INTERNATIONAL STANDARD

ISO/IEC 10164-6

First edition
1993-11-01

Information technology — Open Systems Interconnection — Systems Management: Log control function

Technologies de l'information — Interconnexion de systèmes ouverts (OSI) — Gestion-système: Fonction de contrôle de journal

Reference number
ISO/IEC 10164-6:1993(E)

Contents

Foreword

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

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. 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.

International Standard ISO/IEC 10164-6 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Sub-Committee SC21, *Open Systems interconnection, data management and open distributed processing*, in collaboration with CCITT. The identical text is published as CCITT Recommendation X.735.

ISO/IEC 10164 consists of the following parts, under the general title *Information technology – Open Systems Interconnection – Systems Management*:

- *Part 1: Object management function*
- *Part 2: State management function*
- *Part 3: Attributes for representing relationships*
- *Part 4: Alarm reporting function*
- *Part 5: Event report management function*
- *Part 6: Log control function*
- *Part 7: Security alarm reporting function*
- *Part 8: Security audit trail function*
- *Part 9: Objects and attributes for access control*
- *Part 10: Accounting metering function*
- *Part 11: Workload monitoring function*
- *Part 12: Test management function*
- *Part 13: Summarization function*
- *Part 14: Confidence and diagnostic test categories*
- *Part 15: Scheduling function*

Annexes A and B of this International Standard are for information only.

Introduction

ISO/IEC 10164 is a multipart standard developed according to ISO 7498 and ISO/IEC 7498-4. ISO/IEC 10164 is related to the following International Standards

- ISO/IEC 9595:1991, *Information technology – Open Systems Interconnection – Common management information service definition*;
- ISO/IEC 9596-1:1991, *Information technology – Open Systems Interconnection – Common management information protocol – Part 1: Specification*;
- ISO/IEC 10040:1992, *Information technology – Open Systems Interconnection – Systems management overview*;
- ISO/IEC 10165:1992 *Information technology – Open Systems Interconnection – Structure of management information.*

This page intentionally left blank

INTERNATIONAL STANDARD

CCITT RECOMMENDATION

INFORMATION TECHNOLOGY – OPEN SYSTEMS INTERCONNECTION – SYSTEMS MANAGEMENT: LOG CONTROL FUNCTION

1 Scope

This Recommendation | International Standard defines a Systems Management Function which may be used by an application process in a centralized or decentralized management environment to interact for the purpose of systems management, as defined by CCITT Rec. X.700 | ISO/IEC 7498-4. This CCITT Recommendation | International Standard defines the Log Control function and consists of services and two functional units. This function is positioned in the application layer of the CCITT Rec. X.200 | ISO/IEC 7498-1 and is defined according to the model provided by ISO/IEC 9545. The role of systems management functions is described by CCITT Rec. X.701 | ISO/IEC 10040.

This CCITT Recommendation | International Standard

- establishes user requirements for the Log Control function;
- establishes models that relate the services provided by the function to user requirements;
- defines the services provided by the function;
- specifies the protocol that is necessary in order to provide the services;
- defines the relationship between the services and SMI operations and notifications;
- defines relationships with other systems management functions;
- specifies conformance requirements.

This CCITT Recommendation | International Standard does not

- define the nature of any implementation intended to provide the Log Control function;
- specify the manner in which management is accomplished by the user of the Log Control function;
- define the nature of any interactions which result in the use of the Log Control function;
- specify the services necessary for the establishment, normal and abnormal release of a management association;
- specify the authorization requirements for the use of the Log Control function or for any associated activity;
- define the definitions of managed objects related to the management of particular protocol machines.

2 Normative references

The following CCITT Recommendations and International Standards contain provisions which, through reference in this text, constitute provisions of this Recommendation | International Standard. At the time of publication, the editions indicated were valid. All Recommendations and Standards are subject to revision, and parties to agreements based on this Recommendation | International Standard are encouraged to investigate the possibility of applying the most recent editions of the Recommendations and Standards listed below. Members of IEC and ISO maintain registers of currently valid International Standards. The CCITT Secretariat maintains a list of currently valid CCITT Recommendations.

2.1 Identical Recommendations | International Standards

- CCITT Recommendation X.701 (1992) | ISO/IEC 10040:1992, *Information technology – Open Systems Interconnection – Systems management overview.*

- CCITT Recommendation X.721 (1992) | ISO/IEC 10165-2:1992, *Information technology – Open Systems Interconnection – Structure of management information – Part 2: Definition of management information.*

- CCITT Recommendation X.730 (1992) | ISO/IEC 10164-1:1993, *Information technology – Open Systems Interconnection – Systems Management – Part 1: Object management function.*

- CCITT Recommendation X.731 (1992) | ISO/IEC 10164-2:1993, *Information technology – Open Systems Interconnection – Systems Management – Part 2: State management function.*

- CCITT Recommendation X.733 (1992) | ISO/IEC 10164-4:1992, *Information technology – Open Systems Interconnection – Systems Management – Part 4: Alarm reporting function.*

- CCITT Recommendation X.734 (1992) | ISO/IEC 10164-5:1993, *Information technology – Open Systems Interconnection – Systems Management – Part 5: Event report management function.*

2.2 Paired Recommendations | International Standards equivalent in technical content

- CCITT Recommendation X.200 (1988), *Reference Model of Open Systems Interconnection for CCITT Applications.*

  ISO 7498:1984, *Information processing systems – Open Systems Interconnection – Basic Reference Model.*

- CCITT Recommendation X.210 (1988), *Open Systems Interconnection Layer Service Definition Conventions.*

  ISO/TR 8509:1987, *Information processing systems – Open Systems Interconnection – Service conventions.*

- CCITT Recommendation X.208 (1988), *Specification of Abstract Syntax Notation One (ASN.1).*

  ISO/IEC 8824:1990, *Information technology – Open Systems Interconnection – Specification of Abstract Syntax Notation One (ASN.1).*

- CCITT Recommendation X.209 (1988), *Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1).*

  ISO/IEC 8825:1990, *Information technology – Open Systems Interconnection – Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1).*

- CCITT Recommendation X.700 (1992), *Management Framework Definition for Open Systems Interconnection for CCITT Applications.*

  ISO/IEC 7498-4:1989, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 4: Management framework.*

- CCITT Recommendation X.710 (1991), *Common Management Information Service Definition for CCITT Applications.*

  ISO/IEC 9595:1991, *Information technology – Open Systems Interconnection – Common management information service defintion.*

- CCITT Recommendation X.290 (1992), *OSI Conformance Testing Methodology and Framework for protocol Recommendations for CCITT applications – General concepts.*

  ISO/IEC 9646-1:1991, *Information technology – Open Systems Interconnection – Conformance testing methodology and framework – Part 1: General concepts.*

2.3 Additional references

– ISO/IEC 9545:1989, *Information technology – Open Systems Interconnection – Application Layer structure.*

3 Definitions

For the purposes of this Recommendation | International Standard, the following definitions apply.

3.1 Basic reference model definitions

This Recommendation | International Standard makes use of the following term defined in Recommendation X.200 | ISO 7498.

systems management

3.2 Service convention definitions

This Recommendation | International Standard makes use of the following term defined in CCITT Rec. X.210 | ISO/TR 8509.

primitive

3.3 Management framework definitions

This Recommendation | International Standard makes use of the following terms defined in CCITT Rec. X.700 | ISO/IEC 7498-4.

a) management information;

b) managed object;

c) systems-management-application-entity.

3.4 Systems management overview definitions

This Recommendation | International Standard makes use of the following terms defined in CCITT Rec. X.701 | ISO/IEC 10040.

a) agent role;

b) dependent conformance;

c) general conformance;

d) manager role;

e) management application protocol;

f) management support object;

g) notification;

h) systems management operation;

i) systems management functional unit.

3.5 Event report management function definitions

This Recommendation | International Standard makes use of the following term defined in CCITT Rec. X.734 | ISO/IEC 10164-5.

discriminator input object

3.6 Common management information service definitions

This Recommendation | International Standard makes use of the following term defined in CCITT Rec. X.710 | ISO/IEC 9595.

attribute

3.7 OSI conformance testing definitions

This Recommendation | International Standard makes use of the following term defined in CCITT Rec. X.290 | ISO/IEC 9646-1.

system conformance statement

3.8 Additional definitions

3.8.1 **log:** A management support object class that models resources used as a repository for log records.

3.8.2 **log record:** A management support object class that models units of information stored in a log.

3.8.3 **potential log record:** A type of discriminator input object that is defined for the purpose of discriminating information to be included in the log. A potential log record consists of all information required for the inclusion of a log record in the log.

4 Abbreviations

ASN.1	Abstract Syntax Notation One
CMIS	Common management information service
CMISE	Common management information service element
Id	identifier
MAPDU	management application protocol data unit
PDU	Protocol data unit
SMAE	systems management application entity
SMFU	systems management functional unit
SMI	structure of management information

5 Conventions

This Recommendation | International Standard uses some of the descriptive conventions in the OSI Service Conventions in ISO/IEC TR 8509.

6 Requirements

For the purpose of many management functions it is necessary to be able to preserve information about events that may have occurred or operations that may have been performed by or on various objects. In a real open system various resources may be allocated to store such information. In OSI management these resources are modeled by **logs** and **log records** contained in the logs.

The management needs for the type of information that is to be logged may change from time to time. Furthermore, when such information is retrieved from a log the manager must be able to determine whether any records were lost or whether the characteristics of the records stored in the log where modified at any time.

The above needs give rise to the following requirements to be satisfied:

a) the definition of a flexible log control service which will allow selection of records that are to be logged by a management system in a particular log;

b) the ability for an external system to modify the criteria used in logging records;

c) the ability for an external system to determine whether the logging characteristics were modified or whether log records have been lost;

d) specification of a mechanism to control the time during which logging occurs, for example, by suspending and resuming logging;

e) the ability for an external system to retrieve and delete log records;

f) the ability for an external system to create and delete logs.

7 Model for the log control function

7.1 Introduction

The model for the log control function describes the conceptual components that provide for the logging of information in open systems. The model also describes the messages for the control of these components. Figure 1 is a schematic description of the logging capability of a system.

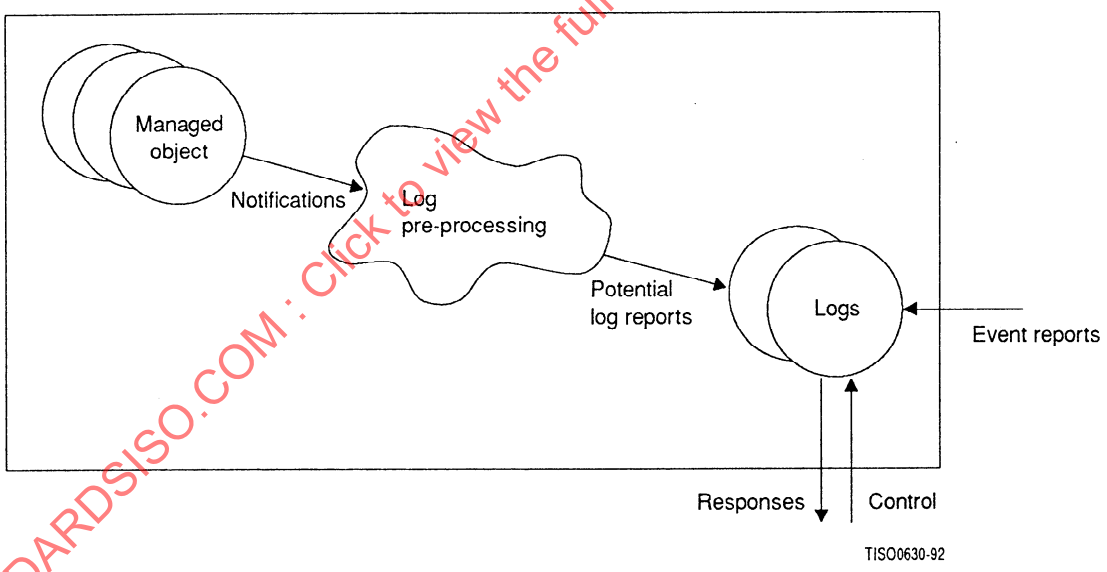

Figure 1 – Log management model

Conceptually, logs store incoming event reports and local system notifications. However, logs can be used to store information that is derived from notifications in the local open system, incoming event reports and PDUs received or transmitted by the open system. These three sources of information are modelled in two basic ways, so that conceptually the log only deals with event reports and local system notifications.

– The conceptual log preprocessing function receives notifications from managed objects within the local system and forms potential log records. Conceptually these potential log records are distributed to all logs that are contained within the local open system. A potential log record is perceived as a discriminator input object for the purpose of discrimination by the log only and is not visible outside the local system.

PDUs (other than systems management event reports) that are to be logged are modelled as giving rise to local system notifications that are processed as described above. The resource generating these PDUs must, therefore, be represented by a managed object. This results in treating PDUs exactly like local system notifications.

NOTE – It is the responsibility of the particular layer groups in defining managed objects that represent protocol entities to define which PDUs generate notifications and the parameters to be associated with that notification. In particular it is viewed that systems management application PDUs will give rise to notifications that may have to be logged.

To allow the logging of incoming PDUs in the log it is necessary to define a subclass of the log record managed object class that can contain the internal notifications and associated parameters.

- Systems management event reports, on the other hand, are not modelled as giving rise to notifications, but are presented directly to be processed for logging.

  Incoming event reports are conceptually distributed to all logs within the receiving open system.

The log in addition to conceptually storing the logged information determines which information is to be logged. Each log contains a discriminator construct which specifies the characteristics a potential log record or received event report must have in order to be selected for logging. Information that is selected for logging is supplemented with additional information generated as a part of the logging process (e.g. record identifiers and logging time). Each record has an identifier attribute value assigned on record creation. Values are assigned locally in ascending sequential order. The identifier attribute can, therefore, be used to determine the order of record creation in the log.

7.2 The log model

The log is a repository for **records**, and is the OSI abstraction of logging resources in real open systems. Records contain information that is logged.

The log managed object class is characterised by a mandatory package and several conditional packages; these packages provide the log with the following capabilities:

- the mandatory log package

  This package is characterised by the following:

  - **a log identifier,** uniquely identifying an instance of a log relative to its superior managed object;
  - an **Administrative state** and an **Operational state**, representing the state of the log;
  - a description of the type of information to be logged, this property is supported by the discriminator construct attribute;
  - the behaviour of the log when its maximum capacity is reached. This property is supported by the log full action attribute;
  - notifications generated when the log is created, deleted, suspended, resumed and modified. This property is supported by the object creation, object deletion, state change and attribute value change notifications of CCITT Rec. X.730 | ISO/IEC 10164-1 and CCITT Rec. X.731 | ISO/IEC 10164-2.

- the finite log size conditional package

  This package is characterised by the following:

  - a maximum log size (which may be indeterminate), this property is supported by the maximum log size attribute;
  - the current log size, supported by the current log size attribute;
  - the number of records currently in the log. Together with the current log size, this may be used to obtain an estimate of the average record size and, therefore, of the number of records that can still be logged. This property is supported by the number of records attribute.

- the scheduling conditional packages

  The log control function uses several conditional packages that provide various levels of sophistication in scheduling the activity of the log. These packages are characterised by the following:

  - the time during which logging is active, this property is supported by time-related attributes in the conditional packages that contain information related to scheduling.

- the log alarm conditional package

This package is characterised by the following:

– capacity alarm thresholds defined as percentages of the maximum log size. The capacity alarm thresholds are used to generate events that will indicate that various levels of the log full condition have been approached. This property is supported by the capacity alarm threshold attribute.

8 Generic definitions

This Recommendation | International Standard provides generic definitions of managed objects, attributes, and notifications associated with the log and log record managed objects.

8.1 Managed objects

8.1.1 The log managed object

8.1.1.1 Mandatory log package

The following mandatory attributes are defined for the log class.

8.1.1.1.1 Log Id

This attribute is used to uniquely identify the instance of a log.

8.1.1.1.2 Discriminator construct

This attribute specifies tests on the information that is to be logged. The discriminator construct may operate on any of the parameters of the information to be logged.

8.1.1.1.3 Administrative state

This attribute represents the administrative capability of the log to perform its function. The following Administrative states are defined:

a) **Unlocked** – Use of the log has been permitted by a managing system. Information from subordinate records may be retrieved and, conditional on the values of other state and status attributes, new records may be created;

b) **Locked** – Use of the log has been prohibited by a managing system. Information from subordinate records may be retrieved but new records shall not be created. Records may be deleted.

8.1.1.1.4 Operational state

This attribute represents the operational capability of the log to perform its function. The following Operational states are defined:

a) **Enabled** – The log is operational and is ready for use. Information from subordinate records may be retrieved and, conditional on the values of other state and status attributes, new records may be created;

b) **Disabled** – The log is not available for use. New records cannot be created.

8.1.1.1.5 Log full action

This attribute specifies the action to be taken when the maximum size of the log has been reached. Options are

a) **wrap** – The oldest records in the log, as determined by the log record identifier, will be deleted to free resources for the creation of new records;

b) **halt** – No more records will be logged. Records already in the log will be retained.

Both options shall be supported by any log.

8.1.1.1.6 Availability status

This attribute reflects the availability status of the managed object. The attribute may indicate a "log-full" condition; indicating that records can be retrieved but that no new records can be added.

8.1.1.2 Finite log size package

This package provides additional information regarding the current status of finite sized logs. It shall be present whenever supported by the underlying resource.

8.1.1.2.1 Max log size

This attribute specifies the size of the log measured in number of octets. A log may have an indeterminate size. A max log size of zero shall be used to specify that the log size has no predefined limit.

NOTE – Since the log size is specified in octets the actual amount of information that is contained in a log will be determined by data representation used in the log. This data representation is not subject to standardization. The maximum log size does not include the system overhead involved in establishing the log. Thus, immediately after creation the current log size should read zero.

8.1.1.2.2 Current log size

This attribute specifies the current size of the log measured in octets.

8.1.1.2.3 Number of records

This attribute specifies the current number of records contained in the log.

8.1.1.3 Log alarm package

This package provides for transmission of alarms when a log full condition approaches. This package shall be present whenever a log is of finite size and halts logging when the log full availability status occurs. This package contains the following attribute:

Capacity alarm threshold

This attribute specifies, as a percentage of max log size, the points at which an event will be generated to indicate that a log full or log wrap condition is approaching. This attribute is set-valued. Support of this attribute is mandatory for the halt behaviour. When a log is created with the **wrap** option the capacity threshold events are triggered as if coupled to a gauge that counts from zero to the highest capacity threshold value defined and then resets to zero.

8.1.1.4 Scheduling packages

Scheduling packages provide logs with the ability to automatically switch between their On-Duty and Off-Duty conditions.

To accommodate various levels of complexity in scheduling logging activity periods, conditional packages that are related to scheduling are defined for logging.

8.1.1.4.1 Availability status package

This conditional package shall be present if any of the other scheduling related packages are instantiated. This package contains the following attribute:

availability status

This attribute reflects the availability status of the managed object. When the resource has been made unavailable in accordance with a predetermined time schedule its value will be "Off-Duty". The attribute is read-only. The value on creation is determined by the scheduling parameters specified and the status of the resource. The required value set for this attribute in this package is "Off-Duty".

No state change notification is generated when this attribute changes value.

NOTE – The log makes use of the availability status to indicate the log-full condition; the presence of this conditional package makes available the "Off-Duty" value to the object.

8.1.1.4.2 Duration package

The duration package provides the ability to automatically control the time that a managed object starts and stops functioning through the use of the start time and stop time attributes.

a) Start time

This attribute defines the date and time at which an unlocked and enabled managed object starts functioning. If the value of the Start time attribute is not specified in the create request, its value defaults to the time of creation of the managed object and thus causing it to function immediately.

A change in the start time attribute results in an attribute change notification.

b) Stop time

This attribute defines the date and time at which a managed object stops functioning. If the value of the Stop time attribute is not specified in the create request, its value defaults to "continuous operation". Continuous operation is represented by a null value for the stop time.

A change in the stop time attribute results in an attribute change notification.

8.1.1.4.3 Daily scheduling package

The daily scheduling conditional package provides the capability of scheduling logging with a periodicity of 24 hours.

The scheduling attributes and their associated defaults, are defined below.

intervals of day

This attribute defines the list of time intervals (interval-start and interval-end times of day) for which the logs will exhibit the logging-on condition. During excluded intervals the log exhibits the logging-off condition. If not specified in the create request, the value of this component defaults to a single interval encompassing the entire 24 h period of a day.

8.1.1.4.4 Weekly scheduling package

The weekly scheduling conditional package provides the capability of scheduling logging with a periodicity of one week.

The scheduling attributes and their associated defaults, are defined below.

week mask

This structured attribute defines a set of mask components, each specifying a set of time intervals on a 24-hour time-of-day clock, pertaining to selected days of the week. The week mask attribute defaults to a scheduling criteria of "always on" at logs creation. The components of each mask are defined below.

a) Days of week

This component defines the days of the week on which the log's scheduling mechanism will allow the log to have intervals during which logging may occur. This component, if not present in a create, will default to all seven days of the week.

b) Intervals of day

This component defines the list of time intervals (interval-start and interval-end times of day) for which the log will exhibit the logging-on condition, if the current day is one of the days that is selected within the corresponding Days Of Week. During excluded intervals the log exhibits the logging-off condition. If not specified in the create request, the value of this component defaults to a single interval encompassing the entire 24 h period of a day.

8.1.1.4.5 External scheduler scheduling package

The external schedular scheduling conditional package provides the capability of scheduling logging based on a schedule defined in an external schedular managed object. The logs' logging-on and logging-off conditions will be changed in accordance with the scheduling characteristics specified by a schedular managed object.

The scheduling attribute is defined below

scheduler name

This attribute specifies the name of the scheduler managed object that is related to the logs. This relationship implies that the log's logging-on and logging-off conditions will be scheduled by the external scheduler. This attribute is read-only.

8.1.1.5 Normal operation of logs

The log's behaviour is determined by its state attributes, availability status, its discriminator construct, finite log size package, availability status package, log alarm package and its scheduling packages, if any.

The behaviour of a particular instance of the log is influenced by the conditional packages that were instantiates at the time it was created. The text below describes the way in which the log behaves when various conditional packages have been instantiated.

Whether or not a particular record is logged depends on the following characteristics of the log:

- the operational state;
- the availability status;
- the administrative state;
- the scheduling packages, if any; and
- the discriminator construct.

New log records will only be created, if the discriminator input object satisfies the conditions specified in the discriminator construct of the log and if the log is in the unlocked administrative state, is not in the disabled operational state, and has neither the log-full (for a log that halts), nor the off duty availability status. The off-duty availability status will only be supported by the log if one of the scheduling packages and the associated availability status package have been instantiated.

The administrative state of the log affects the creation of new records. When the log is in the "locked" state the log will not create new records however, records contained in the log are available for retrieval. When the log is in the "unlocked" state new records can be created unless the log is in the "disabled" operational state. Since log records are contained in logs, the operational state of the log affects operations that can be performed on log records. When the operational state of the log is disabled, records can not be retrieved.

Additionally, if the log is instantiated with a conditional scheduling package, the log will not create any new records if the log has the off-duty availability status.

The operational state of the log and the availability status cannot be changed by direct management action, but reflect the internal activity of the log and its scheduling packages, if any.

For the behaviour of the log when the maximum log size has been reached (known as the **log full** availability status) two options have been defined. The log may either **halt** logging or the log may **wrap**. A log that halts upon reaching the log full condition will always generate a capacity alarm threshold notification that indicates that this condition has been reached, and shall therefore, include the log alarm package. The behaviour of such a log corresponds to a log that discards the most recent information in preference to older information.

A log that wraps upon reaching the log full condition will discard an integral number of records when it reaches that condition in order to log new records. The behaviour of such a log corresponds to a log that discards old information in preference to new information.

8.1.1.6 Management of logs

In general, all non-status attribute values may be modified, though restrictions may exist. For example, the max log size attribute may not be modified to a value less than the value of the Current log size attribute. Additionally, in some systems, attempts to increase or decrease the value of the max log size attribute after creation may fail. The Log Id attribute value is not settable.

The values of the availability status, Operational state, current log size, and number of records, reflect the operation of the log and may not be modified directly by the manager.

Whenever a settable non-state attribute is modified an attribute change notification may be generated. All log attributes except the number of records and current log size attributes shall generate such notifications. The latter attribute changes are not coupled to a notification since they are expected to change frequently in response to normal operation of the log.

The log administrative state may be changed by use of a set operation. Whenever the administrative state of a log is changed a state change notification is generated. A change in operational state shall generate a state change notification.

8.1.2 Log records

Log records are managed objects that represent information stored in logs. The log record managed object class serves as a superclass for other record classes. As a part of the specialisation of the log record class additional attributes may be assigned to the new subclass.

The log record class has the following properties:

- **a log record identifier;**
- **a logging time.**

8.1.2.1 Log record behaviour

Log records are created as a result of the receipt of an event report or notifications, they are not created by explicit management operations. Log records may only be retrieved and deleted; attributes of a log record cannot be modified.

The operations that can be performed on a log record depend on the state of the log in which the records are contained and may also be subject to security constraints.

8.1.2.2 Log record attributes

The following mandatory attributes are defined for the log record class:

8.1.2.2.1 Log record Id

This attribute uniquely identifies each record in the log. The log record identifier is a number that is unique within the scope of the log and is assigned sequentially. The identification number used may wrap; however, at no time shall there be more than one record with the same identifier in the log. The logRecordId has the syntax of an integer.

8.1.2.2.2 Logging time

This attribute identifies the time at which the record was entered into the log. In the absence of time synchronization this time may be greater or less than the source time (if specified).

8.2 Imported generic definitions

This Recommendation | International Standard makes use of the following generic definitions in CCITT Rec. X.730 | ISO/IEC 10164-1, CCITT Rec. X.731 | ISO/IEC 10164-2 and CCITT Rec. X.733 | ISO/IEC 10164-4.

- attribute value change notification;
- state change notification;
- processing error alarm notification;
- object creation notification;
- object deletion notification.

The attribute value change notification and the state change notification are used to report changes in the non-state attribute values and states of the log, respectively.

The log also generates events indicating that a capacity threshold has been reached or exceeded. For a log that is configured to halt upon reaching a log-full condition an event indicating that this condition has occurred (i.e. a current log size of 100% has been reached) shall always be generated. For a log that is configured to halt, the event indicating a log-full condition shall be generated at latest when the first new record had to be discarded because of a lack of storage capacity. The event may be generated before this if it is known that there are insufficient resources to create additional records. For a log that is configured to wrap, all capacity threshold alarms are optional.

In reporting the capacity threshold event, use is made of the alarm report defined in CCITT Rec. X.733 | ISO/IEC 10164-4. Only the following parameters of the alarm report shall be used and all parameters are mandatory when used for reporting log capacity threshold alarms.

Managed Object Class	This parameter shall identify the log class.
Managed Object Instance	This parameter shall identify the instance of the log that generated the event.
Alarm Type	This parameter shall indicate that a **processing error alarm** has occurred.
Event Time	This parameter carries the time at which the capacity threshold event occurred.
Perceived Severity	This parameter will indicate the severity assigned to the capacity threshold event. When the 100% log full condition is reached a severity value of critical shall be assigned to this event.
Monitored Attributes	This parameter shall carry the maximum log size attribute of the log.
Probable Cause	This parameter shall carry the value **storage capacity problem.**
Threshold Info	This parameter shall carry the capacity threshold value (as percentage of total capacity) that was reached or exceeded in generating this event.

9 Service definition

This Recommendation | International Standard does not define any services. The use of services defined in other functions is described below.

9.1 Introduction

The information needs and management control requirements between systems may change with time and changes in the management or communications environment. It is, therefore, necessary to provide a mechanism for administering OSI management services.

It is considered that a manager should have the capability of modifying the operation of a log in a remote system. In particular, the operations required, that can be applied to each instance of a log, are

- creation of a log;
- deletion of a log;
- modification of log attributes;
- suspension of the activity of the log;
- deletion and retrieval of log records; and
- resumption of the log activity.

These operations will thus provide a means for a system to initiate, terminate, suspend, resume and modify the logging capability.

9.2 Initiation of logging

The PT-CREATE service defined in CCITT Rec.X.730 | ISO/IEC 10164-1 is used to allow one open system to request that another open system create a log, thereby requesting that new or additional logs be defined.

The semantics of the log attributes are defined in 7.1.2. The following describes the values that will be assigned to log attributes in response to a PT-CREATE request and the required response.

Max log size: This attribute specifies the size of the log to be created. When this attribute is absent then either a log of indeterminate size is created or a system defined default size may be assigned. When this parameter is absent in the indication it shall be returned in the response.

Capacity alarm threshold: This attribute specifies capacity levels at which an alarm notification will be generated. For a log that has a log full action of "halt", this attribute is mandatory and if not specified a single threshold set at 100% will be assumed.

Log full action: This attribute specifies the action to be taken when the maximum capacity of the log is reached. If this parameter is not specified "wrap" is assumed.

Discriminator construct: This attribute specifies the test conditions which will be used by the log in testing potential log records. If no value is specified for this parameter in the incoming request then an empty discriminator construct will be defined.

Administrative state: This attribute specifies the administrative state in which the log is to be created. The log may be created in a Unlocked or Locked state. If no administrative state is specified, the Unlocked state is assumed.

Operational state: This attribute specifies the operational state of the log. The operational state shall not be specified as part of the create request, but shall be returned in the response and will reflect the actual state of the created log.

Availability status: This attribute specifies the availability status of the log. The availability status shall not be specified as part of the create request, but shall be returned in the response and will reflect the actual status of the created log.

Packages: This attribute specifies the conditional packages to be included in the managed object to be created. If no packages are specified, no scheduling is assumed to be requested.

9.3 Termination of logging

The PT-DELETE service defined in CCITT Rec. X.730 | ISO/IEC 10164-1 is used to allow one open system to request that another open system delete one or more logs.

9.4 Modification of logging attributes and suspension and resumption of logging

The PT-SET service defined in CCITT Rec. X.730 | ISO/IEC 10164-1 is used to allow one open system to request that another open system change the administrative state of the log or set the value of a settable attribute. When the state is changed to locked, logging of records will be suspended; when the state is changed to unlocked, logging may be resumed.

9.5 Retrieving logging attributes

The PT-GET service defined in CCITT Rec. X.730 | ISO/IEC 10164-1 may be used to retrieve any of the readable attributes of the log. All attributes of the log are readable.

9.6 Retrieval of log records

Log records may be retrieved from a log by means of the PT-GET service. If a scoped and filtered PT-GET service is used multiple log records can be retrieved with one request.

9.7 Deletion of log records

Log records may be deleted from a log by means of the PT-DELETE service. If a scoped and filtered PT-DELETE service is used, multiple log records can be deleted with one request.

10 Functional units

Two functional units are defined in this Recommendation | International Standard for the management of logs:

a) log control functional unit;

b) monitor log functional unit.

The monitor log functional unit requires the support of PT-GET services for instances of the log and log record or any of their subclasses. The log control functional unit requires the support of PT-GET and PT-DELETE for instances of the log and log record or any of their subclasses, and requires the support of PT-SET, PT-CREATE, object creation reporting, object deletion reporting, attribute value change reporting, state change reporting and the alarm reporting services for instances of the log or any of its subclasses.