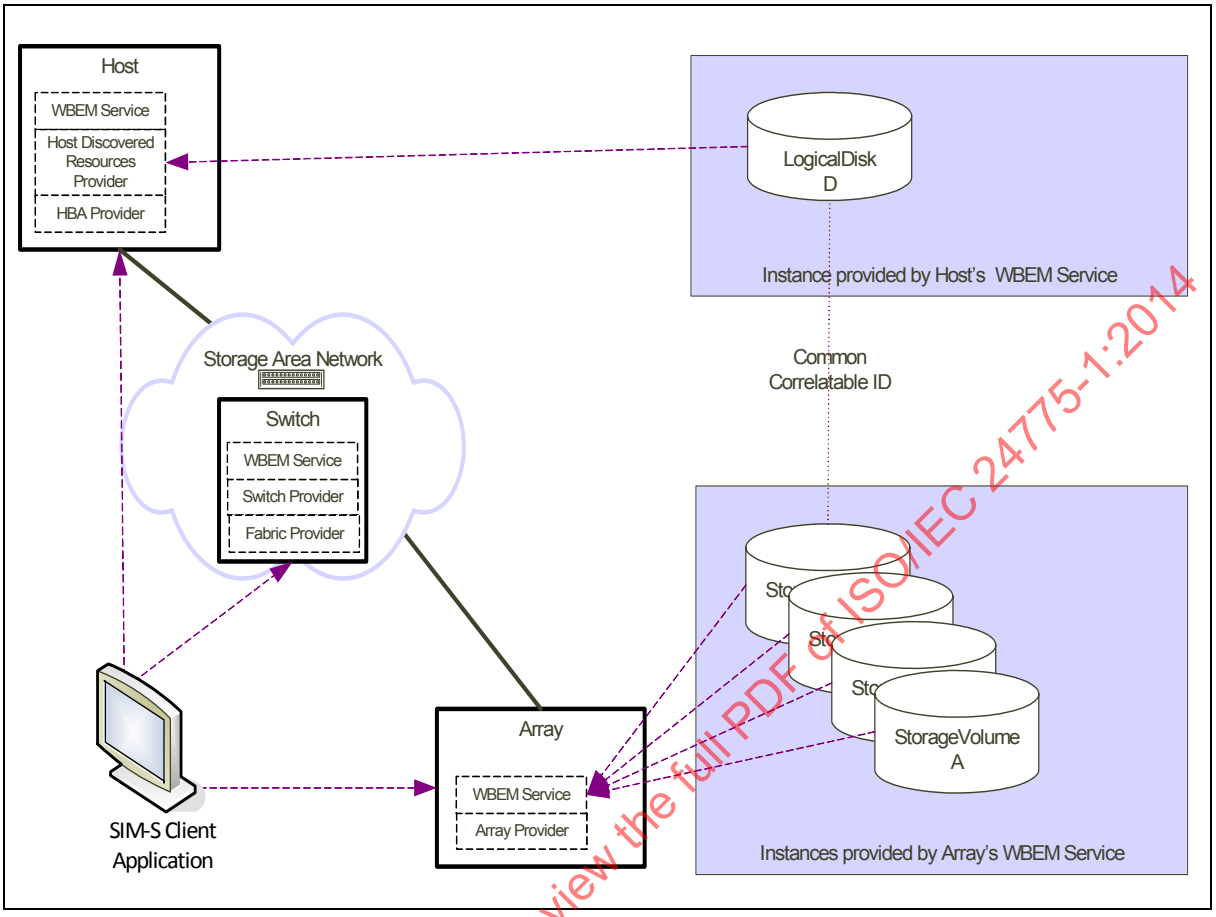

Figure 8 – Object model/server relationship

In Figure 8, an Information Technology – Storage Management client obtains object classes and instances that it can use to manage the storage. At this level of discussion, the focus is on Information Technology – Storage Management conformant WBEM Clients and Servers. The WBEM Servers have providers for the various components that are responsible for the class and association instances that allow the underlying component implementation to be managed.

A standard, object-oriented interface, together with a standard interface protocol, allows WBEM Clients to discover, monitor, and control storage and network devices, regardless of the underlying implementation of those devices.

The goal of this document is to clearly and precisely describe the information expected to be available to a WBEM Client from an Information Technology – Storage Management compliant WBEM Service. It relies upon UML diagrams, easy-to-use tables and machine-readable, CIM-compliant Managed Object Format (MOF) (through the CIM model maintained at the DMTF). This is intended to ease the task of client implementation and to ease the task of using existing WBEM Servers. It should be noted that the MOF Interface Description Language is a precise representation of the object model in this standard, and developers are encouraged to learn this means of expression when implementing this interface. Programmers implementing this interface should reference MOF representations of the object model when faced with implementation decisions.

Information Technology – Storage Management compliant WBEM Servers provide instances in a manner conformant to one or more Information Technology – Storage Management profiles (*Information Technology – Storage Management, Part 3 Common Profiles* 4 Profile Introduction). The object model supporting these instances may be extended by the vendor as long as it remains conformant to the relevant Information Technology – Storage Management profiles. Generally, vendor-unique code is necessary in a WBEM client to take advantage of vendor

defined model extensions. Regardless of the presence of vendor extensions, a generic WBEM client is able to leverage all Information Technology – Storage Management features defined for a supported profile.

Figure 9 illustrates this requirement.

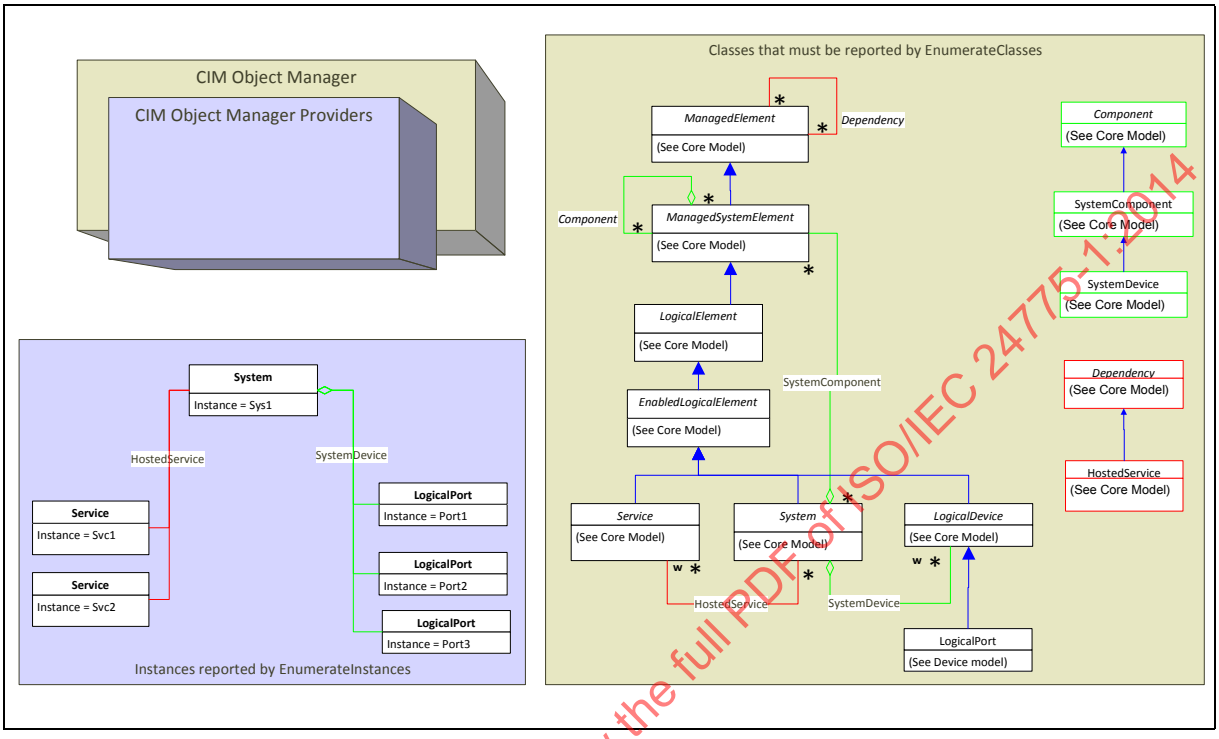

Figure 9 – Canonical inheritance

Figure 9 illustrates that even though a Fibre Channel Switch may only report instances and allow associated method execution for certain objects, when asked by a client to enumerate its Object Classes it reports the entire hierarchy of classes in its tree. Similarly a server that instantiates an array controller reports the complete set of object classes that links it to the base canonical object of the Information Technology – Storage Management model. It is this single canonical root that allows any Information Technology – Storage Management client to discover, map, and operate upon the complete set of objects in a given SAN.

The object model presented in this standard is intended to facilitate interoperability not limiting the expression of unique features that differentiate manufacturers in the market. For this reason, the object model provided only serves as a"core" to compel multi-vendor interoperability. In the interest of gaining a competitive advantage, a given vendor's implementation of the interface may include additional object classes, properties, methods, events, and associations around this "core". These vendor-unique extensions to the object model may, in select cases (e.g., extrinsic methods), require the modification of client code above and beyond that required to support the core.

6.3 Messaging-based interface

A messaging-based interface, rather than a more traditional procedure call interface, was selected so that platform and language independence could be achieved across the breadth of devices, clients, and manufacturers that may implement the interface. This messaging-based environment also eases the task of transporting management actions over different communications transports and protocols that may emerge as the computer industry evolves.

An example fragment of an Information Technology – Storage Management CIM-XML message is provided in Figure 10.

```
<!DOCTYPE CIM SYSTEM HTTP://www.dmtf.org/cim-v2.dtd/>
<CIMVERSION=”2.0” DTDVersion=”2.0”>
     <CLASS NAME=”ManagedSystemElement”>
        <QUALIFIER NAME=”abstract”></QUALIFIER>
        <PROPERTY NAME=”Caption” TYPE=”string”>
           <QUALIFIER NAME=”MaxLen” TYPE=”sint32”>
              <VALUE>64</VALUE>
           </QUALIFIER>
        </PROPERTY>
        <PROPERTY NAME=”Description” TYPE=”string”></PROPERTY>
        <PROPERTY NAME=”InstallDate” TYPE=”datetime”>
           <QUALIFIER NAME=”MappingStrings” TYPE=”string”>
              <VALUE>MIF.DMTF|ComponentID|001.5</VALUE>
           </QUALIFIER>
        </PROPERTY>
        <PROPERTY NAME=”Status” TYPE=”string”>
           <QUALIFIER NAME=”Values” TYPE=”string” ARRAY=”TRUE”>
              <VALUE>OK</VALUE>
              <VALUE>Error</VALUE>
```

Figure 10 – Sample CIM-XML message

7 Functionality matrix

7.1 Overview

The functionality enabled by this version of Information Technology – Storage Management follows a multi-level model. Within each level of this model, several broad categories of management are described. This creates a functionality matrix, which serves two purposes. First, it organizes a complex set of capabilities enabled by the overall SMI-S approach. Second, it helps to ensure good management functionality coverage for the managed devices comprehended by SMI-S. This clause provides an overview of the functionality matrix approach for describing the management functionality provided by this version of Information Technology – Storage Management. A blank functionality matrix is provided in Table 1.

Table 1 – Functionality matrix

	Fault management	Configuration management	Accounting management	Performance management	Security management
Application Level					
File / Record Level					
Block Level					
Connectivity Level					
Device Level					

7.2 Multi-level model of networked storage management functionality

The lowest level of the multi-level model of networked storage management functionality applies to managing the basic physical aspects of the elements found in a networked storage environment, and the upper levels are involved with managing the different logical levels supported by these managed elements. Each level in this model depends upon the lower levels being in place.

Shown in top-down order, the functionality levels are:

- (Level 5) Application Level Functionality,
- (Level 4) File/Record Level Functionality,
- (Level 3) Block Level Functionality,
- (Level 2) Connectivity Level Functionality,
- (Level 1) Device Level Functionality.

Managed physical elements in a networked storage environment shall support Level 1 functionality, and may support additional functionality levels as well, depending upon the logical capabilities of the managed physical element. The functionality supported by a managed element will normally involve a contiguous set of levels in this model. If a managed physical element supports functionality for a particular upper level, then it will also support functionality for each level between that level and Level 1.

As an example of this last point, consider a NAS Head device. It has a physical component (Level 1). It is connected to other physical components in the networked storage environment (Level 2). It deals with Block storage (Level 3), and it deals with Files (Level 4). A NAS Head device can therefore be expected to support functionality in levels 1 through 4 of this multi-level model of networked storage management functionality. Similarly, a regular NAS device would support management functionality in each of these same levels, although the functionality supported within each level might be slightly different, since the regular NAS device does not have a SAN back-end.

7.3 FCAPS

Within each level of this model, a basic set of functionality is needed that allows management applications to exercise FCAPS capabilities over elements supporting that level. FCAPS is a model of the working objectives of network management, and these same concepts are applied to each of the levels in the multi-level model of networked storage management functionality. A summary of FCAPS capabilities includes:

- **F**ault Management: Identifying, isolating, correcting, and logging managed element faults. Includes running diagnostics, generating fault alarms, and keeping error statistics,
- **C**onfiguration Management: Discovering, configuring, and monitoring managed elements. Includes adding, altering, and removing managed elements,
- **A**ccounting Management: Measuring and tracking usage of managed elements or services. Includes distributing resources, setting quotas, and billing,
- **P**erformance Management: Monitoring of performance, error rate, and utilization metrics for managed elements. Includes setting thresholds, problem reporting, logging of data, and examining historical data
- **S**ecurity Management: Ensuring legitimate use of managed elements or services. Includes checking user access rights, maintaining an audit trail log, generating security events and alarms, and maintaining data confidentiality where necessary.

By specifying FCAPS capabilities within each of its levels, this multi-level model is used to describe the functionality that is provided by SMI-S overall, and by individual profiles and subprofiles. The actual degree of support for FCAPS capabilities within each level is determined by individual SMI-S profiles.

7.4 Management functionality within each level of the model

7.4.1 (Level 1) Device level functionality

This level includes all functionality needed to allow management applications to deal with the physical aspects of managed elements in the networked storage environment. The physical aspects of HBAs, Switches, Storage Systems etc. are handled by functionality in this level. This level also handles functionality that is not exposed to other elements in the networked storage environment, like the managing of storage devices within a Storage System prior to their being allocated to storage pools that are accessible over the data network.

7.4.2 (Level 2) Connectivity level functionality

This level includes all functionality associated with allowing management applications to deal with the logical aspects of the managed connectivity between physical elements in the networked storage environment. This level is where things like Fibre Channel Fabrics and Zones are handled, and is also where iSCSI Sessions are handled. This level also handles the logical aspects of switch and extender connectivity.

7.4.3 (Level 3) Block level functionality

This level includes all functionality necessary to allow management applications to deal with storage volumes in a networked storage environment. This level applies to Logical Units, LUN Masking and Mapping, block aggregators like Volume Managers, etc. It also applies to block-level virtualization.

7.4.4 (Level 4) File/Record level functionality

This level includes all functionality associated with allowing management applications to deal with data objects like file systems in a networked storage environment. Note that this level not only applies to file systems, it also applies to records, for the structured usage of block storage by middleware applications such as databases and e-mail servers. This level provides the functionality that enables management applications to determine the capacity utilization of the storage volumes handled by the Block Level Functionality.

7.4.5 (Level 5) Application level functionality

This level includes all functionality needed to allow management applications to deal with managed applications in the networked storage environment. This level applies to database applications, e-mail server applications, etc. that work directly with the data objects handled by the File/Record Level Functionality.

7.5 Referring to levels and capabilities in the multi-level model

To simplify talking about the different levels and capabilities within this multi-level model of networked storage management functionality, the following short-hand notation may be used in SMI-S.

Individual functionality levels are referred to as L1 through L5, and a single letter appended to this level indicates a particular kind of FCAPS capability. For instance, fault management functionality within the connectivity layer would be referred to as L2F functionality, and configuration management functionality for a physical device would be referred to as L1C functionality.

7.6 Functionality descriptions in SMI-S profiles

To make it easier to understand the management functionality coverage provided by individual profiles and subprofiles in this SMI-S document, each profile lists the functionality provided by the profile and its subprofiles. If a function is provided by a subprofile, this is indicated, including whether the subprofile is optional or required. Functionality listed in the profile is organized by Level, and within each Level by FCAPS category, as defined here by the Functionality Matrix.

7.7 Capabilities of this version

This section summarizes, at a high level, the capabilities provided by this SMI-S version based on the Functionality Matrix, and is organized by Level.

7.7.1 Device Level

7.7.1.1 Fault Management

SMI-S device profiles that include the Health Package (*Information Technology – Storage Management, Part 3 Common Profiles* 26 Health Package) provide capabilities for reporting of the SAN device health and status, including the type, category, and source of the failures. Asynchronous notification for changes in device health status is also provided via the Indications Subprofile (*Information Technology – Storage Management, Part 3 Common Profiles* 43 Indication Profile).

7.7.1.2 Configuration Management

SMI-S defines the capabilities needed for the discovery, configuration, and monitoring of devices in a SAN. Asynchronous notification for changes in device configuration is provided via the Indications Subprofile (see *Information Technology – Storage Management, Part 3 Common Profiles* 43 Indication Profile).

7.7.1.3 Accounting Management

Other than basic device discovery, SMI-S provides no specific capabilities for device Accounting Management.

7.7.1.4 Performance Management

SMI-S enables performance management of some SAN devices (see *Information Technology – Storage Management, Part 4 Block Devices* 8 Block Server Performance Subprofile).

7.7.1.5 Security Management

SMI-S provides device-level security via basic authentication capabilities. See the SMI-S Security section (*Information Technology – Storage Management, Part 2 Common Architecture*