

INTERNATIONAL STANDARD

ISO/IEC 24775

First edition
2007-06

Information technology – Storage management



Reference number
ISO/IEC 24775:2007(E)



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2007 ISO/IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester.

If you have any questions about ISO/IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

IEC Central Office
3, rue de Varembe
CH-1211 Geneva 20
Switzerland
Email: inmail@iec.ch
Web: 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.

- Catalogue of IEC publications: www.iec.ch/searchpub

The IEC on-line Catalogue enables you to search by a variety of criteria (reference number, text, technical committee,...). It also gives information on projects, withdrawn and replaced publications.

- IEC Just Published: www.iec.ch/online_news/justpub

Stay up to date on all new IEC publications. Just Published details twice a month all new publications released. Available on-line and also by email.

- Customer Service Centre: www.iec.ch/webstore/custserv

If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:

Email: csc@iec.ch
Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00

INTERNATIONAL STANDARD

ISO/IEC 24775

First edition
2007-06

Information technology – Storage management



PRICE CODE **XM**

For price, see current catalogue

FOREWORD.....	22
INTRODUCTION	23
1 Scope	24
2 Normative References	25
2.1 International standards	25
2.2 Other specifications	25
3 Definitions, symbols, abbreviations, and conventions	26
3.1 Definitions	26
3.1.1	34
3.2 Symbols and abbreviations.....	40
3.3 Keywords	40
3.4 Conventions	41
4 Introduction	43
4.1 Preamble	43
4.2 Business rationale	43
4.3 Interface definition	43
4.4 Technology trends	45
4.5 Management environment	47
4.6 Architectural objectives	48
5 Overview	50
5.1 Base capabilities	50
5.1.1 General	50
5.1.2 Object Oriented	50
5.1.3 Messaging-based interface	52
5.2 Capabilities of this version	54
5.2.1 Overview.....	54
5.2.2 Determine and monitor the configuration of a SAN	54
5.2.3 Monitoring the health of key resources in a SAN	55
5.2.4 Monitoring the available performance of interconnections in a SAN	55
5.2.5 Monitoring and controlling the zones in a SAN.....	55
5.2.6 Discovering/monitoring/controlling the storage volumes in a SAN	55
5.2.7 Requiring authenticated clients in a SAN	55
5.3 Operational environment	56
5.4 Using this standard	57
5.5 Language bindings	57
6 Transport and reference model	58
6.1 Introduction	58
6.1.1 Overview.....	58
6.1.2 Language requirements.....	58
6.1.3 Communications requirements	58
6.1.4 XML Message Syntax and Semantics.....	58
6.2 Transport stack	59

6.3	Reference model	60
6.3.1	Overview.....	60
6.3.2	Roles for Interface Constituents	60
6.3.2.1	Client	60
6.3.2.2	Agent	60
6.3.2.3	CIM Server	61
6.3.2.4	Provider	61
6.3.2.5	Lock Manager	61
6.3.2.6	Directory Server.....	61
6.3.3	Cascaded Agents	61
7	Object model	62
7.1	Model overview (key resources)	62
7.1.1	Overview.....	62
7.1.2	Introduction to CIM UML Notation	62
7.2	Techniques	63
7.2.1	CIM fundamentals	63
7.2.2	Modelling profiles.....	66
7.2.3	Naming	67
7.2.4	Correlatable and Durable Names	68
7.2.4.1	Overview.....	68
7.2.4.2	Correlatable Names Formation.....	70
7.2.4.3	Testing equality of Correlatable Names.....	70
7.2.4.4	Standard Formats for Correlatable Names.....	70
7.2.4.5	Case Sensitivity	72
7.2.4.6	Preferred Correlatable Names.....	72
7.2.4.7	Concatenation	72
7.2.5	Events – CIM indications	73
7.2.5.1	Background	73
7.2.5.2	Using indications	73
7.2.5.3	Indication hierarchy	75
7.2.5.4	Agent/Provider Considerations.....	76
7.2.5.5	Client Considerations	77
7.2.5.6	Requirements	78
7.2.5.7	Implementation Considerations	78
7.2.6	Device Credentials	78
7.2.7	Recipe Conventions	79
7.2.7.1	Recipe Definition	79
7.2.7.2	Recipe Pseudo Code Conventions.....	79
7.2.7.3	Common Recipes	84
7.3	Profiles.....	85
7.3.1	Profile content.....	85
7.3.1.1	Profile and subprofile definition	85
7.3.1.2	Format for Profile Specifications.....	85
7.3.1.3	Registry of Profiles and Subprofiles	87
7.3.2	Common CIM Packages.....	89
7.3.2.1	Description.....	89
7.3.2.2	Physical Package “package”	89

7.3.2.3	Software Package	95
7.3.3	Common subprofiles.....	99
7.3.3.1	Overview.....	99
7.3.3.2	Access Points subprofile	99
7.3.3.3	Cluster Subprofile	103
7.3.3.4	Disk Drive subprofile.....	108
7.3.3.5	Extent Mapping subprofile	120
7.3.3.6	Location subprofile	124
7.3.3.7	Software Subprofile	127
7.3.3.8	Copy Services Subprofile	128
7.3.3.9	Job Control Subprofile	154
7.3.3.10	Pool Manipulation Capabilities and Settings Subprofile	160
7.3.3.11	LUN Creation Subprofile.....	183
7.3.3.12	Device Credentials subprofile	203
7.3.3.13	Backend Ports subprofile.....	208
7.3.3.14	LUN Masking and Mapping	215
7.3.4	Fabric.....	248
7.3.4.1	Fabric Profile	248
7.3.4.2	Switch Profile	297
7.3.5	Hosts	311
7.3.5.1	FC HBA Profile	311
7.3.6	Storage	325
7.3.6.1	Array Profile	325
7.3.6.2	In-Band Virtualization Profile	347
7.3.6.3	Storage Library Profile	362
7.3.7	Server Profile	384
7.3.7.1	Description.....	384
7.3.7.2	Standard dependencies.....	384
7.3.7.3	Profile dependencies	384
7.3.7.4	CIM Server requirements	385
7.3.7.5	Instance Diagram	386
7.3.7.6	Durable names and other correlatable IDs.....	387
7.3.7.7	Methods.....	387
7.3.7.8	Client considerations	388
7.3.7.9	Recipes.....	388
7.3.7.10	Instrumentation requirements.....	397
7.3.7.11	Required CIM Elements	399
7.3.7.12	Required properties for CIM Elements	399
7.3.7.13	Optional Subprofiles and Profiles.	406
7.3.7.14	ObjectManagerAdapter Subprofile	406
7.4	Cross Client considerations	410
7.4.1	Overview.....	410
7.4.1.1	HBA model	410
7.4.1.2	Switch model	411
7.4.1.3	Array model	411
7.4.1.4	Out of band virtualization model	413
7.4.1.5	Durable names	413

7.4.1.6	Fabric Topology (HBA, Switch, Array)	414
7.4.1.7	Storage Connections (FC HBA, Array)	420
7.4.1.8	Zoning	420
7.4.1.9	Fabric Route Discovery	421
7.4.1.10	Durable names	421
7.4.2	General recipes	421
7.4.2.1	Indications' Status	421
7.4.2.2	Listenable Instance Notification	422
7.4.2.3	Life Cycle Event Subscription description	422
7.4.2.4	Subscription for alert indications	423
7.4.2.5	Listenable Interface Modification Notification	423
7.4.2.6	Subscribe for Lifecycle Events where OperationalStatus Changes	423
7.4.2.7	Subscription for alert indications	424
8	Security	425
8.1	Introduction	425
8.2	Background	425
8.3	Requirements	426
8.3.1	General	426
8.3.2	Certificate usage with SSL 3.0 and TLS	426
8.3.2.1	Functional goals	426
8.3.2.2	Requirements	427
8.4	Modelling device credentials	428
8.4.1	General requirements	428
8.4.2	Instrumentation requirements	428
9	Service Discovery	429
9.1	Objectives	429
9.2	Overview	429
9.3	SLP messages	430
9.4	Scopes	431
9.5	Services definition	432
9.5.1	General	432
9.5.2	Service Type	432
9.5.3	Service Attributes	432
9.6	User Agents (UA)	434
9.7	Service Agents (SAs)	434
9.8	Directory Agents (DAs)	434
9.9	Service Agent Server (SA Server)	435
9.9.1	General Information	435
9.9.2	SA Server (SAS) Implementation	435
9.9.3	SA Server (SAS) Clients	435
9.9.3.1	Description	435
9.9.3.2	SAS Client Requests – SA Server Responses	436
9.9.4	SA Server configuration	436
9.9.4.1	Overview	436
9.9.4.2	SLP Configuration File	436
9.9.4.3	Programmatic configuration	436

9.9.4.4	DHCP configuration	437
9.9.4.5	Scope	437
9.9.5	SA Server discovery	437
9.9.6	SAS Client registration	437
9.10	'Standard WBEM' Service Type Templates.....	438
10	SMI-S Roles	442
10.1	Introduction	442
10.2	SMI-S Client.....	443
10.2.1	Overview.....	443
10.2.2	SLP functions	443
10.2.3	CIM-XML protocol functions	443
10.2.4	Security considerations	443
10.2.5	Lock management functions.....	443
10.3	Dedicated SMI-S Server	443
10.3.1	Overview.....	443
10.3.2	SLP functions	444
10.3.3	CIM-XML Protocol Functions.....	444
10.3.3.1	General.....	444
10.3.3.2	Required intrinsic methods	444
10.3.3.3	Required model support	445
10.3.4	Security considerations	445
10.3.5	Lock management functions.....	445
10.4	General Purpose SMI-S Server	445
10.4.1	Overview.....	445
10.4.2	SLP functions	445
10.4.3	CIM-XML Protocol functions.....	445
10.4.3.1	General.....	445
10.4.3.2	Required intrinsic methods	445
10.4.3.3	Required model support	446
10.4.3.4	Security considerations	446
10.4.4	Lock management functions.....	446
10.4.5	Provider Subrole.....	446
10.4.5.1	Overview.....	446
10.4.5.2	Required model support	446
10.5	Directory Server.....	446
10.5.1	General.....	446
10.5.2	SLP functions	446
10.5.3	CIM-XML Protocol functions.....	446
10.5.4	Security considerations	446
10.5.5	Lock management functions.....	446
10.6	Combined Roles on a Single System	446
10.6.1	Overview.....	446
10.6.2	General Purpose SMI-S Server as a Profile Aggregator	447
10.6.2.1	SLP functions	447
10.6.2.2	CIM-XML Protocol functions.....	447
10.6.2.3	Security considerations	447
10.6.2.4	Lock management functions.....	447

11	Installation and upgrade.....	448
11.1	Introduction	448
11.2	Role of the Administrator	448
11.3	Goals	448
11.3.1	Non-Disruptive Installation and De-installation.....	448
11.3.2	Plug-and-Play	448
11.4	Installing device support	449
11.4.1	General.....	449
11.4.2	Installation	449
11.4.3	Discovery and initialization of Device support	449
11.4.4	Removal/Update.....	450
11.4.5	Reconfiguration	450
11.4.6	Failure.....	451
11.5	Object manager	451
11.5.1	Installation	451
11.5.2	Multiple CIMOMs on a Single Server	451
11.5.3	Removal, reconfiguration and upgrade	452
11.5.4	Failure.....	452
11.6	Client	452
11.6.1	Removal	452
11.6.2	Reconfiguration	452
11.6.3	Failure.....	452
11.7	Directory Server	452
11.7.1	Installation	452
11.7.2	Removal/Failure	452
11.8	Management domains	452
11.8.1	General.....	452
11.8.2	Initial configuration.....	452
11.8.3	Reconfiguration	453
11.9	Lock manager	453
Annex A	(informative) Futures	454
A.1	Overview	454
A.2	HBA LUN masking and persistent binding	454
A.3	Managed Hub Section.....	454
A.4	IP Storage	454
A.5	Multi-Path Modelling.....	454
A.6	Provider Modelling	454
A.7	Non-Fibre Fabrics	454
A.8	Compliance notification	454
A.9	Cascaded Agents.....	455
A.10	Network Storage	455
A.11	Synchronization of file system elements through copy services ..	455
A.12	Model size distinctions in Disk Drive	455
A.13	Expanded extent mapping	455
A.14	Locking.....	455
A.15	Policy management	456
Annex B	(informative) Experimental Profiles.....	459

B.1	Overview	459
B.2	Common Profiles and Subprofiles.....	459
B.3	SML Subprofiles	462
B.4	Extender profile	498
B.5	Management Appliance profile.....	513
B.6	Out of Band Virtualizer Profile	521
B.7	JBOD Profile	546
B.8	Extra Capacity Set Subprofile	557
B.9	Host Discovered Resources Profile (EXPERIMENTAL)	563
B.10	Router Profile	584
Annex C	(informative) Mapping CIM Objects to SNMP MIB Structures.....	601
C.1	Purpose of this Annex	601
C.2	CIM-to-MIB Mapping Overview	601
C.3	CIM-to-MIB mapping methodology	601
C.4	Example mapping	604
Annex D	(normative) Compliance with this standard	622
D.1	Compliance statement	622
D.2	Compliance declaration.....	622
D.3	Server Profile and compliance	622
D.4	Example	622
Annex E	(informative) Optional Profiles and Subprofiles	624
E.1	Introduction	624
E.2	Provider Subprofile.....	624
Bibliography		631

Table 1 – Standard dependencies for SMI-S.....	25
Table 2 – SLP properties	66
Table 3 – Standardized Name Formats	71
Table 4 – Profile components	86
Table 5 – Registry of profiles and subprofiles.....	88
Table 6 – Required CIM Elements.....	92
Table 7 – Required Properties for SystemPackaging.....	93
Table 8 – Required Properties for PhysicalPackage	93
Table 9 – Required Properties for Product	94
Table 10 – Required Properties for ProductPhysicalComponent.....	94
Table 11 – Required Properties for Container	95
Table 12 – Required Properties for ProductParentChild.....	95
Table 13 – Required Properties for Realizes	95
Table 14 – Required CIM Elements.....	98
Table 15 – Required Properties for InstalledSoftwareIdentity.....	98
Table 16 – Required Properties for SoftwareIdentity	99
Table 17 – RemoteAccessPoint.InfoFormat and AccessInfo Properties	101
Table 18 – Required CIM Elements.....	102
Table 19 – Required Properties for HostedAccessPoint.....	102
Table 20 – Required Properties for SAPAvailableForElement.....	103
Table 21 – Required Properties for RemoteServiceAccessPoint.....	103
Table 22 – Optional Profiles or Subprofiles	103
Table 23 – OperationStatus for Component ComputerSystem.....	106
Table 24 – Required CIM Elements.....	107
Table 25 – Required Properties for ComponentCS	107
Table 26 – Required Properties for ComputerSystem	108
Table 27 – Optional Profiles or Subprofiles	108
Table 28 – Required Functional Profiles.....	109
Table 29 – DiskDrive Status	111
Table 30 – Required CIM Elements.....	114
Table 31 – Required Properties for BasedOn.....	115
Table 32 – Required Properties for ConcreteComponent.....	115
Table 33 – Required Properties for Container	116
Table 34 – Required Properties for ProductParentChild.....	116
Table 35 – Required Properties for ElementSoftwareIdentity	116
Table 36 – Required Properties for DiskDrive.....	117
Table 37 – Required Properties for MediaPresent.....	117
Table 38 – Required Properties for PhysicalMedia.....	118
Table 39 – Required Properties for Realizes	118
Table 40 – Required Properties for RealizesExtent.....	119
Table 41 – Required Properties for SoftwareIdentity	119
Table 42 – Required properties for StorageExtent	120
Table 43 – Optional profiles or subprofiles	120
Table 44 – Required Functional Profiles.....	121
Table 45 – Required CIM Elements.....	123

Table 46 – Required Properties for BasedOn	123
Table 47 – Required Properties for ConcreteComponent	123
Table 48 – Required Properties for StorageExtent	124
Table 49 – Optional Profiles or Subprofiles	124
Table 50 – Required CIM Elements	126
Table 51 – Required Properties of Location	126
Table 52 – Required Properties for PhysicalElementLocation	127
Table 53 – Optional Profiles or Subprofiles	127
Table 54 – Required CIM Elements	128
Table 55 – Optional Profiles or Subprofiles	128
Table 56 – Copy Services Standard Dependencies	129
Table 57 – Required Functional Profiles	129
Table 58 – Name Formats	132
Table 59 – Subprofile Required Classes, Associations, Methods and Indications	146
Table 60 – Required Properties for ElementCapabilities	147
Table 61 – Required Properties for HostedService	147
Table 62 – Required Properties for StorageConfigurationService	148
Table 63 – Required Properties for StorageConfigurationCapabilities	148
Table 64 – Required Properties for StorageSynchronized	149
Table 65 – Required Properties for StorageCapabilities	150
Table 66 – Required Properties for ElementSettingData	153
Table 67 – Required Properties for StorageSetting	153
Table 68 – Copy Services Optional Subprofiles and Profiles	154
Table 69 – Job Control Services Standard Dependencies	155
Table 70 – Required Functional Profiles	155
Table 71 – Subprofile Required Classes, Associations, Methods and Indications	158
Table 72 – AffectedJobElement Required Properties	158
Table 73 – Required Properties for ConcreteJob	159
Table 74 – Required Properties for OwningJobElement	160
Table 75 – Optional Profiles or Subprofiles	160
Table 76 – Pool Manipulation Capabilities and Settings Standard Dependencies	161
Table 77 – Required Functional Profiles	162
Table 78 – Example RAID Mapping Table	169
Table 79 – Required CIM Elements	173
Table 80 – Required Properties for ElementCapabilities	174
Table 81 – Required Properties for StorageConfigurationService	174
Table 82 – Required Properties for StorageConfigurationCapabilities	174
Table 83 – Required Properties for StorageCapabilities	176
Table 84 – Required Properties for ElementSettingData	179
Table 85 – Required Properties for StorageSetting	179
Table 86 – Required Properties for StorageSettingWithHints	181
Table 87 – HostedService Required Properties	183
Table 88 – Optional Profiles or Subprofiles	183
Table 89 – LUN Creation Standard Dependencies	184

Table 90 – Required Functional Profiles	184
Table 91 – Required CIM Elements	202
Table 92 – Required Properties for StorageConfigurationService	202
Table 93 – Optional Profiles or Subprofiles	203
Table 94 – Device Credentials Standard Dependencies	203
Table 95 – Required Functional Profiles	204
Table 96 – Required CIM Elements	206
Table 97 – Required Properties for SharedSecretService	206
Table 98 – Required Properties for SharedSecret	206
Table 99 – SharedSecretIsShared Required Properties	207
Table 100 – HostedService Required Properties	207
Table 101 – Optional Profiles or Subprofiles	208
Table 102 – Device Credentials Standard Dependencies	208
Table 103 – Required Functional Profiles	209
Table 104 – Required CIM Elements	211
Table 105 – Required Properties for FCPort	211
Table 106 – Required Properties from ProtocolControllerForPort	213
Table 107 – Required Properties from ProtocolControllerAccessesUnit	213
Table 108 – Required Properties for SCSIProtocolController	213
Table 109 – Required Properties for StorageExtent	214
Table 110 – Required Properties for SystemDevice	214
Table 111 – Optional Profiles or Subprofiles	214
Table 112 – LUN Masking Standard Dependencies	215
Table 113 – Required Functional Profiles	216
Table 114 – Subprofile Required Classes, Associations, Methods and Indications	239
Table 115 – Required Properties for AuthorizedPrivilege	240
Table 116 – Required Properties for AuthorizedSubject	241
Table 117 – Required Properties for AuthorizedTarget	241
Table 118 – Required Properties for ConcreteDependency	241
Table 119 – Required Properties for ControllerConfigurationService	241
Table 120 – Required Properties for ElementSettingData	242
Table 121 – Required Properties for HostedCollection	242
Table 122 – Required Properties for HostedDependency	242
Table 123 – Required Properties for ProtocolControllerMaskingCapabilities	243
Table 124 – Required Properties for PrivilegeManagementService	245
Table 125 – Required Properties for StorageClientSettingData	246
Table 126 – Required Properties for StorageHardwareID	246
Table 127 – Required Properties for StorageHardwareIDManagementService	247
Table 128 – Required Properties for SystemSpecificCollection	247
Table 129 – Fabric Standard Dependencies	250
Table 130 – Required Functional Profiles	250
Table 131 – Durable Names Usage	254
Table 132 – Port OperationalStatus	254
Table 133 – OperationalStatus for ComputerSystem	254
Table 134 – Required CIM Elements	257
Table 135 – Required Properties for ActiveConnection	259

Table 136 – Required Properties for AdminDomain	259
Table 137 – Required Properties for Component	259
Table 138 – Required Properties for ComputerSystem	260
Table 139 – Required Properties for ContainedDomain	260
Table 140 – Required Properties for DeviceSAPImplementation	260
Table 141 – Required Properties for ElementCapabilities	261
Table 142 – Required Properties for ElementSettingData	261
Table 143 – Required Properties for FCPort	261
Table 144 – HostedAccessPoint	264
Table 145 – Required Properties for HostedCollection	264
Table 146 – Required Properties for ConnectivityCollection	264
Table 147 – Required Properties for LogicalPortGroup	264
Table 148 – Required Properties for MemberOfCollection	265
Table 149 – Required Properties for MemberOfCollection	265
Table 150 – Required Properties for ProtocolEndpoint	266
Table 151 – Required Properties for SystemDevice	266
Table 152 – Required Properties for Zone	266
Table 153 – Required Properties for ZoneCapabilities	267
Table 154 – Required Properties for ZoneMembershipSettingData	268
Table 155 – Required Properties for ZoneSet	268
Table 156 – Optional Profiles or Subprofiles	268
Table 157 – Required Functional Profiles	269
Table 158 – Required CIM Elements	283
Table 159 – Required Properties for HostedService	283
Table 160 – Required Properties for ZoneService	283
Table 161 – Optional Profiles or Subprofiles	284
Table 162 – Required CIM Elements	289
Table 163 – Required Properties for HostedCollection	289
Table 164 – Required Properties of MemberOfCollection	289
Table 165 – Required Properties for NamedAddressCollection	289
Table 166 – Required Properties for ZoneService	290
Table 167 – Optional Profiles or Subprofiles	290
Table 168 – Required CIM Elements	292
Table 169 – Required Properties for ControlledBy	292
Table 170 – Required Properties for ElementSoftwareIdentity	293
Table 171 – Required Properties for FCPort	293
Table 172 – Required Properties for LogicalPortGroup	295
Table 173 – Required Properties of MemberOfCollection	295
Table 174 – Required Properties for PortController	295
Table 175 – Required Properties of ProtocolControllerForPort	296
Table 176 – Required Properties for SCSIProtocolController	296
Table 177 – Switch Standard Dependencies	297
Table 178 – Required Functional Profiles	297
Table 179 – Required CIM Elements	300
Table 180 – Required Properties for ComputerSystem	300
Table 181 – Required Properties for ElementStatisticalData	302
Table 182 – Required Properties for FCPort	302

Table 183 – Required Properties for FCPortRateStatistics.....	304
Table 184 – Required Properties for FCPortStatistics	304
Table 185 – Required Properties for SystemDevice	306
Table 186 – Optional Profiles or Subprofiles	306
Table 187 – Required CIM Elements	309
Table 188 – Required Properties for LogicalModule.....	309
Table 189 – Required Properties for ModulePort	310
Table 190 – Required Properties for SystemDevice	310
Table 191 – Optional Profiles or Subprofiles	310
Table 192 – HBA Standard Dependencies	311
Table 193 – Required Functional Profiles	311
Table 194 – Required CIM Elements	316
Table 195 – Required Properties for ComputerSystem	317
Table 196 – Required Properties for ControlledBy	317
Table 197 – Required Properties for ElementSoftwareIdentity	317
Table 198 – Required Properties for ElementStatisticalData	317
Table 199 – Required Properties for FCPort	318
Table 200 – Required Properties for FCPortStatistics	319
Table 201 – Required Properties for HostedCollection.....	319
Table 202 – Required Properties for InstalledSoftwareIdentity.....	320
Table 203 – Required Properties for LogicalPortGroup	320
Table 204 – Required Properties of MemberOfCollection	320
Table 205 – Required Properties for PhysicalPackage	320
Table 206 – Required Properties for PortController.....	321
Table 207 – Required Properties for Product	321
Table 208 – Required Properties for ProductPhysicalComponent.....	322
Table 209 – Required Properties of ProtocolControllerForPort	322
Table 210 – Required Properties for Realizes	322
Table 211 – Required Properties for SCSIProtocolController.....	323
Table 212 – Required Properties for SystemDevice	323
Table 213 – Required Properties for SoftwareIdentity	323
Table 214 – Optional Profiles or Subprofiles	324
Table 215 – Array Standard Dependencies	325
Table 216 – Required Functional Profiles.....	326
Table 217 – OperationalStatus for ComputerSystem	329
Table 218 – OperationalStatus for StorageVolume	330
Table 219 – Port State/Status.....	331
Table 220 – Required CIM Elements.....	335
Table 221 – Required Properties for AllocatedFromStoragePool	336
Table 222 – Required Properties for ElementCapabilities	336
Table 223 – Required Properties for ElementSettingData	336
Table 224 – Required Properties for ComputerSystem	336
Table 225 – Required Properties for FCPort	338
Table 226 – Required Properties from HostedStoragePool.....	340
Table 227 – Required Properties from ProtocolControllerForPort	340
Table 228 – Required Properties from ProtocolControllerForUnit	340
Table 229 – Required Properties for SCSIProtocolController.....	340

Table 230 – Required Properties from StorageCapabilities.....	342
Table 231 – Required Properties for StoragePool	342
Table 232 – Required Properties from StorageSetting	343
Table 233 – Required Properties for StorageVolume	343
Table 234 – Required Properties for SystemDevice	345
Table 235 – Optional Profiles or Subprofiles	346
Table 236 – In-Band Virtualizer Standard Dependencies	347
Table 237 – Required Functional Profiles	347
Table 238 – Required CIM Elements	351
Table 239 – Required Properties for AllocatedFromStoragePool	353
Table 240 – Required properties for ComputerSystem.....	353
Table 241 – Required properties for ConcreteComponent	353
Table 242 – Required properties for ElementCapabilities.....	354
Table 243 – Required properties for ElementSettingData	354
Table 244 – Required properties for FCPort	354
Table 245 – Required properties from HostedStoragePool	356
Table 246 – Required properties for ProtocolControllerAccessesUnit.....	356
Table 247 – Required Properties from ProtocolControllerForPort	357
Table 248 – Required Properties from ProtocolControllerForUnit	357
Table 249 – Required properties for SCSIProtocolController	357
Table 250 – Required properties from StorageCapabilities	358
Table 251 – Required properties for StorageExtent	358
Table 252 – Required Properties for StoragePool	359
Table 253 – Required properties from StorageSetting	359
Table 254 – Required properties for StorageVolume	359
Table 255 – Required properties for SystemDevice	361
Table 256 – Optional Profiles or Subprofiles	361
Table 257 – Storage Library Standard Dependencies	362
Table 258 – Required Functional Profiles	363
Table 259 – Required CIM Elements	371
Table 260 – Required Properties for ChangerDevice	373
Table 261 – Required properties for Chassis	374
Table 262 – Required properties for Container.....	374
Table 263 – Required properties for ProtocolControllerForUnit.....	375
Table 264 – Required properties for SCSIProtocolController	375
Table 265 – Required properties for DeviceSoftware	375
Table 266 – Required properties for LibraryPackage	376
Table 267 – Required properties for MediaAccessDevice	376
Table 268 – Required properties for PackagedComponent.....	376
Table 269 – Required properties for PhysicalMedia	377
Table 270 – Required properties for PhysicalMediaInLocation.....	377
Table 271 – Required properties for ProductPhysicalComponent.....	377
Table 272 – Required properties for Realizes	378
Table 273 – Required properties for SoftwareIdentity	378
Table 274 – Required Properties for StorageLibrary	379
Table 275 – Required Properties for StorageMediaLocation	379
Table 276 – Required properties for SystemDevice	380

Table 277 – Optional Profiles or Subprofiles	380
Table 278 – Required CIM Elements	382
Table 279 – Required Properties for LimitedAccessPort	382
Table 280 – Optional Profiles or Subprofiles	383
Table 281 – CIM Server Standard Dependencies	384
Table 282 – Required Functional Profiles	385
Table 283 – Profile Required Classes, Associations, Methods and Indications	399
Table 284 – Required Properties for ObjectManager	400
Table 285 – Required Properties for System	400
Table 286 – Required Properties for HostedService	401
Table 287 – Required Properties for CIMXMLCommunicationMechanism	401
Table 288 – Required Properties for HostedAccessPoint	402
Table 289 – Required Properties for CommMechanismForManager	402
Table 290 – Required Properties for Namespace	403
Table 291 – Required Properties for NamespaceInManager	403
Table 292 – Required Properties for RegisteredProfile	404
Table 293 – Required Properties for RegisteredSubProfile	404
Table 294 – Required Properties for ReferencedProfile	405
Table 295 – Required Properties for SubProfileRequiresProfile	405
Table 296 – Required Properties for ElementConformsToProfile	406
Table 297 – CIM Server Profile Optional Subprofiles and Profiles	406
Table 298 – Subprofile Required Classes, Associations, Methods and Indications	408
Table 299 – Required Properties for ObjectManagerAdapter	408
Table 300 – Required Properties for CommMechanismForObjectManagerAdapter	409
Table 301 – Cross-Profile Durable Names	413
Table 302 – Cross Profile Durable Names	421
Table 303 – Message Types	431
Table 304 – Required Configuration Properties for SA as DA	436
Table 305 – Required Configuration Properties for SA	436
Table 306 – Functional Profiles	444
Table B.1 – Required CIM Elements	461
Table B.2 – Required Properties for IsSpare	461
Table B.3 – Required Properties of MemberOfCollection	461
Table B.4 – Required Properties for SparedSet	461
Table B.5 – Optional Profiles or Subprofiles	462
Table B.6 – Required CIM Elements	464
Table B.7 – Required Properties for InterLibraryPort	464
Table B.8 – Required Properties for LibraryExchange	464
Table B.9 – Optional Profiles or Subprofiles	465
Table B.10 – Required CIM Elements	467
Table B.11 – Required Properties for DeviceServicesLocation	467
Table B.12 – Optional Profiles or Subprofiles	467
Table B.13 – Required CIM Elements	470
Table B.14 – Required Properties for FCPort	470
Table B.15 – Required Properties for ProtocolControllerForPort	472

Table B.16 – Required CIM Elements	474
Table B.17 – Required Properties for DeviceServicesLocation	474
Table B.18 – Optional Profiles or Subprofiles	474
Table B.19 – Required CIM Elements	476
Table B.20 – Required Properties for ConfigurationCapacity	476
Table B.21 – Required Properties for ElementCapacity	476
Table B.22 – Optional Profiles or Subprofiles	476
Table B.23 – Required Properties for AlertIndication.....	478
Table B.24 – LibraryAlert Property Settings.....	478
Table B.25 – Vendor Specific Properties of LibraryAlert.....	479
Table B.26 – Variable Alert Properties for LibraryAlert	479
Table B.27 – SCSI TapeAlert-based Properties	479
Table B.28 – LibraryAlert AlertIndication Properties	480
Table B.29 – Optional Profiles or Subprofiles	497
Table B.30 – Extender Standard Dependencies.....	498
Table B.31 – Required Functional Profiles	499
Table B.32 – Required CIM Elements	502
Table B.33 – Required Properties for ActiveConnection for ATM.....	504
Table B.34 – Required Properties for ActiveConnection for FC.....	504
Table B.35 – Required Properties for BindTo	504
Table B.36 – Required Properties for ComputerSystem.....	504
Table B.37 – Required Properties for DeviceSAPImplementation.....	506
Table B.38 – Required Properties for FCPort	506
Table B.39 – Required Properties for ForwardingService.....	508
Table B.40 – Required Properties for ForwardsAmong	508
Table B.41 – Required Properties for HostedNetworkPipe.....	508
Table B.42 – Required Properties for IPProtocolEndpoint.....	508
Table B.43 – Required Properties for NetworkPort.....	510
Table B.44 – Required Properties for Network	511
Table B.45 – Required Properties for NetworkPipe	511
Table B.46 – Required Properties for ProtocolEndpoint	511
Table B.47 – Required Properties for TCPProtocolEndpoint	511
Table B.48 – Required Properties for SystemDevice.....	512
Table B.49 – Optional Profiles or Subprofiles	512
Table B.50 – Management Appliance Standard Dependencies	513
Table B.51 – Required Functional Profiles	513
Table B.52 – Required CIM Elements	516
Table B.53 – Required Properties for ComputerSystem.....	516
Table B.54 – Required Properties for FCPort	517
Table B.55 – Required Properties from HostedService	518
Table B.56 – Required Properties from Installed SoftwareElement.....	518
Table B.57 – Required Properties for LogicalPortGroup	518
Table B.58 – Required Properties for MemberOfCollection.....	518
Table B.59 – Required Properties for RemoteServiceAccessPoint	519
Table B.60 – Required Properties for ServiceAvailableToElement.....	519
Table B.61 – Required Properties for SoftwareElement	519
Table B.62 – Optional Profiles or Subprofiles	520

Table B.63 – OutofBand Virtualizer Standard Dependencies	522
Table B.64 – Required Functional Profiles	523
Table B.65 – Required CIM Elements	529
Table B.66 – Required Properties for AllocatedFromStoragePool.....	531
Table B.67 – Required Properties for BasedOn	531
Table B.68 – Required Properties for Component	531
Table B.69 – Required Properties for ComputerSystem - Metadata Controller	531
Table B.70 – Required Properties for ComputerSystem - Translation Engine.....	532
Table B.71 – Required Properties for ElementCapabilities.....	532
Table B.72 – Required Properties for FCPort	533
Table B.73 – Required Properties from HostedCollection	534
Table B.74 – Required Properties from HostedStoragePool	534
Table B.75 – Required Properties from LogicalPortGroup.....	534
Table B.76 – Required Properties for MemberOfCollection.....	535
Table B.77 – Required Properties from ProtocolControllerForPort.....	535
Table B.78 – Required Properties from ProtocolControllerForUnit.....	535
Table B.79 – Required Properties for SCSIProtocolController	535
Table B.80 – Required Properties from StorageCapabilities	536
Table B.81 – Required Properties for StoragePool.....	537
Table B.82 – Required Properties from StorageSetting.....	537
Table B.83 – Required Properties for StorageExtent.....	537
Table B.84 – Required Properties for StorageVolume.....	542
Table B.85 – Required Properties for SystemDevice.....	542
Table B.86 – Optional Profiles or Subprofiles	542
Table B.87 – JBOD Standard Dependencies	546
Table B.88 – Required Functional Profiles	546
Table B.89 – Required CIM Elements	548
Table B.90 – Required Properties for ComputerSystem.....	548
Table B.91 – Required Properties for ComputerSystemPackage.....	551
Table B.92 – Required Properties for FCPort	551
Table B.93 – Required Properties for ConcretelIdentity	554
Table B.94 – Required Properties for SCSIProtocolController	554
Table B.95 – Required Properties for ProtocolControllerForUnit.....	556
Table B.96 – Required Properties for SystemDevice.....	556
Table B.97 – Optional Profiles or Subprofiles	556
Table B.98 – OperationStatus for Component ComputerSystem	559
Table B.99 – Required CIM Elements	560
Table B.100 – Required Properties for ComputerSystem.....	561
Table B.101 – Required Properties for ExtraCapacitySet.....	561
Table B.102 – Required Properties for ConcretelIdentity	562
Table B.103 – Required Properties of MemberOfCollection	562
Table B.104 – Optional Profiles or Subprofiles	562
Table B.105 – HostDiscoveredResources Standard Dependencies.....	564
Table B.106 – Required Functional Profiles	564
Table B.107 – SCSI Device Type Mapping	568
Table B.108 – Required CIM Elements	569
Table B.109 – Required Properties for AdminDomain	570

Table B.110 – Required Properties for Component	570
Table B.111 – Required Properties for DeviceSAPImplementation	570
Table B.112 – Required Properties for FCPort	570
Table B.113 – Required Properties for HostedCollection	575
Table B.114 – Required Properties of ProtocolControllerForPort	575
Table B.115 – Required Properties for LogicalNetwork	575
Table B.116 – Required Properties of MemberOfCollection	575
Table B.117 – Required Properties for ProtocolEndpoint	576
Table B.118 – Required Properties for SystemDevice	576
Table B.119 – Required Properties for StorageVolume	576
Table B.120 – Optional Profiles or Subprofiles	578
Table B.121 – Required CIM Elements	579
Table B.122 – Required Properties for ProtocolControllerForPort	579
Table B.123 – Required Properties for SCSIProtocolController	579
Table B.124 – Required Properties for ProtocolControllerAccessesUnit	580
Table B.125 – Optional Profiles or Subprofiles	580
Table B.126 – Required CIM Elements	582
Table B.127 – Required Properties for SCSIProtocolController	582
Table B.128 – Required Properties for ProtocolControllerForUnit	582
Table B.129 – Optional Profiles or Subprofiles	583
Table B.130 – Router Standard Dependencies	584
Table B.131 – Required Functional Profiles	584
Table B.132 – Required CIM Elements	587
Table B.133 – Required Properties for ComputerSystem	588
Table B.134 – Required Properties for ComputerSystemPackage	590
Table B.135 – Required Properties for FCPort	591
Table B.136 – Required Properties for LogicalDevice	596
Table B.137 – Required Properties for Concretelidentity	596
Table B.138 – Required Properties for LogicalPortGroup	596
Table B.139 – Required Properties of MemberOfCollection	596
Table B.140 – Required Properties for SCSIProtocolController	597
Table B.141 – Required Properties for ProtocolControllerAccessesUnit	599
Table B.142 – Required Properties for ProtocolControllerForUnit	599
Table B.143 – Optional Profiles or Subprofiles	600
Table C.1 – CIM/SNMP Data Type Mapping	602
Table E.1 – Subprofile Required Classes, Associations, Methods and Indications	626
Table E.2 – Required Properties for Provider	626
Table E.3 – Required Properties for ProviderCapabilities	627
Table E.4 – Required Properties ProviderElementCapabilities	628
Table E.5 – Required Properties for ClassSupportForNamespace	628
Table E.6 – Required Properties for ProviderModule	628
Table E.7 – Required Properties for ProviderInModule	629
Table E.8 – Required Properties for IndicationFilter	629
Table E.9 – Required Properties for FiltersSupported	629
Table E.10 – Required Properties for ObjectManagerIsProviderRequired	630

Figure 1 – Interface functions	44
Figure 2 – Large SAN Topology	47
Figure 3 – Example Client Server Distribution in a SAN	48
Figure 4 – SMI-S Modelling Conventions	50
Figure 5 – Object Model/Server Relationship	51
Figure 6 – Canonical inheritance	52
Figure 7 – Sample CIM-XML Message	53
Figure 8 – Operational environment	56
Figure 9 – Transport stack	59
Figure 10 – Reference Mode	60
Figure 11 – Cluster model.....	65
Figure 12 – Common elements.....	66
Figure 13 – Server Profile Instance Diagram	67
Figure 14 – Volume shared across namespaces.....	68
Figure 15 – Indication Filter Schema	74
Figure 16 – Indications Schema	75
Figure 17 – Physical Package Instance	90
Figure 18 – Software Instance Diagram	97
Figure 19 – Access Point Instance Diagram	100
Figure 20 – Cluster Instance	105
Figure 21 – Disk Drive Instance Model	110
Figure 22 – Extent Mapping Instance	122
Figure 23 – Location Instance.....	125
Figure 24 – Instance Diagram for Copy Services	130
Figure 25 – StorageSynchronized Association	131
Figure 26 – State Diagram for Snapshot	142
Figure 27 – State Diagram for Mirrors	144
Figure 28 – Job Control Subprofile Model	156
Figure 29 – Storage Configuration.....	157
Figure 30 – Pool Manipulation Instance Diagram	163
Figure 31 – Storage Configuration.....	168
Figure 32 – Pool Creation - Initial State	170
Figure 33 – Pool Creation - Step 2	170
Figure 34 – Pool Creation - Step 3	171
Figure 35 – Pool Creation - Step 4	171
Figure 36 – LUN Creation Instance Diagram.....	185
Figure 37 – Storage Pool Example	187
Figure 38 – Volume Creation - Initial State	188
Figure 39 – Volume Creation - Step 1	188
Figure 40 – Volume Creation - Step 2	189
Figure 41 – Volume Creation - Step 3	190
Figure 42 – DeviceCredentials Subprofile Model.....	204
Figure 43 – Back-end Ports Instance.....	210
Figure 44 – Generic System with no ConfigurationService.....	217
Figure 45 – Generic System with ControllerConfiguration Service	217
Figure 46 – Authorization and Access Rights	219
Figure 47 – Initiator Setting Data Example	220

Figure 48 – Entire Model.....	221
Figure 49 – Simple StorageVolume Model	226
Figure 50 – Two view/Two LogicalDevice Use Case	226
Figure 51 – Volume used in multiple views.....	227
Figure 52 – Fabric Instance Diagram.....	251
Figure 53 – Zoning Instance Diagram (AdminDomain).....	252
Figure 54 – Zoning Instance Diagram (ComputerSystem).....	253
Figure 55 – Switch Instance Diagram	298
Figure 56 – Switch Blade Instance Diagram	307
Figure 57 – FC HBA Instance Diagram	312
Figure 58 – Array Profile Instance Diagram	327
Figure 59 – Array Packages Diagram	345
Figure 60 – In Band Virtualization Overview Diagram	348
Figure 61 – In Band Virtualization System Instance	349
Figure 62 – StorageLibrary-centric Instance Diagram	364
Figure 63 – MediaAccessDevice-centric Instance Diagram.....	365
Figure 64 – ChangerDevice-centric Instance Diagram	365
Figure 65 – Physical View Instance Diagram	366
Figure 66 – StorageMediaLocation Instance Diagram.....	367
Figure 67 – LimitedAccessPort Linkages.....	381
Figure 68 – Server Model	386
Figure 69 – ObjectManagerAdapter Subprofile Model.....	407
Figure 70 – System Diagram	410
Figure 71 – Host Bus Adapter Model.....	410
Figure 72 – Switch Model	411
Figure 73 – Array Instance.....	412
Figure 74 – Virtualization Instance.....	413
Figure 75 – Fabric Topology	414
Figure 76 – SA Server Configuration	437
Figure 77 – Complete Reference Model	442
Figure 78 – Configuration Administration.....	450
Figure A.1 – Reference Model with Policy Server.....	457
Figure A.2 – Policy Components	458
Figure B.1 – Sparing Instance	460
Figure B.2 – InterLibraryPort Connection Instance Diagram	463
Figure B.3 – Virtual ChangerDevices.....	466
Figure B.4 – Instance Diagram for Fibre Channel Connection	468
Figure B.5 – Virtual ChangerDevices Sharing a Chassis.....	473
Figure B.6 – Library Capacity Instance Diagram	475
Figure B.7 – Extender Instance Diagram.....	500
Figure B.8 – Management Appliance Subprofile Diagram.....	514
Figure B.9 – Management Appliance Instance Diagram	514
Figure B.10 – Out-of-band Virtualization Block Diagram	522
Figure B.11 – Out-of-Band Virtualization Subprofile Diagram.....	524
Figure B.12 – Metadata System Instance Diagram	525
Figure B.13 – Translation Engine Instance Diagram	527
Figure B.14 – Translation Engine Back-end Ports Instance	528

Figure B.15 – Virtualizer/Fabric Interaction Overview.....	544
Figure B.16 – Extra Capacity Set Instance Diagram	558
Figure B.17 – Host Discovered Resources Instance Diagram 1.....	565
Figure B.18 – Host Discovered Resources Instance Diagram 2.....	566
Figure B.19 – Router Instance Diagram	585
Figure E.1 – Provider Subprofile Model	625

INFORMATION TECHNOLOGY — STORAGE MANAGEMENT

FOREWORD

- 1) ISO (International Organization for Standardization) and IEC (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. Their preparation is entrusted to technical committees; any ISO and IEC member body interested in the subject dealt with may participate in this preparatory work. International governmental and non-governmental organizations liaising with ISO and IEC also participate in this preparation.
- 2) In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.
- 3) 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 and ISO member bodies.
- 4) IEC, ISO and ISO/IEC publications have the form of recommendations for international use and are accepted by IEC 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.
- 5) In order to promote international uniformity, IEC 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 publication and the corresponding national or regional publication should be clearly indicated in the latter.
- 6) ISO and IEC provide no marking procedure to indicate their approval and cannot be rendered responsible for any equipment declared to be in conformity with an ISO/IEC publication.
- 7) All users should ensure that they have the latest edition of this publication.
- 8) 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 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.
- 9) 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.
- 10) Attention is drawn to the possibility that some of the elements of this International Standard 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 was prepared by subcommittee 25: Interconnection of Information technology equipment, of ISO/IEC joint technical committee 1: Information technology.

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.

INTRODUCTION

The SNIA (Storage Networking Industry Association) Storage Management Initiative Specification standard (SM-S) is divided into a number of clauses and annexes.

Clause 1 defines the scope of this standard and places it in context of other standards and standards projects.

Clause 2 enumerates the normative references that apply to this standard.

Clause 3 specifies definitions, symbols, abbreviations, and document conventions.

Clause 4 describes the underlying concepts of the interface, including its anticipated usage model and business rationale.

Clause 5 identifies high-level requirements and capabilities addressed by this standard.

Clause 6 defines the transport layer and reference model employed in the standard.

Clause 7 defines the object model underlying the standard.

Clause 8 defines the security model for the standard.

Clause 9 defines the discovery mechanism assumed by the standard.

Clause 10 defines the users roles assumed by the standard.

Clause 11 defines the installation and upgrade process defined by the standard.

Annex A describes potential enhancements and future developments for the standard (informative).

Annex B defines profiles which are currently in development (informative).

Annex C defines a mapping between the CIM object model and SNMP MIB structures. (informative).

Annex D defines a compliance procedure for the standard (normative).

Annex E defines optional profiles in the context of the standard (informative).

The bibliography provides useful context for the understanding of this standard.

INFORMATION TECHNOLOGY – STORAGE MANAGEMENT

1 Scope

This International Standard defines the a method for the interoperable management of a heterogeneous Storage Area Network (SAN).

This International Standard describes the information available to a WBEM Client from an SMI-S compliant CIM Server.

This International Standard describes an object-oriented, XML-based, messaging-based interface designed to support the specific requirements of managing devices in and through Storage Area Networks (SANs).

2 Normative references

2.1 International standards

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 14165-414, *Information technology - Fibre Channel - Part 414: Generic Services - 4 (FC-GS-4)*

ISO/IEC 14776-452, *Information technology - Small Computer System Interface (SCSI) - Part 452: Primary Commands-2 (SPC-2) [ANSI INCITS 351-2001]*

ITU-T Rec. X.509: May 2000, *The Directory: Public-key and attribute certificate frameworks (DER encoded)*

2.2 Other specifications

All references in this subclause were correct at the time of approval of this International Standard. The provisions of the referenced specifications, as identified in this subclause, are valid within the context of this International standard. The reference to a specification within this International Standard does not give it any further status within ISO or IEC. In particular, it does not give the referenced specification the status of an International Standard.

Table 1 - Standard dependencies for SMI-S

Standard	Version	Organization
CIM Specification	2.2	DMTF
CIM Operations over HTTP	1.1	DMTF
CIM Schema	2.8 Preliminary	DMTF
CIM-XML		DMTF
UML		OMG
SLP		IETF
Key words for use in RFCs to Indicate Requirement Levels		IETF (RFC2119)
Hypertext Transfer Protocol - HTTP	1.0 (1.1)	IETF (RFC1945, RFC2068)
An Extension to HTTP: Digest Access Authentication		IETF (RFC2069)
Secure Sockets Layer (SSL)	3.0	IETF
Multipurpose Internet Mail Extensions (MIME) - Part One: Format of Internet Message Bodies	November, 1996	IETF (RFC2045)
PKCS #12: Personal Information Exchange Syntax	1.0	RSA Laboratories

3 Definitions, symbols, abbreviations, and conventions

3.1 Definitions

3.1.1

Address masking

Address masking is a function of a host I/O controller (device driver) that filters access to certain storage resources on the SAN. It puts the responsibility of segregating I/O paths on the individual server system in the SAN and requires coordination of all servers to avoid access collisions. Also called Host-based LUN Masking

3.1.2

Addressable Unit

Storage addressable unit (e.g. LUN, Virtual Disk, Logical Disk, Logical Volume, Volume Set)

3.1.3

Agent

Object Manager that includes the provider service for a limited set of resources

NOTE An Agent may be embedded or hosted and can be an aggregator for multiple devices.

3.1.4

Aggregation

strong form of an association. For example, the containment relationship between a system and the components that make up the system can be called an aggregation. An aggregation is expressed as a Qualifier on the association class. Aggregation often implies, but does not require, that the aggregated objects have mutual dependencies

3.1.5

ATM

acronym for Asynchronous Transfer Mode

3.1.6

Attributes

collection of tags and values describing the characteristics of a service

3.1.7

Attribute Reply (AttrRply)

reply to an Attribute Request (optional)

3.1.8

Attribute Request (AttrRqst)

request for attributes of a given type of service or attributes of a given service (optional)

3.1.9

Cardinality

the number of values that may apply to an attribute for a given entity. Refer to UML Standards

3.1.10

CIM

acronym for Common Information Model. An object oriented description of the entities and relationships in a business' management environment maintained by the Distributed Management Task Force. Abbreviated CIM. 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

3.1.11

Client

process that issues requests for service. Formulating and issuing requests may involve multiple client processes distributed over one or more computer systems. The collection of client processes involved in formulating and issuing requests is known as a consumer

3.1.12

Completion Semantics

specifies how a method notifies its caller that its operations have completed. To this end, notification of completion is accomplished in either of two ways:

Asynchronous notification: Upon return of the method, its operations may not have yet completed. The caller is then required to employ some other mechanism to determine when the operations complete. Events, callbacks and polling are examples of mechanisms available to the caller in this regard.

Synchronous notification: The thread calling the method blocks until the method's operations succeed or fail.

Completion semantics refer to the operations executed by the method and not the method completion itself. For example, suppose we write a method to resync a split-mirror. We recognize that this could take an indeterminate amount of time, so we design a method, *resync()*, to spawn a task to manage the set of operations required for the resynchronization and then return to the caller. When the method, *resync()*, completes and returns to the caller, the resynchronization of the mirrors will most likely not have completed. So, the method has completed but its operations have not.

3.1.13

Consumer

host, identified by HBA WWN or other identifier, that is allowed access to a storage addressable unit

3.1.14

Control Software

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

3.1.15

Concurrency Control Protocol

set of rules for identifying and resolving resource conflicts between multiple, non-cooperating clients. The three most common concurrency protocols are the following.

Lock ordering: Transactions are ordered according to the order of arrival of their operations at the resource(s).

Optimistic ordering: Transactions proceed until they are ready to commit, whereupon a check is made to see whether they have performed conflicting operations.

Timestamp ordering: Transactions are ordered according to the time they were initiated.

3.1.16

Cooperating Clients

set of consumer processes that are aware of each other and are able to coordinate access to (and control of) resources among themselves

3.1.17

DA Advertisements (DAAdvert)

solicited (unicast) or unsolicited (multicast) advertisement of Directory Agent availability

3.1.18

Data Invariant

data invariant is the name given to the consistency-state of shared data. A data invariant shall always be TRUE. When the data invariant is violated, the invariant shall be protected via mutual exclusion. For example, suppose I have a list of records and a record pointer, *i*, that is always set to point to the last record in the list. In this example, the invariant is *the record pointer always points to the last record*

But observe what happens when I append a record to the list as follows:

- (a) Add record to record[i];
- (b) $i += 1$.

After (a) completes, but before (b) is invoked, *i* no longer points to the last record in the list. Now, suppose another thread comes along and attempts to read the last record in the list. In this case, the thread will get the penultimate record, not the last one – Because *i* has not yet been updated. The solution to this problem is to serialize access to both operations using a lock or a semaphore.

BEGIN LOCK

- (a) Add record to record[i]
- (b) $i += 1$;

END LOCK

3.1.19

Device

storage system that is addressable from the SAN

3.1.20

DHCP

acronym for dynamic host control protocol. An Internet protocol that allows nodes to dynamically acquire ("lease") network addresses for periods of time rather than having to pre-configure them. Abbreviated DHCP. DHCP greatly simplifies the administration of large networks, and networks in which nodes frequently join and depart

3.1.21

Directory

repository of information about objects that may be accessed via a Directory Service

3.1.22

Directory Agent (DA):

in the context of SLP, a process that caches SLP service advertisements registered by Service Agents and forwards the service advertisements to User Agents on demand

3.1.23

Discovery

discovery provides information about what physical and logical SAN entities have been found within the management domain. Enough information is provided to support the creation of correct Topology maps. This information changes dynamically, as SAN entities are added, moved or removed

3.1.24

DLT

acronym for Digital Linear Tape. A family of tape device and media technologies developed by Quantum Corporation

3.1.25

DRM

the Disk Resource Management (DRM) Work Group is defining standard data and interfaces for the management of disk storage facilities, as well as creating guidelines for implementing well-managed block-oriented storage systems.

3.1.26

DMTF

Distributed Management Task Force. An industry organization that develops management standards for computer system and enterprise environments. DMTF standards include WBEM, CIM, DMI, DEN and ARM. Abbreviated DMTF. The DMTF has a web site at www.dmtf.org

3.1.27

Enclosure

box or cabinet

3.1.28

Enumerate

operation that is used to enumerate subclasses, subclass names, instances and instance names in the target Namespace. If successful, the method returns zero or more requested elements that meet the required criteria

3.1.29

Extent

set of consecutively addressed FBA disk blocks that is allocated to consecutive addresses of a single file;

set of consecutively located tracks on a CKD disk that is allocated to a single file;

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

3.1.30

Extrinsic Method

method defined as part of CIM Schema. Extrinsic methods are invoked on a CIM Class (if static) or Instance (otherwise). An extrinsic method call is represented in XML by the <METHODCALL> element and the response to that call represented by the <METHODRESPONSE> element. cf. Intrinsic Method

3.1.31

Fabric

any interconnect between two or more Fibre Channel N_Ports, including point-to-point, loop and Switched Fabric

Switched Fabric: fabric comprised of one or more Switches

3.1.32

FC-GS-3

Fibre Channel - Generic Services 3. Abbreviation FC-GS-3 or GS-3

3.1.33

FIP

Acronym for Federal Information Processing Standard. Standards (and guidelines) produced by NIST for government-wide use in the specification and procurement of Federal computer systems

3.1.34

Grammar

formal definition of the syntactic structure of a language (see syntax), normally given in terms of production rules that specify the order of constituents and their sub-constituents in a sentence (a well-formed string in the language). Each rule has a left-hand side symbol naming a syntactic category (e.g. "noun-phrase" for a natural language grammar) and a right-hand side that is a sequence of zero or more symbols. Each symbol may be either a terminal symbol or a non-terminal symbol. A terminal symbol corresponds to one "lexeme" - a part of the sentence with no internal syntactic structure (e.g. an identifier or an operator in a computer language). A non-terminal symbol is the left-hand side of some rule

3.1.35

GS-3

Refer FC-GS-3

3.1.36

HBA

host bus adapter, card that contains ports for host systems

3.1.37

Host

computer running an O/S

3.1.38

HTTP

request-reply protocol called the Hypertext Transfer Protocol, HTTP

3.1.39

Hub

interconnect element that supports a ring topology

3.1.40

Inheritance Relationship

refer to UML Standards

3.1.41

Interconnect Element

non-terminal network elements (Switches, hubs, routers, directors)

3.1.42

Interface Definition Language (IDL)

high-level declarative language that provides the syntax for interface declarations

Some examples of IDLs in common usage today are:

- DCE's RPC IDL
- Microsoft's DCOM IDL (based on the DCE IDL)
- OMG IDL (used to define the DOM XML interface)
- DMTF MOF (an IDL-derived specification).

3.1.43

Intrinsic Method

Operations made against a CIM server and a CIM Namespace independent of the implementation of the schema defined in the server. Examples of intrinsic methods in XML include the <IMETHODCALL> element and the response to that call represented by the <IMETHODRESPONSE> element, cf. Extrinsic Method

3.1.44

Language-Binding

association of a programming language (e.g., C++, Java, C) with an interface definition language. For example, OMG IDL supports many language bindings because it can be compiled into a variety of programming languages (C, C++, Java, ADA, COBOL, etc.). By contrast, Microsoft's DCOM IDL only supports one language binding, C++. Similarly, Java IDL also supports only one language binding (Java).

Some IDLs do not support any formal language bindings. DMTF's MOF, for example, is derived from OMG's IDL but is used as a data modeling language more in the spirit of SQL than programmatic interfaces.

3.1.45

Lock Manager

short name for Lock Management Server

3.1.46

Logical Unit Number (LUN)

SCSI identifier of a logical unit within a Target

3.1.47

LTO

acronym for Linear Tape Open

3.1.48

LUN Mapping

process of creating a disk resource and defining its external access paths, by configuring LUs (Logical Units) from the disk array logical disk volumes - either by grouping them as a single larger LU or by creating partitions. The "Logical Unit Number (LUN)" is then be mapped to an external ID descriptor (for example: a SCSI Port, Target ID and LU Number). An LU may be mapped for access from multiple ports and/or multiple target IDs, providing alternate paths for nonstop data availability.

LUN Mapping is a necessary task to be able to export the LUN to the Fabric/Server/etc. It can be done independent of any knowledge of the intended use of the LUN. Only LUNs that are exposed via a "Port" are available for access.

3.1.49

LUN Masking

process of configuring software in SAN nodes to determine which hosts have access to exported drives. LUN masking can be either server-based address masking or storage based port mapping, cf. Port Mapping

3.1.50

MAN

acronym for Metropolitan Area 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). Abbreviated MAN. 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

3.1.51

Marshalling

set of operations by which a message is converted into a transfer syntax. In HTTP, requests and replies are marshaled into formatted ASCII-text strings

3.1.52

Method

name of one or more operation(s) performed by an instance of an object class. Methods are distinguished from operations as follows:

A method is a name for one or more operations that may execute when the method is invoked. For example, when the method, `printSelf()`, is called, the operation of printing the state of the reference object is executed.

Synonyms are: Function, procedure or subroutine. Usage of these terms should be deprecated.

In most models, a method is characterized by its name, return-type, parameters, completion semantics (asynchronous or synchronous) and side-effects (e.g., event generation, message propagation, etc.).

Methods are specified in an IDL.

Methods are declared in source header files of a programming language (.h files, Java Interface files, etc.).

Methods are defined (or implemented) in source implementation files (e.g., .cpp, .java, class files).

Method specifications are language independent. Method declarations and implementations are, by construction, language dependent.

3.1.53

Monitoring

monitoring provides management information about the current state of individual logical and physical SAN entities. This information changes dynamically, as SAN entities perform their functions, are serviced, experience errors, etc. Monitoring can only be done on SAN entities that are known via Discovery

3.1.54

NAA

acronym for Network Address Authority. A four bit identifier defined in FC-PH to denote a network address authority (i.e., an organization such as ITU or IEEE that administers network addresses).

3.1.55

NDMP

acronym for Network Data Management Protocol. A communications protocol that allows intelligent devices on which data is stored, robotic library devices and backup applications to intercommunicate for the purpose of performing backups. Abbreviated NDMP.

An open standard protocol for network-based backup of NAS devices. Abbreviated NDMP. NDMP 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 Network Data Management Task Force has a web site at [HTTP://www.ndmp.org](http://www.ndmp.org)

3.1.56

N_Port

refer to Port. Node

a collection of Ports. A Fiber channel device with a group of ports

An addressable entity connected to an I/O bus or network. Used primarily to refer to computers, storage devices and storage subsystems. The component of a node that connects to the bus or network is a port

3.1.57

Non-cooperating clients

set of consumer processes that are independent of each other, compete for resources and execute independently of the other. User processes on a multi-user machine are non-cooperating clients with respect to the operating system

3.1.58

Operation

action executed within the body of a method (AKA procedure, function or subroutine). Operations are distinct from methods (see Method)

3.1.59

Out-of-Band

transmission of management information for Fibre Channel components outside of the Fibre Channel network, typically over Ethernet

3.1.60

PKI

acronym for public key infrastructure. A framework established to issue, maintain and revoke public key certificates accommodating a variety of security technologies

3.1.61

Platform

collection of Nodes

3.1.62

Port

connection point for links

N_Port: A hardware entity that includes a Link_Control_Facility. It may act as an Originator, a Responder or both.

N_Port identifier: A Fabric unique address identifier by which an N_Port is uniquely known. The identifier may be assigned by the Fabric during the initialization procedure. The identifier may also be assigned by other procedures not defined in FC-FS.

Port_Name: As defined in FC-FS.

3.1.63

Port Mapping

function of a storage subsystem to define which hosts have access to exported drives. This configuration authorizes specified server HBA WWNs to access the secured LU while preventing other unauthorized servers/hosts from either seeing the secured LU or accessing the data contained on the secured LU, cf. LUN Masking

3.1.64

Protocol

set of rules that define and constrain data, operations or both. For example, xmlCIM uses XML as its transfer syntax and HTTP as the request-reply protocol HTTP is layered over the TCP/IP network protocol

3.1.65

Provider

COM server that communicates with managed objects to access data and event notifications from a variety of sources, such as the system registry or an SNMP device. Providers forward this information to the CIM Object Manager for integration and interpretation

class provider: A COM server that supplies class definitions. Class providers can support data retrieval, modification, deletion, enumeration and query processing.

property provider: A type of provider that supports the retrieval and modification of the CIM properties.

3.1.66

Relationship

SOURCE (DMTF)

refer to UML Standards.

3.1.67

Required Reference

SOURCE (DMTF)

refer to UML Standards

3.1.68

SA Advertisement (SAAdvert)

information describing a service that consists of the Service Type, Service Access Point, lifetime and Attributes

3.1.69

SAN

Acronym for storage area network.

Acronym for Server Area Network that connects one or more servers.

Acronym for System Area Network for an interconnected set of system elements.

A group of fabrics that have common leaf elements.

3.1.70

Scope

set of services, typically making up a logical administrative group

3.1.71

Semantics

meaning or behavior associated with an entity. For example, we might say the semantics of the method, `resync_mirror()`, is encoded in the method name. By contrast, the semantics of the UNIX `ioctl()` method is encoded in the command parameter.

3.1.72

Server

process that fields and/or dispatches requests. Honoring a request may involve more than one server process distributed over one or more computer systems. The collection of server processes that are involved in honoring a request are known as service providers

3.1.73

Service Access Point

network address and port number of a process offering a service

3.1.74

Service Acknowledgement (SrvAck)

reply to a SrvReg request

3.1.75

Service Agent (SA)

in the context of SLP, this refers to a process working on behalf of one or more services to advertise the services in the network

3.1.76

Service Agent Server (SAServer)

in the context of SLP, this refers to a process working on behalf of one or more Service Agents to listen on a particular port number for SLP service requests

3.1.77

Service Deregister (SrvDereg)

request to deregister a service or some attributes of a service (optional)

3.1.78

Service Register (SrvReg)

request to register a service or some attributes of a service

3.1.79

Service Reply (SrvRply)

reply to a Service Request

3.1.80

Service Request (SrvRqst)

request for a service on the network

3.1.81

SES

ISO/IEC 14776-371 (under study and based on ANSI INCITS 305-1998 (R2003); ANSI INCITS 305-1998/AM-1-2000 (R2003)) for management of environmental factors such as typewriter, power, voltage, etc.

3.1.82

Service Type

class of a network service represented by a unique string (for example a namespace assigned by IANA)

3.1.83

Service Type Reply (SrvTypeRply)

reply to a Service Type Request (optional)

3.1.84

Service Type Request (SrvTypeRqst)

request for all types of service on the network (optional)

3.1.85

Service Type Template

formalized, computer-readable description of a Service Type

3.1.86

Service URL

Uniform Resource Locator for a service containing the service type name, network family, Service Access Point and any other information needed to contact the service

3.1.87

SLP

acronym for Service Location Protocol

3.1.88

SNIA

acronym for Storage Networking Industry Association. An association of producers and consumers of storage networking products whose goal is to further storage networking technology and applications

3.1.89

SNMP

acronym for Simple Network Management Protocol. 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

3.1.90

SNMP Trap

a type of SNMP message used to signal that an event has occurred

3.1.91

Soft Zone

Zone consisting of Zone Members that are made visible to each other through Client Service requests. Typically, Soft Zones contain Zone Members that are visible to devices via Name Server exposure of Zone Members. The Fabric does not enforce a Soft Zone. Note that well known addresses are implicitly included in every Zone

3.1.92

SRM

acronym for storage resource management. Management of physical and logical storage resources, including storage elements, storage devices, appliances, virtual devices, disk volume and file resources.

3.1.93

SSL

acronym for Secure Sockets Layer. 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)

3.1.94

SSP

acronym for Storage Service Provider

3.1.95

Switch

fibre channel interconnect element that supports a mesh topology

3.1.96

Symmetric Virtualization Appliance

synonym for an appliance that provides in-band virtualization. In-band virtualization appliance is the preferred term

3.1.97

Synchronous

method that blocks the calling thread until all operations have completed or failed

3.1.98

Syntax

(The structure of strings in some language. A language's syntax is described by a grammar. For example, the syntax of a binary number could be expressed as

binary_number = bit [binary_number]

bit = "0" | "1"

Meaning that a binary number is a bit optionally followed by a binary number and a bit is a literal zero or one digit. The meaning of the language is given by its semantics

3.1.99

TLS

acronym for Transport Layer Security

3.1.100

Transfer Syntax

formal rules (i.e., the protocol) governing the format (or representation) of messages as they are transferred between clients and servers

3.1.101

UDP

acronym for User Datagram Protocol. An Internet protocol that provides connectionless datagram delivery service to applications. Abbreviated UDP. UDP over IP adds the ability to address multiple endpoints within a single network node to IP

3.1.102

UML Standards

appendix D of the *Common Information Model (CIM) Specification, V2.0* (March 3, 1998)

Class - represented by a **rectangle**.

class name either stands alone in the rectangle or is in the uppermost segment. If present, the segment below the segment containing the name contains the properties of the class. If present, a third region indicates the presence of methods.

Lines indicate:

- **Inheritance** relationships (blue lines with arrows) – Otherwise known as “is-a” relationships

- **Aggregation/component** relationships (green lines with a diamond shape at the “aggregating” end) - Otherwise known as “has-a” relationships
- **Dependency and other** relationships (red lines) – Some of which are “uses-a” relationships
- **Relationship Labels** - Inheritance relationships are not specifically labelled or named, while all other associations are named
- **Cardinality** - the cardinalities of the references on both sides of an association are indicated by numeric values or an asterisk (*) at the endpoints of the association

The following cardinalities are typically used in the CIM Schema:

0..1 - Indicates an optional single-valued reference

1 - Indicates a **required**, single-valued reference

1..n or 1..* - Indicates either a single or multi-valued reference, that is **required***, 0..n or 0..* - Indicates an optional, single or multi-valued reference

Required Reference - the object and the association shall exist (or be instantiated) when the *other* referenced class is defined.

Weak Reference – indicated by the symbol, “w”, indicates that the referenced endpoint or class is “weak” or “weakly associated” with respect to the *other* class participating in the association. This means that the referenced class is scoped or named relative to the other class and the identifying keys of the other class are placed as properties in the “weak” class.

NOTE Note that this is not standard UML convention, but an added symbol in CIM diagrams.

3.1.103

Universal Markup Language (UML)

refer to UML Standards

3.1.104

URL

Uniform Resource Locator

3.1.105

User Agent (UA)

in the context of SLP, a process that attempts to establish contact with one or more services. A User Agent retrieves service information from Service Agents or Directory Agents

3.1.106

VAR

Value Added Remarketeer

3.1.107

Volume Set

synonym for virtual disk

3.1.108

VPD

Vital Product Data, a portion of the SCSI-2 specification (see 2.1, “International standards”)

3.1.109

WAN

acronym for Wide Area Network. A communications network that is geographically dispersed and that includes telecommunications links

3.1.110

Weak Reference

refer to UML Standards

3.1.111

WBEM

acronym for Web Based Enterprise Management. Web-Based Enterprise Management is an initiative in the DMTF. Abbreviated WBEM. It is a set of technologies that enables 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, CIM to create a conceptual view of the enterprise

3.1.112

W3C

World-Wide Web Consortium.

3.1.113

XML

acronym for eXtensible Markup Language. A universal format for structured documents and data on the World-Wide Web. Abbreviated XML. The World-Wide Web Consortium is responsible for the XML specification. cf. <http://www.w3.org/XML/>

3.1.114

XML-CIM Listener

server application that receives and processes XML-CIM Export Message requests and issues CIM Export Message responses

3.1.115

XML-CIM Server

server that receives and processes XML-CIM Operation Requests and issues XML-CIM Operation Responses

3.1.116

Zone

group of ports and switches that allow access. Defined by a zone definition. cf. Hard Zone, Soft Zone

A collection of Zone Members. Zone Members in a Zone are made aware of each other, but not made aware of devices outside the Zone. A Zone can be defined to exist in one or more Zone Sets

3.1.117

Zone Definition

the parameters that define a Zone: the Zone Name, number of Zone Members and Zone Member definition

3.1.118

Zone Member

N_Port (or NL_Port) to be included in a Zone, as specified by its Zone Member Definition. N_Ports at well known addresses shall not be specified as Zone Members

3.1.119

Zone Member Definition

parameter by which a Zone Member is specified. A Zone Member may be specified by:

- a port on a Switch, (specifically by Domain_ID and port number); or,
- the device's N_Port_Name; or,
- the device's address identifier; or,
- the device's Node_Name.

3.1.120

Zone Set

one or more Zones that may be activated or deactivated as a group.

Zone Set Name: The name assigned to a Zone Set.

Zone Set State: The state of a Zone Set, which may be either activated or deactivated.

Active Zone Set: The Zone Set that is currently activated. Only one Zone Set may be activated at any time.

3.2 Symbols and abbreviations

	concatenate
= or EQ	equal
≈	approximately equal
API	application programming interface
CDB	command descriptor block
FC	Fibre Channel
HBA	host bus adapter
IDL	interface definition language
IETF	Internet Engineering Task Force
IMA	iSCSI Management API
IP	Internet Protocol
iSCSI	Internet SCSI
iSD	iSCSI Direct
LSB	least significant bit
OS	operating system
RFC	Request for comments
SCSI	Small Computer System Interface
SAM-3	SCSI architecture model
SAN	storage area network
SNIA	Storage Networking Industry Association
SNMP	simple network management protocol
SPC-3	SCSI primary commands-3
TC	Technical Committee
TCP	Transmission control protocol
UDP	User datagram protocol

3.3 Keywords

3.3.1

expected

keyword used to describe the behavior of the hardware or software in the design models presumed by this standard. Other hardware and software design models may also be implemented

3.3.2

invalid

keyword used to describe an illegal or unsupported bit, byte, word, field or code value. Receipt of an invalid bit, byte, word, field or code value shall be reported as an error

3.3.3

mandatory

keyword indicating an item that is required to be implemented as defined in this standard to claim compliance with this standard

3.3.4

may

keyword that indicates flexibility of choice with no implied preference

3.3.5

may not

keywords that indicates flexibility of choice with no implied preference

3.3.6

obsolete

keyword indicating that an item was defined in prior standards but has been removed from this standard

3.3.7

opaque

keyword indicating that a value has no semantics or internal structure

3.3.8

optional

keyword that describes features that are not required to be implemented by this standard. However, if any optional feature defined by this standard is implemented, it shall be implemented as defined in this standard

3.3.9

reserved

keyword referring to bits, bytes, words, fields and code values that are set aside for future standardization. Their use and interpretation may be specified by future extensions to this or other standards. A reserved bit, byte, word or field shall be set to zero or in accordance with a future extension to this standard. Recipients are not required to check reserved bits, bytes, words or fields for zero values. Receipt of reserved code values in defined fields shall be reported as an error

3.3.10

shall

keyword indicating a mandatory requirement. Designers are required to implement all such requirements to ensure interoperability with other products that conform to this standard

3.3.11

should

keyword indicating flexibility of choice with a preferred alternative, equivalent to the phrase "it is recommended"

3.4 Conventions

Certain words and terms used in this International Standard have a specific meaning beyond the normal English meaning. These words and terms are defined either in clause 3 or in the text where they first appear.

Fields containing only one bit are usually referred to as the name bit instead of the name field.

Numbers that are not immediately followed by lower-case b or h are decimal values.

Numbers immediately followed by lower-case b (xxb) are binary values.

Numbers immediately followed by lower-case h (xxh) are hexadecimal values.

Hexadecimal digits that are alphabetic characters are upper case (i.e., ABCDEF, not abcdef).

Hexadecimal numbers may be separated into groups of four digits by spaces. If the number is not a multiple of four digits, the first group may have fewer than four digits (e.g., AB CDEF 1234 5678h)

Decimal fractions are initiated with a comma (e.g., two and one half is represented as 2,5).

Decimal numbers having a value exceeding 999 are separated with a space(s) (e.g., 24 255).

An alphanumeric list (e.g., a, b, c or A,B,C) of items indicate the items in the list are unordered.

A numeric list (e.g., 1, 2, 3) of items indicate the items in the list are ordered (i.e., item 1 shall occur or complete before item 2).

In the event of conflicting information the precedence for requirements defined in this standard is

- 1) text,
- 2) tables,
- 3) figures.

4 Introduction

4.1 Preamble

Storage Area Networks (SANs) are emerging as a prominent layer of IT infrastructure in enterprise class and midrange computing environments. Applications and functions driving the emergence of SAN technology include:

- Sharing of vast storage resources between multiple systems,
- 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.

To accelerate the emergence of SANs 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 specification (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 SAN topologies. As such, this interface overcomes the deficiencies associated with legacy management.

4.2 Business rationale

This interface is targeted at creating broad multi-vendor management interoperability and thus increasing customer satisfaction. To that end, this specification defines an “open” and extensible interface that allows subsystems and devices within the global context of a SAN 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 SAN management interface, more flexibly select between multiple vendors when building the hierarchy of software systems required to manage a large SAN independent of the underlying hardware systems. Additionally, SAN integrators can more flexibly select between alternate hardware vendors when constructing SAN configurations. Broad adoption of the standards defined and extended in this specification will provide increased customer satisfaction and will

- more rapidly expand the acceptance of SAN,
- accelerate customer acquisition of SAN 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.

4.3 Interface definition

This management interface allows storage management systems to reliably identify, classify, monitor and control physical and logical resources in a SAN. 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 1.

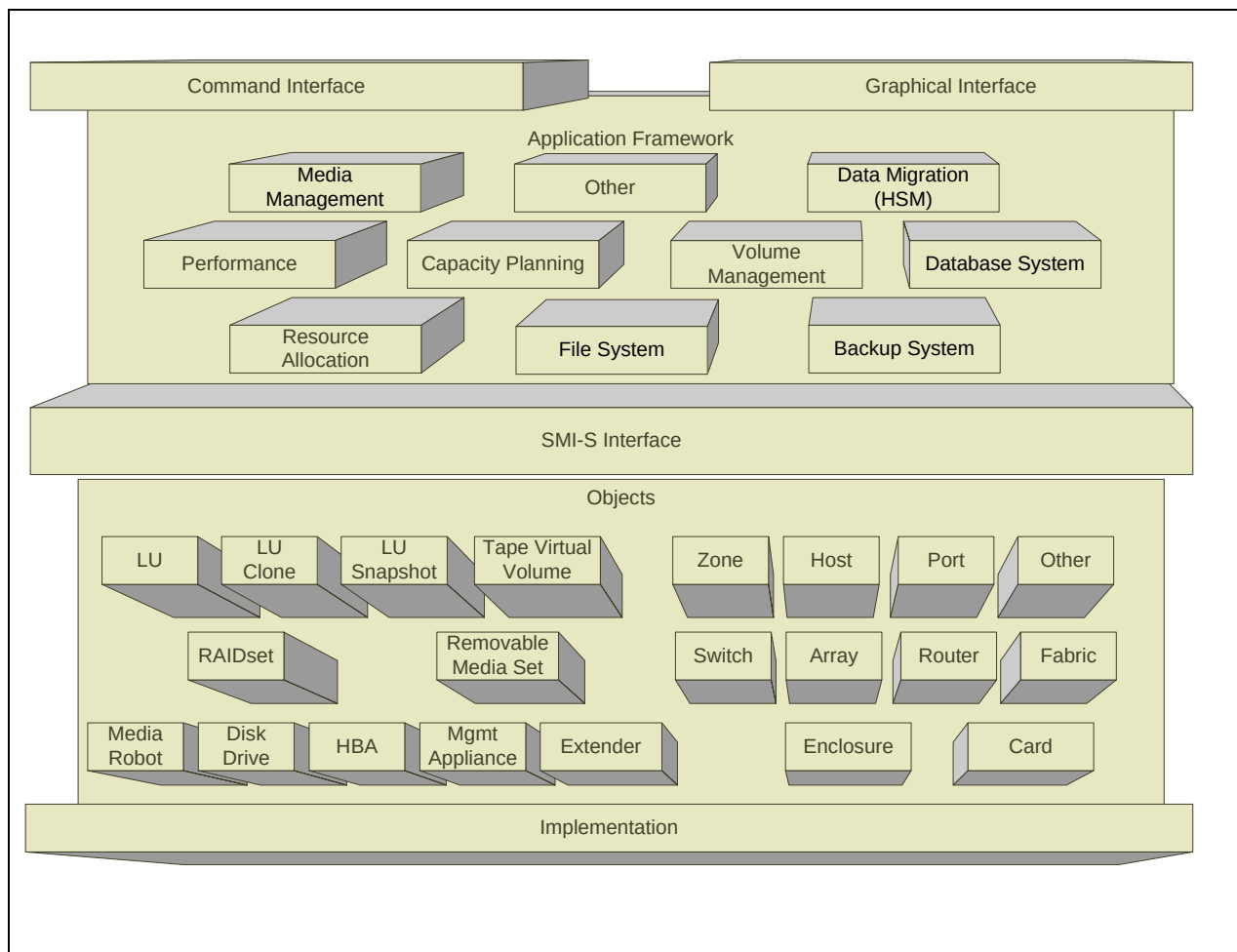


Figure 1 - Interface functions

The diagram illustrates that functions of the interface can be distributed across multiple SAN devices (i.e., Switches or Array Controllers) and/or software systems (i.e., Discovery Systems). While the functionality of the interface is likely to be distributed within or across a SAN, to insure that monitoring and control operations by clients are consistent and reliable, care should be taken to prevent the state of a given resource being 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 will need to be coordinated by a single monitoring entity to insure information consistency. Should the SRM application and Backup engine obtain different available bandwidth information for a given Fibre Channel path from multiple unsynchronized sources, conflicts can arise and degrade the efficiency of the environment.

Satisfying this requirement is the responsibility of parties configuring Storage and Network management clients in conjunction with the primitives defined in the specification.

NOTE Within this architecture (as depicted by the illustration above) entities like an appliance-based volume manager have the option to 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 shall 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) shall 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.

Relative to Figure 1, examples of long-term functional requirements for the interface to properly satisfy the needs of clients using it include the following.

- a) Clients shall be able to obtain sufficient information to discern the topology of the SAN.
- b) Clients shall be able to reliably identify resources that have experienced an error/fault condition that has resulted in degraded/disabled operation.
- c) Clients shall be able to construct a zone of allocation around a select group of host and storage resources.
- d) Clients shall 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 shall 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 shall be able to dynamically allocate non-volatile storage resources.

NOTE 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.

- g) Clients shall be able to access sufficient topology and component information to allow a Storage Resource Management (SRM) application like a SAN performance monitor to examine topology and line utilization, in such a way that performance bottlenecks can be exposed.
- h) Clients shall 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.
- i) Clients shall 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 communication ports.
- j) Clients shall 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 the following.

- a) Select a logical communication port over which to send/receive data.
- b) Read/Write data to a volume.
- c) Identify and recover from data communication errors and failures.
- d) Synchronization message between two cluster nodes.
- e) Log a new communication device into a network.

4.4 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) or available out-of-band (i.e., over a LAN/MAN/WAN) or available over a mix of both, virtually all devices in a SAN have (or soon will have), access to a common communication transport suitable for carrying management information content (e.g., TCP/IP) that is used to transmit a standardized encoding (e.g., CIM-XML) of recognized semantics (e.g., CIM);
- b) **Increased device manageability:** Through a common, general-purpose network transport and, where necessary, the use of proxy services through another resource (e.g., general purpose computer system), devices can support a 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 management protocols with an extensible, platform independent, human readable, content describable communication language for the first time. These protocols provide appropriate abstraction by 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;
- d) **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 maintain-

ing real-time distributed state for logical entities. Figure 2 below provides an example of a single SAN built from multiple classes of components spanning three physical locations (i.e., Sites A, B and C).”.

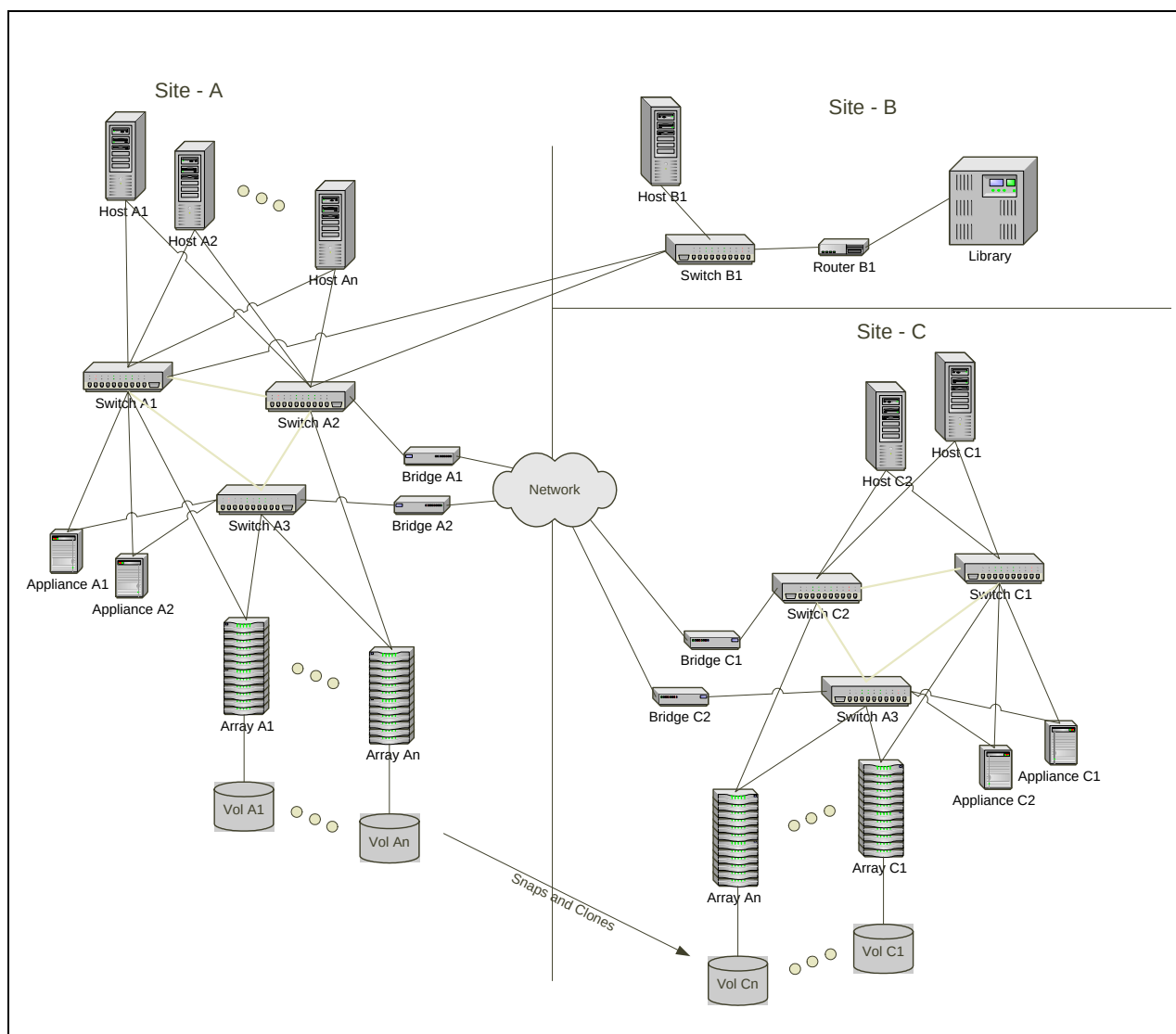


Figure 2 - Large SAN Topology

4.5 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 3 provides an example client/server distribution using in-band TCP/IP communication, out of band TCP/IP communication 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 communication 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 the illustration. All other clients and servers communicate via direct access to a common communication transport.

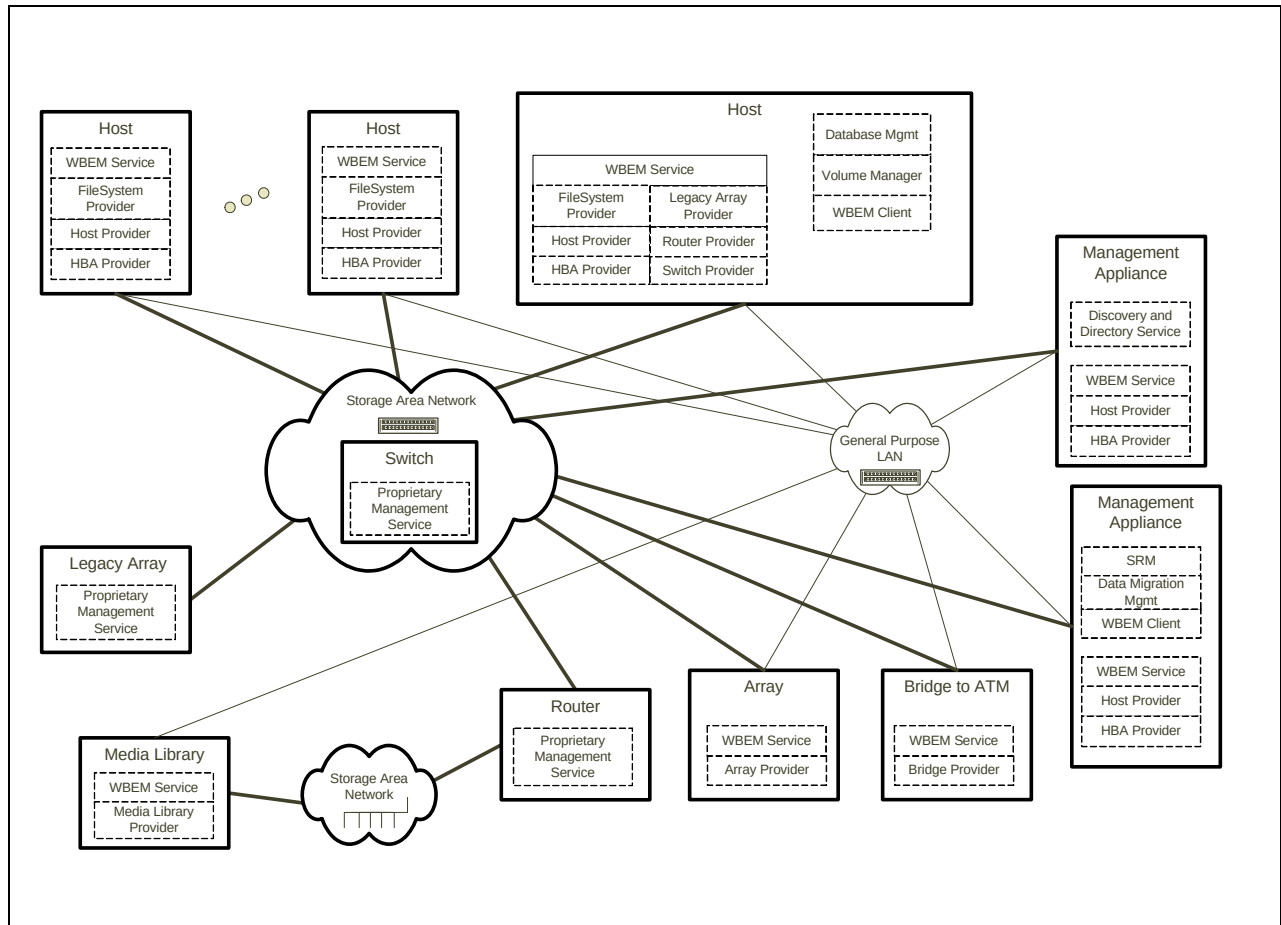


Figure 3 - Example Client Server Distribution in a SAN

4.6 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 Storage Management Initiative Specification.

- a) Consistency: State within an 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 objects is able to do so in isolation of other clients, who are simultaneously executing management actions against those same objects.
- c) Durability: Atomicity, consistency and isolation are preserved independent of the failure of any entity or communication path in the management environment.
- d) Consistent Name Space: Managed objects in the SAN 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: