Technical Standard

Management Protocol Profiles (XMPP)
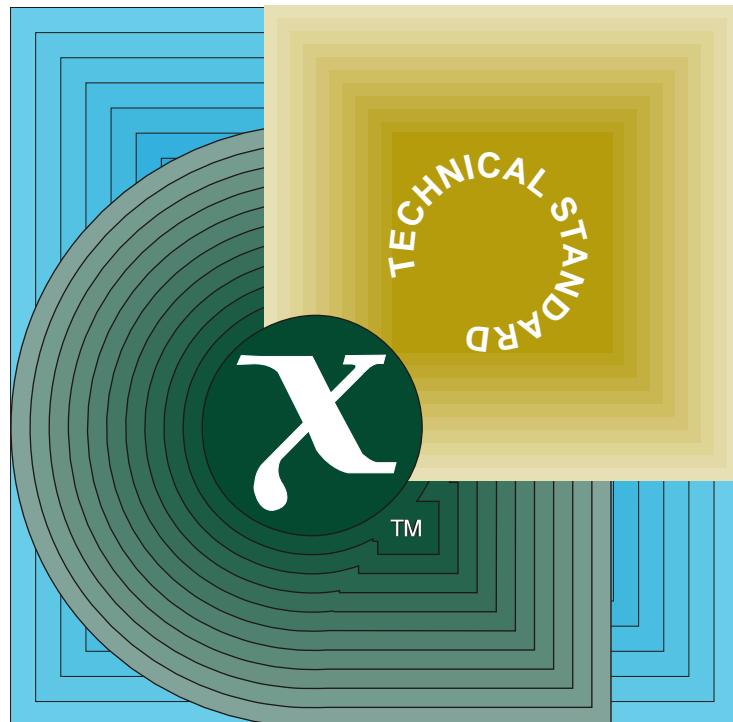
THE *Open* GROUP

[This page intentionally left blank]

X/Open CAE Specification

Systems Management: Management Protocol Profiles (XMPP)

X/Open Company Ltd.

/

Contents

Preface

X/Open

X/Open is an independent, worldwide, open systems organisation supported by most of the world's largest information systems suppliers, user organisations and software companies. Its mission is to bring to users greater value from computing, through the practical implementation of open systems.

X/Open's strategy for achieving this goal is to combine existing and emerging standards into a comprehensive, integrated, high-value and usable system environment, called the Common Applications Environment (CAE). This environment covers the standards, above the hardware level, that are needed to support open systems. It provides for portability and interoperability of applications, and allows users to move between systems with a minimum of retraining.

The components of the Common Applications Environment are defined in X/Open CAE Specifications. These contain, among other things, an evolving portfolio of practical application programming interfaces (APIs), which significantly enhance portability of application programs at the source code level, and definitions of, and references to, protocols and protocol profiles, which significantly enhance the interoperability of applications.

The X/Open CAE Specifications are supported by an extensive set of conformance tests and a distinct X/Open trademark - the XPG brand - that is licensed by X/Open and may be carried only on products that comply with the X/Open CAE Specifications.

The XPG brand, when associated with a vendor's product, communicates clearly and unambiguously to a procurer that the software bearing the brand correctly implements the corresponding X/Open CAE Specifications. Users specifying XPG-conformance in their procurements are therefore certain that the branded products they buy conform to the CAE Specifications.

X/Open is primarily concerned with the selection and adoption of standards. The policy is to use formal approved *de jure* standards, where they exist, and to adopt widely supported *de facto* standards in other cases.

Where formal standards do not exist, it is X/Open policy to work closely with standards development organisations to assist in the creation of formal standards covering the needed functions, and to make its own work freely available to such organisations. Additionally, X/Open has a commitment to align its definitions with formal approved standards.

X/Open Specifications

There are two types of X/Open specification:

- *CAE Specifications*

  CAE (Common Applications Environment) Specifications are the long-life specifications that form the basis for conformant and branded X/Open systems. They are intended to be used widely within the industry for product development and procurement purposes.

Developers who base their products on a current CAE Specification can be sure that either the current specification or an upwards-compatible version of it will be referenced by a future XPG brand (if not referenced already), and that a variety of compatible, XPG-branded systems capable of hosting their products will be available, either immediately or in the near future.

CAE Specifications are not published to coincide with the launch of a particular XPG brand, but are published as soon as they are developed. By providing access to its specifications in this way, X/Open makes it possible for products that conform to the CAE (and hence are eligible for a future XPG brand) to be developed as soon as practicable, enhancing the value of the XPG brand as a procurement aid to users.

- *Preliminary Specifications*

  These are specifications, usually addressing an emerging area of technology, and consequently not yet supported by a base of conformant product implementations, that are released in a controlled manner for the purpose of validation through practical implementation or prototyping. A Preliminary Specification is not a ''draft'' specification. Indeed, it is as stable as X/Open can make it, and on publication has gone through the same rigorous X/Open development and review procedures as a CAE Specification.

  Preliminary Specifications are analogous with the ''trial-use'' standards issued by formal standards organisations, and product development teams are intended to develop products on the basis of them. However, because of the nature of the technology that a Preliminary Specification is addressing, it is untried in practice and may therefore change before being published as a CAE Specification. In such a case the CAE Specification will be made as upwards-compatible as possible with the corresponding Preliminary Specification, but complete upwards-compatibility in all cases is not guaranteed.

In addition, X/Open periodically publishes:

- *Snapshots*

  Snapshots are ''draft'' documents, which provide a mechanism for X/Open to disseminate information on its current direction and thinking to an interested audience, in advance of formal publication, with a view to soliciting feedback and comment.

  A Snapshot represents the interim results of an X/Open technical activity. Although at the time of publication X/Open intends to progress the activity towards publication of an X/Open Preliminary or CAE Specification, X/Open is a consensus organisation, and makes no commitment regarding publication.

  Similarly, a Snapshot does not represent any commitment by any X/Open member to make any specific products available.

X/Open Guides

X/Open Guides provide information that X/Open believes is useful in the evaluation, procurement, development or management of open systems, particularly those that are X/Open-compliant.

X/Open Guides are not normative, and should not be referenced for purposes of specifying or claiming X/Open-conformance.

This Document

To achieve the goal of interoperability between conformant management systems, one of the important requirements is the definition of a common communications protocol. There are several appropriate communications mechanisms for management systems:

- OSI Common Management Information Protocol (CMIP)

- Internet Protocol Suite (IPS) Simple Network Management Protocol (SNMP)

- Remote Procedure Call (RPC) mechanisms

This CAE Specification, the X/Open **Systems Management: Management Protocol Profiles**, addresses communications using the management protocols, CMIP and SNMP. RPC-based mechanisms will be addressed in future documents.

Recognising the existence of significant existing work in this area, this document references profiles and definitions that already exist for these protocols.

Trademarks

X/Open™ and the 'X' device are trademarks of X/Open Company Ltd. in the U.K. and other countries.

Referenced Documents

The following documents are referenced in this specification:

CMISP
Common Management Information Services and Protocols for the Internet (CMOT and CMIP), U.S.Warrior, L.Besaw, L.LaBarre, B.D.Handspicker, RFC 1189, October 1990.

COMIX
Guide to IPS-OSI Coexistence and Migration, X/Open Company Limited, document G140, November 1991.

IP
Internet Protocol (IP), J.Postel, RFC 791, September 1981.

ISO 8072/AD1
ISO 8072/SD1, Information Processing Systems - Open Systems Interconnection - Transport Service Definition - Addendum 1: Connectionless-Mode Transmission, 1986

ISO 8326
ISO 8326:1988, Information processing systems - Open Systems Interconnection - Basic connection oriented session service definition.

ISO 8326/AD2
ISO 8326/AD2, Information processing systems - Open Systems Interconnection - Basic connection oriented session service definition. Addendum 2 to incorporate unlimited user data.

ISO 8327
ISO 8327:1987, Information processing systems - Open Systems Interconnection - Basic connection oriented session protocol specification.

ISO 8327/AD2
ISO 8327/AD2, Information processing systems - Open Systems Interconnection - Basic connection oriented session protocol specification. Addendum 2 to incorporate unlimited user data.

ISO 8649:1988
ISO 8649:1988, Information processing systems - Open Systems Interconnection - Service definition for the Association Control Service Element.

ISO 8649:1988/Amd.1:1990
ISO/IEC 8649:1988/Amd.1:1990, Information Processing Systems - Open Systems Interconnection - ACSE Service Definition, Amendment 1 covering authentication during association establishment.

ISO 8650
ISO 8650:1988, Information processing systems - Open Systems Interconnection - Protocol specification for the Association Control Service Element.

ISO 8650:1988/Cor.1:1990
ISO/IEC 8650:1988/Cor.1:1990, Information Processing Systems - Open Systems Interconnection - Protocol specification for the Association Control Service Element - Technical Corrigendum 1.

ISO 8650:1988/Amd.1:1990
    ISO/IEC 8650:1988/Amd.1:1990, Information Processing Systems - Open Systems Interconnection - ACSE Protocol Specification, Amendment 1 covering authentication during association establishment.

ISO 8822
    ISO 8822:1988, Information processing systems - Open Systems Interconnection - Connection oriented presentation service definition.

ISO 8823
    ISO 8823:1988, Information processing systems - Open Systems Interconnection - Connection oriented presentation protocol specification.

ISO 8824
    ISO 8824:1990, Information processing systems - Open Systems Interconnection - Specification of Abstract Syntax Notation One (ASN.1).

ISO 8825
    ISO 8825:1990, Information processing systems - Open Systems Interconnection - Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1).

ISO 9072-1
    ISO 9072-1:1989, Information processing systems - Text communication - Remote Operations. Part 1 : Model, Notation and Service definition.

ISO 9072-2
    ISO 9072-2:1989, Information processing systems - Text communication - Remote Operations. Part 2 : Protocol specification.

ISO 9595
    ISO 9595:1991, Information processing systems - Open Systems Interconnection - Common management information service definition.

ISO 9596-1
    ISO 9596-1:1991, Information processing systems - Open Systems Interconnection - Common management information protocol definition.

ISO 10040
    ISO 10040, Information processing systems - Open Systems Interconnection - Systems management overview.

ISO ISP 11183-1
    ISO ISP 11183-1, Information technology - International Standardised Profiles AOMnn OSI Management - Part 1 : Specification of ACSE, Presentation and Session protocols for use by CMISE and ROSE.

ISO ISP 11183-2
    ISO ISP 11183-2, Information technology - International Standardised Profiles AOMnn OSI Management - Part 2 : AOM12 - Enhanced Management Communications.

ISO ISP 11183-3
    ISO ISP 11183-3, Information technology - International Standardised Profiles AOMnn OSI Management - Part 3 : AOM11 - Basic Management Communications.

ISO DISP 12059-0
    ISO/IEC DISP 12059-0, Information Technology -International Standardized Profiles AOM2n OSI Management - Common Information for Management Functions - Part 0: Common Definitions, July 1992.

ISO DISP 12059-1
ISO/IEC DISP 12059-1, Information Technology -International Standardized Profiles AOM2n OSI Management - Common Information for Management Functions - Part 1: Object Management, July 1992.

ISO DISP 12059-2
ISO/IEC DISP 12059-2, Information Technology -International Standardized Profiles AOM2n OSI Management - Common Information for Management Functions - Part 2: State Management, July 1992.

ISO DISP 12059-3
ISO/IEC DISP 12059-3, Information Technology -International Standardized Profiles AOM2n OSI Management - Common Information for Management Functions - Part 3: Attributes for Representing Relationships, July 1992.

ISO DISP 12059-4
ISO/IEC DISP 12059-4, Information Technology -International Standardized Profiles AOM2n OSI Management - Common Information for Management Functions - Part 4: Alarm Reporting, July 1992.

ISO DISP 12059-5
ISO/IEC DISP 12059-5, Information Technology -International Standardized Profiles AOM2n OSI Management - Common Information for Management Functions - Part 5: Event Report Management, July 1992.

ISO DISP 12059-6
ISO/IEC DISP 12059-6, Information Technology -International Standardized Profiles AOM2n OSI Management - Common Information for Management Functions - Part 6: Log Control, July 1992.

ISO DISP 12060-1
ISO/IEC DISP 12060-1, Information Technology -International Standardized Profiles AOM2n OSI Management - Management Functions - Part 1: AOM211 - General Management Capabilities, July 1992.

ISO DISP 12060-2
ISO/IEC DISP 12060-2, Information Technology -International Standardized Profiles AOM2n OSI Management - Management Functions - Part 2: AOM212 - Alarm Reporting and State Management, July 1992.

ISO DISP 12060-3
ISO/IEC DISP 12060-3, Information Technology -International Standardized Profiles AOM2n OSI Management - Management Functions - Part 3: AOM213 - Alarm Reporting, July 1992.

ISO DISP 12060-4
ISO/IEC DISP 12060-4, Information Technology -International Standardized Profiles AOM2n OSI Management - Management Functions - Part 4: AOM221 - General Event Report Management, July 1992.

ISO DISP 12060-5
ISO/IEC DISP 12060-5, Information Technology -International Standardized Profiles AOM2n OSI Management - Management Functions - Part 5: AOM231 - General Log Control, July 1992.

ISO TR10000-1
>   ISO TR10000-1:1990, Information technology - Framework and taxonomy of International Standardised Profiles - Part 1 : Framework.

ISO TR10000-2
>   ISO TR10000-2:1990, Information technology - Framework and taxonomy of International Standardised Profiles - Part 2 : Taxonomy.

Problem Statement
>   Systems Management: Problem Statement, Snapshot, X/Open Company Limited, document S110, August 1991.

RFC 1006
>   RFC 1006, ISO transport services on top of the TCP: Version 3, Rose, M.T.; Cass, D.E., May, 1987.

RFC 1085
>   ISO Presentation Services on top of TCP/IP based internets, M.T.Rose, RFC 1085, December 1988.

SNMP
>   Simple Network Management Protocol, J.D.Case, M.Fedor, M.L.Schoffstall, C.Davin, RFC 1157, May 1990.

SNMP2
>   RFC 1448 Protocol Operations for version 2 of the Simple Network Management Protocol (SNMPv2), J.D.Case, K.McCloghrie, M.T.Rose, S.L.Waldbusser, RFC 1448

SNMP2TM
>   Transport Mappings for SNMPv2, J.D.Case, K.McCloghrie, M.T.Rose, S.L.Waldbusser, RFC 1449

TCP
>   Transmission Control Protocol, J.Postel and J.Reynolds, RFC 793, September 1981.

UDP
>   User Datagram Protocol, J.Postel, RFC 768, August 1980.

XMP
>   Systems Management: Management Protocol API, CAE Specification, X/Open Company Limited, document C306, December 1993.

XRM
>   Systems Management: Reference Model, Guide, X/Open Company Limited, document G207, August 1993.

Chapter 1

Introduction

The X/Open **Systems Management Reference Model** (see reference XRM) describes a model of systems management based on the use of managed objects to represent the real resources present in the system.

This document defines a profile of communications protocols that can be used to provide connectivity within such a distributed management system.

The X/Open Systems Management Reference Model is intended to satisfy several high-level system requirements:

Portability
: The ability to make software on managed and managing systems portable in source code form between different vendors' systems by extending the X/Open Common Applications Environment (CAE).

Interoperability
: The ability of management systems, and components of such systems from different vendors, to interwork, thus allowing a network of heterogeneous systems to be managed as a single system.

Location Transparency
: The ability to administer resources without the need to be explicitly aware of their location.

Extensibility
: The ability to extend the scope and capabilities of the management system and to implement different management policies as required. This includes the ability to make use of new communications protocols.

Robustness
: The ability of the management system to provide integrity and the necessary levels of security and reliability.

The X/Open Systems Management Programme (XSM) is defined in terms of a suite of documents that, taken together, will describe all the components needed to achieve the goals listed above.

The first of these documents is the X/Open **Systems Management Problem Statement** (see the referenced Problem Statement). The **Problem Statement** document provides an overview of the problem and a review of the current activities at the time it was published.

The X/Open **Systems Management Reference Model** (see reference XRM) builds on the **Problem Statement**, providing a framework in which the various components of the solution can be identified. The individual components will be defined in subsequent documents.

The Reference Model is based on the use of object-oriented specification techniques. This in no way requires an implementation to use object-oriented technology. Object-oriented techniques have been adopted in this area by several other bodies, including vendors, standards bodies, and other industry consortia.

Scope and Purpose

The X/Open Systems Management Programme (XSM) is concerned with the definition of those specifications necessary for the implementation of distributed management systems. In order to meet the goal of interoperability it is necessary for differing implementations to share both a common means of transferring information *and* a common understanding of that information.

This document addresses the first of these aims, specifically the provision of a profile for a standard management protocol. There are several appropriate communications mechanisms suitable for use in management systems. These include the OSI Common Management Information Protocol (CMIP) and the Internet Protocol Suite (IPS) Simple Network Management Protocol (SNMP).

The XSM programme recognises that these differing mechanisms each have applicability in different circumstances and will provide those specifications needed for management systems to be able to take advantage of the most appropriate mechanism. This document addresses communications based on the management protocols, CMIP and SNMP.

Relationship to Other Work

The XSM programme is intended to be compatible with existing *de jure* and *de facto* standards and specifications. Recognising the existence of such work in this area, this specification makes reference to the International Standardised Profile (ISP) developed within the OSI Regional Workshops, and to the relevant RFCs developed within the Internet Engineering Task Force (IETF).

Benefits of Profiles

The use of profiles increases the likelihood of interoperability between systems. This is done by reducing the number of permutations available from combining standards and options. Thus, implementors can build systems having more confidence of interoperability with other systems. Procurers can purchase with the same degree of confidence. In turn, this confidence is reflected in the marketplace by increased availability and choice of conforming systems.

Systems that are intended to conform to the XSM specifications need not support all of the management protocol specifications referenced in this document. However, if a system supports a particular management protocol that is specified in this document, it is required to implement the specification referenced here.

Relationship to Other XSM Specifications

- **Reference Model**
  The profiles in this document define part of a Communications Mechanism as described in the X/Open **Systems Management Reference Model** (see reference XRM).

- **Management Protocols (XMP) API**
  The **Systems Management Management Protocols (XMP) API Specification** (see reference XMP) defines an API suitable to access the services supported by these profiles.

OSI Management Profiles

The Common Management Information Protocol (CMIP) is the management protocol developed as part of the OSI protocol suite. It is defined in ISO/IEC 9596-1:1991.

Implementations intended to operate within an OSI environment shall conform to one or more of the OSI Management Profiles, AOM1n or AOM2n. The AOM1n profiles define basic and enhanced management communications. The AOM2n profiles are based on the OSI system management functions.

CMIP may also be implemented within an Internet environment using the functionality defined within RFC1006.

3.1   AOM1n Profiles

The AOM1n profiles are defined in ISP 11183, which consists of 3 parts as follows:

- 11183-1 Specification of ACSE, Presentation and Session protocols for use by CMISE and ROSE

- 11183-2 Enhanced Management Communications (AOM12)

- 11183-3 Basic Management Communications (AOM11)

3.1.1   11183-1

This part of ISO/IEC 11183 specifies how the Association Control Service Element, the Presentation Layer, and the Session Layer standards shall be used to provide the required upper layer functions for the CMISE/ROSE functions. These specifications are therefore the common basis for the application functions as defined in ISO/IEC ISP 11183-2, ISO/IEC 11183-3, and any subsequent parts that might be developed.

This part of ISO/IEC ISP 11183 is the first part, as common text, of a multipart ISP identified in ISO/IEC TR 10000-2 as "AOM, OSI Management Communications".

The profile may be combined with any T-profiles (see ISO/IEC TR 10000) specifying the OSI connection-mode transport service.

The model used is one of two end systems running an end-to-end association using the ACSE, Presentation and Session services and protocols.

Any systems management application entity (SMAE), located on each end system, may be an association-initiator or an association-responder, by agreeing on a common application context definition.

The upper layer functions required for supporting the OSI Management Communications functions are specified in the set of standards identified in the table below.

	ISO Standard	**Corresponding CCITT recommendation**
Application Layer	ISO 9595 (CMIS), 9596-1 (CMIP) ISO 9072-1 (ROSE), 9072-2 (ROP) ISO 8649 (ACSE), 8650 (ACP) ISO 8649:Amd.1, ISO 8659:Amd.1/Cor.1	X.710 (CMIS), X.711 (CMIP) X.219 (ROSE), X.229 (ROP) X.217 (ACSE), X.227 (ACP)
Presentation Layer	ISO 8822 (COPS), 8823 (COPP) ISO 8824 (ASN.1), 8825 (BER)	X.216 (COPS), X.226 (COPP) X.208 (ASN.1), X.209 (BER)
Session Layer	ISO 8326 (COSS), 8327 (COSP) ISO 8326/AD2[1] ISO 8327/AD2[1]	X.215 (COSS), X.225 (COSP) X.215 X.225

[1] AD2 - Addendum 2: incorporation of unlimited user data

3.1.2   AOM12 (11183-2)

This profile specifies how the OSI Common Management Information Service Element (CMISE) combined with the OSI Remote Operation Service Element (ROSE) and based upon Association Control Service Element (ACSE), Presentation layer protocol and Session layer protocol, shall be used to provide the complete set of operation and notification services to the CMISE-service-users of two end systems. The profile AOM12 comprises the support of parts 1 and 2 of ISO/IEC ISP 11183.

The general purpose of AOM12 is to offer a complete platform of complementary communications services between CMISE-service-users within two end systems, whatever the management roles they play: Manager and/or Agent. Therefore, this profile specifies general purpose management communication capabilities by requiring the support of the following CMIP functional units (FUs): kernel, multiple object selection, multiple reply, filter, cancel get; the extended service is out of the scope of this profile. The CMIP FUs are defined in ISO/IEC 9595 and 9596-1.

The support of the complete set of operation and notification services, and of the corresponding protocol elements implies that a conforming implementation of AOM12 does not restrict the capabilities of the CMISE-service-users, and complies with the static CMIP conformance requirements specified in ISO/IEC 9596-1 and 9596-2. It does not imply that all these features shall be used in all instances of communications: the selection of the features depends on the needs and dynamic requirements of the CMISE-service-users. On an individual association, an implementation shall be able to support the use of any subset of the CMIP FUs that includes the kernel FU (the extended service FU is out of scope for this profile): when negotiating FUs, only those for which both CMISE-service-users require support shall be used.

This profile may be referred to by any Application profiles of Management Functions, AOM2n.

This profile requires use of a Connection Oriented Transport Service.

An end system implementing this profile can interwork with an end system implementing profile 11183-3 (AOM11) (Basic Management Communications) in the mode of operation identified by 11183-3 (AOM11). An implementor of this profile must specify whether it is prepared to negotiate downwards to the level of service provided by 11183-3 (AOM11).

3.1.3   AOM11 (11183-3)

This profile specifies how the OSI Common Management Information Service Element (CMISE) combined with the OSI Remote Operation Service Element (ROSE) and based upon Association Control Service Element (ACSE), Presentation layer protocol and Session layer protocol, shall be used to provide a basic subset of operation and notification services to the CMISE-service-users of two end systems. The profile AOM11 comprises the support of parts 1 and 3 of ISO/IEC ISP 11183.

The general purpose of AOM11 is to offer a minimum platform of complementary communications services between CMISE-service-users within two end systems, whatever the management roles they play: Manager and/or Agent. Therefore, this profile defines the support level of the OSI management communication features needed by implementations for providing the kernel FU only. All other FUs are out of the scope of this profile. The CMIP FUs are defined in ISO/IEC 9595 and 9596-1.

The support of this subset of operation and notification services, and of the corresponding protocol elements only implies that a conforming implementation of AOM11 complies with the static CMIP conformance requirements specified in ISO/IEC 9596-1 and 9596-2. It does not imply that all these features shall be used in all instances of communications: the selection of

the features depends on the needs and dynamic requirements of the CMISE-service-users.

This profile specifies a true subset of the AOM12 capabilities: implementations conforming to AOM11 shall be able to interoperate with implementations conforming to AOM12, based on the subset of functions specified in the part 3 of ISO/IEC ISP 11183.

This profile may be referred to by some Application profiles of Management Functions, AOM2n.

This profile requires use of a Connection Oriented Transport Service.

An end system implementing this profile can interwork with an end system implementing profile 11183-2 (AOM12) (Enhanced Management Communications) in the mode of operation identified by 11183-3 (AOM11), as long as the end system implementing 11183-2 (AOM12) is prepared to negotiate downwards to the level of service provided by 11183-3 (AOM11).

3.2   AOM2n Profiles

Management function standards define the management information required to achieve a specific management objective (e.g. state management). The management function profiles are used to specify the requirements for the implementation of a set of management function standards. These sets of functions are selected according to the requirements identified by the industry.

3.2.1   AOM211 (12060-1)

The AOM211 profile is based on the Object management, State management, Attributes for representing relationships and Alarm reporting base standards. The profile is intended for systems implementing fault reporting and configuration management capabilities. These capabilities include the ability to create and delete managed objects, to retrieve and modify managed object attributes, reporting of changes in state, relationship or other attribute values of managed objects, and reporting of alarms. An agent system conforming to this profile has the ability to provide the general management of any managed object. Although the specification of any particular managed object is outside the scope of this profile, an agent system would need to provide access to the managed object. A manager system conforming to this profile should provide the above management capabilities for the management of any managed object.

Since not all of the management functions require the use of all the services offered by CMISE (i.e. systems that are designed to operate in manager-only or agent-only roles, or systems that need to support only a limited set of CMIP capabilities), each of the management function profiles specifies a subset of CMIP capabilities that is required to support the corresponding profile. This is done by referencing the appropriate tables in ISP 11183-2. It is important to note that if a product conforms to a management function profile it does not need to conform to a management communication profile (AOM1x profiles).

The profiles specify the requirements in terms of manager and agent roles. In this way interoperating systems in complimentary management roles conform to the same profile.

Profile	Title	ISP Parts
AOM211	General Management Capability	DISP 12060-1 DISP 12059-0 DISP 12059-1 DISP 12059-2 DISP 12059-3 DISP 12059-4 ISP 11183-1 ISP 11183-2

3.2.2   AOM212 (12060-2)

The AOM212 profile is a subset of AOM211. It is defined for systems requiring alarm reporting and state management. The AOM212 requires the support of alarm notifications, state change notifications and the ability to retrieve and modify the state attributes specified by ISO standards 10164 parts 2 and 4. This profile is most suitable for manager systems that are restricted to a limited management functionality (i.e. only receive alarms and state change reports). On the agent side more functional capabilities are required to enable full management of managed objects.

Since not all of the management functions require the use of all the services offered by CMISE (i.e. systems that are designed to operate in manager-only or agent-only roles, or systems that

need to support only a limited set of CMIP capabilities), each of the management function profiles specifies a subset of CMIP capabilities that is required to support the corresponding profile. This is done by referencing the appropriate tables in ISP 11183-3. It is important to note that if a product conforms to a management function profile it does not need to conform to a management communication profile (AOM1x profiles).

The profiles specify the requirements in terms of manager and agent roles. In this way interoperating systems in complimentary management roles conform to the same profile.

Profile	Title	ISP Parts
AOM212	Alarm Reporting and State Management Capability	DISP 12060-2 DISP 12059-0 DISP 12059-2 DISP 12059-4 ISP 11183-1 ISP 11183-3

3.2.3 AOM213 (12060-3)

The AOM213 profile is a subset of AOM211. It is defined for systems requiring only alarm reporting. The AOM213 requires the support of alarm notifications defined in ISO/IEC 10164-4. This profile is most suitable for manager systems that are restricted to a limited management functionality (i.e. only receive alarms). On the agent side more functional capabilities are required to enable full management of managed objects.

Since not all of the management functions require the use of all the services offered by CMISE (i.e. systems that are designed to operate in manager-only or agent-only roles, or systems that need to support only a limited set of CMIP capabilities), each of the management function profiles specifies a subset of CMIP capabilities that is required to support the corresponding profile. This is done by referencing the appropriate tables in ISP 11183-3. It is important to note that if a product conforms to a management function profile it does not need to conform to a management communication profile (AOM1x profiles).

The profiles specify the requirements in terms of manager and agent roles. In this way interoperating systems in complimentary management roles conform to the same profile.

Profile	Title	ISP Parts
AOM213	Alarm Reporting Capability	DISP 12060-3 DISP 12059-0 DISP 12059-4 ISP 11183-1 ISP 11183-3

3.2.4 AOM221 (12060-4)

The AOM221 profile is based on the Event report management function. The profile specifies the implementation requirements for Event Forwarding Discriminator (EFD) managed objects. The profile specifies the ability to select which notifications are sent by a resource and where they are sent to. An agent system conforming to this profile needs to implement at least one instance of the EFD object class and the ability to manage it. This includes the ability to create and delete an EFD object, and to retrieve and modify its attributes. A manager system should be able to send and receive the required messages to manage the EFD.

Since not all of the management functions require the use of all the services offered by CMISE (i.e. systems that are designed to operate in manager-only or agent-only roles, or systems that need to support only a limited set of CMIP capabilities), each of the management function profiles specifies a subset of CMIP capabilities that is required to support the corresponding profile. This is done by referencing the appropriate tables in ISP 11183-2. It is important to note that if a product conforms to a management function profile it does not need to conform to a management communication profile (AOM1x profiles).

The profiles specify the requirements in terms of manager and agent roles. In this way interoperating systems in complimentary management roles conform to the same profile.

Profile	Title	ISP Parts
AOM221	General Event Report Management	DISP 12060-4 DISP 12059-0 DISP 12059-1 DISP 12059-2 DISP 12059-5 ISP 11183-1 ISP 11183-2

3.2.5   **AOM231 (12060-5)**

The AOM231 profile is based on the Log control management function. The profile specifies the implementation requirements for log and record managed objects. The profile specifies the ability to select which notifications, generated locally or remotely, are logged within the system. The criteria for the selection is specified as part of the log managed object. An agent system conforming to this profile needs to demonstrate the logging of notifications and the management of log and log record managed objects (retrieval of log records, for example). A manager system should be able to send and receive the required messages to manage the log managed object, and to retrieve log records.

Since not all of the management functions require the use of all the services offered by CMISE (i.e. systems that are designed to operate in manager-only or agent-only roles, or systems that need to support only a limited set of CMIP capabilities), each of the management function profiles specifies a subset of CMIP capabilities that is required to support the corresponding profile. This is done by referencing the appropriate tables in ISP 11183-2. It is important to note that if a product conforms to a management function profile it does not need to conform to a management communication profile (AOM1x profiles).

The profiles specify the requirements in terms of manager and agent roles. In this way interoperating systems in complimentary management roles conform to the same profile.

Profile	Title	ISP Parts
AOM231	General Log Control	DISP 12060-5
		DISP 12059-0
		DISP 12059-1
		DISP 12059-2
		DISP 12059-4
		DISP 12059-6
		ISP 11183-1
		ISP 11183-2

3.3   CMIP on TCP/IP

The network and system management environment will most certainly include multiple management and transport protocols. The telecom service provider environment will be largely based on ISO/CCITT protocols. A large company's Information Technology needs will likely require combinations of TCP/IP, Appletalk, Novell IPX, Microsoft Lan Manager, and legacy solutions, for example, SNA. As users combine elements of telecom and computing in their IT solutions, the single point management of multiple environments will become more important. Many companies have chosen an enterprise management strategy based on an ISO/CCITT backplane connected to various subnets which have different management protocols. One of the predominant transports used by IT departments for enterprise networking is TCP/IP.

The combination of ISO/CCITT management and a TCP/IP transport will help meet a portion of the enterprise management requirements. It specifically addresses the need for ISO management communication with another ISO manager or ISO agent across the Internet. OSF/DME has selected this configuration as one of those supported in the Network Management Option.

The requirement of ISO management combined with a prevalent transport infrastructure can best be satisfied by a configuration of CMIP with ISO upper layers and TCP/IP. The IETF OSI Internet Management Working Group developed several RFCs to address CMIS/CMIP for the Internet (CMOT). However, CMOT included use of a lightweight presentation protocol which had a significant disadvantage: it required modified, special-purpose presentation and session layers. Consequently, the CMOT RFCs (RFC 1189 and its predecessor RFC1095) have been deprecated (obsoleted) by the IETF.

The preferred configuration today combines the full ISO upper layers with TCP/IP. RFC 1006 defines the glue between ISO session layer and TCP. It specifies the primitives, protocol, and packet format such that TCP can meet the ISO transport service primitives. A standard ISO session layer can interface to RFC 1006 without modification. This is the configuration included in the OSF/DME Network Management Option. A key advantage of this configuration is that the end CMISE stacks will not require change if going through an intermediate TCP/IP network.
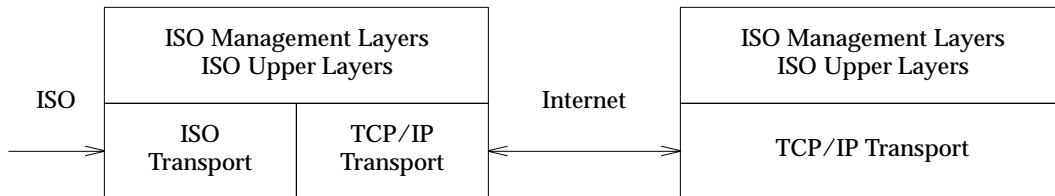

Figure 3-1 OSI Management on TCP/IP

Implementation of this configuration requires functionality specified in the following ISO and Internet documents:

	Title
ISO/CCITT Management Profiles	Any of the profiles in Section 3.1 or 3.2
Internet Lower Layers	RFC 1006 (TCP-ISO Transport Services) RFC 793 (TCP) RFC 791 (IP)

Simple Network Management Protocol

The Internet Protocol Suite (IPS) includes a Simple Network Management Protocol (SNMP). Implicit in th SNMP architectural model is a collection of management stations and network elements. Management stations execute management applications which monitor and control network elements. SNMP is used to communicate management information between management stations and agents in the network elements.

Implementations intended to provide SNMP within an Internet Protocol (IPS) environment shall conform to either or both of the following versions of SNMP.

4.1   SNMP Version 1

SNMP Version 1 is defined in RFC 1157. Implementation of this RFC requires functionality specified in the following Internet documents:

Application Layer	RFC 1157 (SNMPv1)
Transport Layer	RFC 793 (TCP), RFC 768 (UDP)
Network Layer	RFC 791 (IP)

4.2   SNMP Version 2

SNMP Version 2 is defined in RFC 1448. Transport mappings for SNMP Version 2 are defined in RFC 1449. Implementation of these RFCs require functionality specified in the following Internet documents:

Application Layer	RFC 1448 (SNMPv2)
Transport Layer	RFC 1449 (TP Mappings) RFC 768 (UDP) Other Options

where "Other Options" are specified in RFC1449 as follows:

- SNMPv2 over OSI Connectionless Transport Service (ISO 8072/AD 1)

- SNMPv2 over DDP (Appletalk)

- SNMPv2 over IPX (Novell)

Within the context of this CAE Specification these are options that may be provided. For systems implementing the SNMPv2 profile, support for UDP is mandatory.

Glossary

The following abbreviations appear in this document:

ACP
Association Control Protocol

ACSE
Association Control Service Element

AOM
Application: OSI management

CMIP
Common Management Information Protocol

CMIS
Common Management Information Service

CMOT
CMIP over TCP/IP (RFC 1189)

COPP
Connection Oriented Presentation Protocol

COPS
Connection Oriented Presentation Service

COSP
Connection Oriented Session Protocol

COSS
Connection Oriented Session Service

DIS
Draft International Standard

DISP
Draft International Standardised Profile

EFD
Event Forwarding Discriminator

FU
Functional Unit

IEC
International ElectroTechnical Commission

IEEE
Institute of Electrical and Electronics Engineers

IETF
Internet Engineering Task Force

IP
Internet Protocol

IPS
Internet Protocol Suite

IS
International Standard

ISO
International Organization for Standardization

ISP
International Standardised Profile

OSI
Open Systems Interconnect

RFC
Request For Comments

ROP
Remote Operations Protocol

ROSE
Remote Operations Service Element

RPC
Remote Procedure Call

SMAE
System Management Application Entity

SNMP
Simple Network Management Protocol

TCP
Internet Transmission Control Protocol

UDP
User Datagram protocol

XMP
X/Open Management Protocol API

XSM
X/Open Systems Management

Index