International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

M.3705

(03/2013)

SERIES M: TELECOMMUNICATION MANAGEMENT, INCLUDING TMN AND NETWORK MAINTENANCE

Integrated services digital networks

Common management services – Log management – Protocol neutral requirements and analysis

Recommendation ITU-T M.3705

ITU-T M-SERIES RECOMMENDATIONS

TELECOMMUNICATION MANAGEMENT, INCLUDING TMN AND NETWORK MAINTENANCE

Introduction and general principles of maintenance and maintenance organization	M.10–M.299
International transmission systems	M.300–M.559
International telephone circuits	M.560–M.759
Common channel signalling systems	M.760–M.799
International telegraph systems and phototelegraph transmission	M.800–M.899
International leased group and supergroup links	M.900–M.999
International leased circuits	M.1000–M.1099
Mobile telecommunication systems and services	M.1100–M.1199
International public telephone network	M.1200–M.1299
International data transmission systems	M.1300–M.1399
Designations and information exchange	M.1400–M.1999
International transport network	M.2000–M.2999
Telecommunications management network	M.3000–M.3599
Integrated services digital networks	**M.3600–M.3999**
Common channel signalling systems	M.4000–M.4999

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T M.3705

Common management services – Log management – Protocol neutral requirements and analysis

Summary

Recommendation ITU-T M.3705 provides the requirements and analysis for one of the common management services – log management. This Recommendation is a rewrite of Recommendation ITU-T X.735 under the new methodology specified in Recommendation ITU-T M.3020 to provide a protocol neutral information model for log management.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T M.3705	2013-03-16	2

Keywords

Common management service, log management.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T M.3705

Common management services – Log management – Protocol neutral requirements and analysis

1 Scope

This Recommendation defines the requirements for basic log management which includes the following: specify what to log, start/suspend/resume/stop logging, retrieve log records, and generate an alarm when encountering certain logging problems. The technique-specific and device-specific event and message logging will be derived from this Recommendation, and the generic logging management objects, attributes and operations will be reused.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T M.3020] Recommendation ITU-T M.3020 (2011), *Management interface specification methodology*.

[ITU-T M.3160] Recommendation ITU-T M.3160 (2008), *Generic, protocol-neutral management information model*.

[ITU-T M.3700] Recommendation ITU-T M.3700 (2010), *Common management services – Object management – Protocol neutral requirements and analysis.*

[ITU-T M.3701] Recommendation ITU-T M.3701 (2010), *Common management services – State management – Protocol neutral requirements and analysis*.

[ITU-T M.3702] Recommendation ITU-T M.3702 (2010), *Common management services – Notification management – Protocol neutral requirements and analysis.*

[ITU-T M.3703] Recommendation ITU-T M.3703 (2010), *Common management services – Alarm management – Protocol neutral requirements and analysis*.

[ITU-T X.680] Recommendation ITU-T X.680 (2008) | ISO/IEC 8824-1:2008, *Information Technology – Abstract Syntax Notation One (ASN.1) – Specification of basic notation*.

[ITU-T X.701] Recommendation ITU-T X.701 (1997) | ISO/IEC 10040:1998, *Information technology – Open Systems Interconnection – Systems management overview*.

[ITU-T X.735] Recommendation ITU-T X.735 (1992) | ISO/IEC 10164-6:1993, *Information Technology – Open Systems Interconnection – Systems Management: Log control function.*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following term defined elsewhere:

3.1.1 notification [ITU-T X.701].

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 notification log: A managed resource in which notifications are stored. Notification logs contain notification log records. A notification log may represent a physical or a logical/virtual storage, which may not be visible to a manager.

3.2.2 notification log record: A notification log record records track information about when a particular notification entered the notification log and the details of the notification. Each notification log record is associated with one notification.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CORBA Common Object Request Broker Architecture

DN Distinguished Name

EMS Element Management System

IOC Information Object Class

IRP Integration Reference Point

NE Network Element

NL Notification Log

NM Network Manager

NMS Network Management System

NR Network Resource

OS Operations System

UML Unified Modelling Language

XML extensible Markup Language

5 Conventions

This Recommendation uses the conventions defined in [ITU-T M.3020] for requirements capture and analysis.

6 Requirements

A general-purpose notification logging mechanism is required to hold notifications related to different functional areas in the network.

This service uses the following services and thus implicitly imports all the requirements defined therein:

- Notification management [ITU-T M.3702]
- State management [ITU-T M.3701]

In addition, the following specific requirements apply for log management as specified in this and subsequent clauses.

6.1 Business level requirements

6.1.1 List of requirements

6.1.1.1 General requirements

Identifier	Definition
REQ-LM-FUN-01	Any notification log must be capable of storing all data related to any type of notification (i.e., any class which extends Notification as defined in [ITU-T M.3702]).
REQ-LM-FUN-02	The notification log control service will allow the selection of notification log records that are to be logged by a management system (NMS or EMS) in a new notification log or a particular existing notification log.
REQ-LM-FUN-03	It will be possible to start and stop logging to a specific notification log or all notification logs.
REQ-LM-FUN-04	The ability for a client system to modify the criteria used in logging notification records.
REQ-LM-FUN-05	Specification of a mechanism to enable notification logging to be suspended and subsequently to be resumed.
REQ-LM-FUN-06	The ability for a client system to retrieve and delete notification log records.
REQ-LM-FUN-07	The ability for a client system to create and delete those notification logs.
REQ-LM-FUN-08	The ability to log partial notifications.
REQ-LM-FUN-09	The manager may request a list of all log activities currently managed by the agent. The agent returns a list of notification log identifiers to the manager. The manager may then use these identifiers to query a log or parts of it.
REQ-LM-FUN-10	The agent will assign a unique identifier to each notification log whether created autonomously by the agent or on the request of a manager.
REQ-LM-FUN-11	All notifications available at the agent for potential transmission shall be logged if requested by a start log request, irrespective of the notification subscriptions and filter settings.
REQ-LM-FUN-12	The notification log record will contain a notification as specified by [ITU-T M.3702].
REQ-LM-FUN-13	The notification log record is time-stamped, allowing the operator to determine the time at which the notification log record was added to the notification log.
REQ-LM-FUN-14	The agent should avoid the logging of notifications resulting from asynchronous alarm synchronization.

6.1.1.2 Status of the notification log state

Identifier	Definition
REQ-LM-FUN-15	The ability for a client system to determine whether the logging characteristics were modified or whether any notification log records have been lost.
REQ-LM-FUN-16	The notification log management system must notify all interested OS about its current state. An event-based approach is used to update OS on the current state of the notification log. To facilitate the notification of attribute or state changes, a notification log has the capability to generate such events according to the object management functions defined in [ITU-T M.3700].
REQ-LM-FUN-17	The notification log management system may also emit notification log creation and log deletion notifications to signal the creation or deletion of a particular log according to the object management functions defined in [ITU-T M.3700].

Identifier	Definition
REQ-LM-FUN-18	To notify OSs about the loss or imminent loss of notification log records, the system is able to emit capacity threshold alarms as defined in [ITU-T M.3703] that alert the subscribed OSs that a capacity threshold has been crossed in a particular notification log. This threshold value may indicate that the notification log is full and incoming notifications shall be dealt with in a predetermined manner set by an operator.
REQ-LM-FUN-19	The system may emit other events to notify an OS of the completion of an I/O intensive operation, such as the deletion of notification log records.

6.1.1.3 Notification log/notification log record retrieval

Identifier	Definition
REQ-LM-FUN-20	An OS may retrieve notification log records by querying a particular notification log with a filter.

The ability of an OS to export some subsets of notification logs maintained by itself to the W3C XML log format is for further study.

6.1.1.4 Notification log full action

Identifier	Definition
REQ-LM-FUN-21	The OS must be able to set the behaviour of a notification log when it becomes full. Two actions are recommended, halt and wrap: – A notification log that halts when full implies the agent should notify the OS by way of generating a capacity threshold alarm. New notifications, which should be logged according to the notification log's filter criteria, are discarded. This behaviour implies that the old notification log records are more important than new ones. – An OS can set the behaviour of the notification log to wrap when full. In this case the notification log behaves like a circular buffer, replacing the oldest notification log records with new ones. This behaviour implies that new notification log records are more important than old notification log records.

6.1.2 Actor roles

The capabilities described in this Recommendation are available and relevant to all agents and managers.

6.1.3 Telecommunication resources

The log management functionality is applicable to all types of telecommunication resources.

6.1.4 High level use case diagrams

The first overview use-case diagram in Figure 1 shows the overall interaction of the Notification log management function.

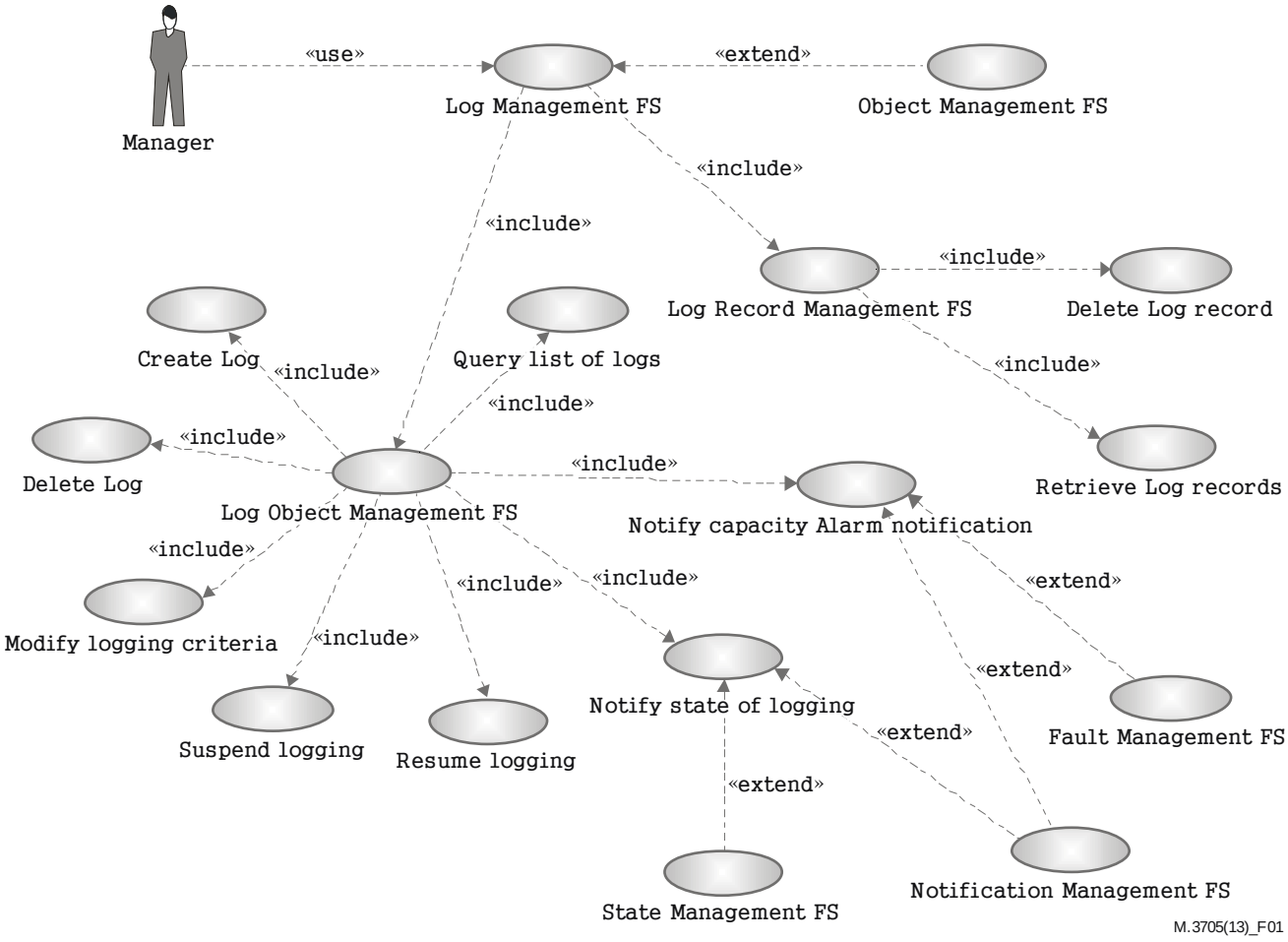

Figure 1 – Log management function set

6.1.4.1 Use case: modify logging criteria

Use case stage	Evolution/Specification	<<Uses>> Related use
Goal	The manager needs to change the attribute values of a log in the agent, such as the filtering criteria of event logging, the log full action, the capacity alarm threshold, and so on. The manager modifies the attribute values of a log through the management interface.	
Actor and roles	The manager invokes operations on the agent.	
Assumptions	The communication between manager and agent is available. The agent supports the function of modifying a log.	
Pre-conditions	The specified log exists in the agent and it is suspended.	
Begins when	The manager sends the request to the agent.	
Step 1	The manager sends a request to the agent to modify the attribute values of a log. The input parameters are the attribute names to be modified and the corresponding new values. The attributes that can be modified include: max log size, log full action,	

Use case stage	Evolution/Specification	<<Uses>> Related use
	capacity alarm threshold, and filtering criteria.	
Step 2.1	The agent updates the specific log with a new attribute value; if the modification succeeds, the log will use new criteria to record events and act according to these new attribute values.	
Step 2.2	If the modification fails, the agent will return an exception.	
Ends when	The agent has finished the update on the log.	
Exceptions	Invalid parameter Log not suspended Agent processing error Communication error	
Post-conditions	The log is modified by the agent on the request of the manager. The agent may send the corresponding attribute value change notification to the manager. The newly modified log then begins to record events with the new criteria and behaves according to the new attribute values.	
Traceability	REQ-LM-FUN-01, REQ-LM-FUN-03, REQ-LM-FUN-04	

6.1.4.2 Use case: suspend logging

Use case stage	Evolution/Specification	<<Uses>> Related use
Goal	The manager temporarily needs to suspend a log-in agent. The manager temporarily does not want the log to record event information in the agent, or the manager needs to change the attribute values of the log object. The manager can suspend a log through the management interface. Thereafter, the log will not record any events until it has resumed.	
Actor and roles	The manager invokes operations on the agent.	
Assumptions	The communication between the manager and the agent is available. The agent supports the function of suspending a log.	
Pre-conditions	The specified log exists in the agent and it is not suspended.	
Begins when	The manager sends a request to suspend the log.	
Step 1	In this use case, the manager sends a request to the agent to suspend a log, that is, to set the administrative state of the log object from "unlocked" to "locked".	
Step 2	The agent updates the administrative state value. If the operation succeeds, the log object will not record any events until it has resumed. If the operation fails, Agent will return an exception.	

Use case stage	Evolution/Specification	<<Uses>> Related use
Ends when	The agent suspends the log and a state change notification is sent.	
Exceptions	Log already suspended; agent processing error; communication error.	
Post-conditions	The log is suspended by the agent on the request of the manager. The agent may send the corresponding state change notification to the manager, and the log does not record any events until it has resumed.	
Traceability	REQ-LM-FUN-05	

6.1.4.3 Use case: resume logging

Use case stage	Evolution/Specification	<<Uses>> Related use
Goal	The manager can resume a suspended log through the management interface, so that the log can record events again.	
Actor and roles	The manager invokes operations on the agent.	
Assumptions	The communication between the manager and the agent is available. The agent supports the function of resuming a log.	
Pre-conditions	The specified log exists in the agent and it is suspended.	
Begins when	The manager sends the request to the agent.	
Step 1	In this use case, the manager sends a request to the agent to resume a suspended log, that is, to set the administrative state of the log object from "locked" to "unlocked".	
Step 2	The agent updates the administrative state of the log. If the operation succeeds, the log object will begin to record events again. If the operation fails, the agent will return an exception.	
Ends when	The agent has finished updating the log and continues logging.	
Exceptions	Log not suspended Agent processing error Communication error	
Post-conditions	The log is resumed by the agent on the request of the manager. The agent may send the corresponding state change notification to the manager. The log continues to record events according to its filtering criteria.	
Traceability	REQ-LM-FUN-05	

6.1.4.4 Use case: create log

Use case stage	Evolution/Specification	<<Uses>> Related use
Goal	The manager needs the agent to log event information so that the information may be queried in the future for some specific situations such as data loss. The manager creates a log through the management interface.	
Actor and roles	The manager invokes operations on the agent.	
Assumptions	The communication between the manager and the agent is available. The agent supports the function of creating a log. In the case that the agent can initialize a log instance(s) by itself, it is not required to provide this function in the interface.	
Pre-conditions		
Begins when	The manager sends the request to the agent.	
Step 1	The manager requests the agent creates a log. The parameters in the request include the initial administrative state, max log size, log full action, capacity alarm threshold, and filtering criteria of the log object.	
Step 2	The agent creates a log object using given parameters. If the log has been created successfully, the agent will then return the identifier of the log and send an object creation notification to the manager. Whether events will be recorded as log records, depends on the filtering criteria defined in the log. If the creation fails, the agent will return an exception.	
Ends when	Log object is created and the object create notification is sent.	
Exceptions	Invalid parameter Agent processing error Communication error	
Post-conditions	The log is created by the agent on the request of the manager. The agent returns the identifier of the log and may send the corresponding object creation notification to the manager. The events will be recorded according to the filtering criteria in the newly created log.	
Traceability	REQ-LM-FUN-02, REQ-LM-FUN-03, REQ-LM-FUN-06, REQ-LM-FUN-07, REQ-LM-FUN-10	

6.1.4.5 Use case: delete log

Use case stage	Evolution/Specification	<<Uses>> Related use
Goal	The manager does not need the log in the agent to record any event information. The manager deletes a log through the management interface. In the case that the agent system can initialize a log instance(s), it is not required to provide this function in the interface.	
Actor and roles	The manager invokes operations on the agent.	
Assumptions	The communication between the manager and the agent is available. The agent supports the function of deleting a log.	
Pre-conditions	The specified log exists in the agent and it is suspended.	
Begins when	The manager sends the request to the agent.	
Step 1	The manager requests the agent deletes a log. The parameter in the request is the ID of the log object.	
Step 2	The agent deletes the specific log object. If the log has been deleted successfully, the agent may then send the corresponding object deletion notification to the manager. If the deletion fails, the agent will return an exception.	
Ends when	The log is deleted and an object delete notification is sent.	
Exceptions	Unknown log Log not suspended Agent processing error Communication error	
Post-conditions	The log and the associated log records are deleted by the agent on the request of the manager. The agent may send the corresponding object deletion notification to the manager.	
Traceability	REQ-LM-FUN-06, REQ-LM-FUN-07	

6.1.4.6 Use case: query list of logs

Use case stage	Evolution/Specification	<<Uses>> Related use
Goal	The manager may query the attribute values of a log, including administrative state, operational state, max log size, current log size, log full action, number of records, alarm status, capacity alarm threshold, filtering criteria, and so on. The manager queries a specific log or all log objects in the agent.	
Actor and roles	The manager invokes operations on the agent.	

Use case stage	Evolution/Specification	<<Uses>> Related use
Assumptions	The communication between the manager and the agent is available. The agent supports the function of querying a log.	
Pre-conditions	The specified log exists in the agent.	
Begins when	The manager sends the request to the agent.	
Step 1	The manager sends a request to query a log. The parameters in the request are the specific object name of the log to be queried and the attribute names to be queried.	
Step 2	If the operation succeeds, the agent will return the corresponding attribute values. Otherwise, the agent will return an exception.	
Ends when	The query response is sent.	
Exceptions	Invalid parameter Agent processing error Communication error	
Post-conditions	The agent returns the attribute values of the log requested by the manager.	
Traceability	REQ-LM-FUN-09	

6.1.4.7 Use case: notify state of logging

Use case stage	Evolution/Specification	<<Uses>> Related use
Goal	The manager may want to know the latest logging state. The agent will notify the manager when the logging state has changed.	
Actor and roles	The agent notifies the manager.	
Assumptions	The communication between the manager and the agent is available. The manager has subscribed to this kind of notifications. See [ITU-T M.3702]	
Pre-conditions	The notification service defined in [ITU-T M.3702] is supported.	
Begins when	The value of the state attributes defined in [ITU-T M.3700] has changed, including administrativeState, operationalState, availabilityStatus, loggingState.	
Step 1	The agent constructs a state Change Notification as defined in [ITU-T M.3700], the content will include the changed state attributes and values.	
Step 2	The agent sends the notification to the manager, following the notification service rule in [ITU-T M.3702].	
Step 3	The notification will also be logged if it satisfies the logging criteria.	
Ends when	The notification is logged if it satisfies the logging criteria.	

Use case stage	Evolution/Specification	<<Uses>> Related use
Exceptions	Invalid parameter Agent processing error Communication error	
Post-conditions	A new notification log record is generated if the notification satisfies the logging criteria.	
Traceability	REQ-LM-FUN-16	

6.1.4.8 Use case: retrieve log records

Use case stage	Evolution/Specification	<<Uses>> Related use
Goal	In the case that the notification information between the manager and the agent is not synchronized due to broken communication, abnormal data, lost data or other reasons, the manager needs to query log records in the agent to synchronize the notification information between two systems. The manager queries the log records contained in a log according to certain criteria.	
Actor and roles	The manager invokes operations on the agent.	
Assumptions	The communication between the manager and the agent is available. The agent supports the function of querying log records.	
Pre-conditions	The specified log exists in the agent.	
Begins when	The manager sends the request to the agent.	
Step 1	The manager sends a "query log record" request to the agent. The parameters in the request are the filtering criteria and the time boundary.	
Step 2	If the query succeeds, the agent will return the log records that satisfy the criteria and the time boundary. Otherwise, if the query fails, the agent will return an exception.	
Ends when	The agent response with the log records according to the query condition.	
Exceptions	Invalid parameter No such log records Agent processing error Communication error	
Post-conditions	The corresponding log records are returned by the agent.	
Traceability	REQ-LM-FUN-20	

6.1.4.9 Use case: delete log record

Use case stage	Evolution/Specification	<<Uses>> Related use
Goal	In the case where the information in some log records is of no use to the manager (too old or having been transferred to the manager), the manager can delete some or all log records in the agent. The manager deletes log records contained in a log according to certain criteria.	
Actor and roles	The manager invokes operations on the agent.	
Assumptions	The communication between the manager and the agent is available. The agent supports the function of deleting log records.	
Pre-conditions	The specified log exists in the agent.	
Begins when	The manager sends the request to the agent.	
Step 1	The manager sends a deletion request to the agent. The parameters in the request are the filtering criteria and the time boundary.	
Step 2	The agent will find out and delete the corresponding records that satisfy the criteria and the time boundary. If the deletion fails, the agent will return an exception.	
Ends when	Log records are successfully deleted.	
Exceptions	Invalid parameter No such log records Agent processing error Communication error	
Post-conditions	The log records that satisfy the filtering criteria and the time boundary are deleted.	
Traceability	REQ-LM-FUN-06	

6.1.4.10 Use case: notify capacity alarm notification

Use case stage	Evolution/Specification	<<Uses>> Related use
Goal	In case the number of log records has reached the threshold of log record capacity, the agent will send an alarm notification to notify the manager.	
Actor and roles	The agent will send an alarm notification to the manager.	
Assumptions	The communication between the manager and the agent is available. The manager had subscribed to such a notification. See [ITU-T M.3702]	
Pre-conditions	The notification service defined in [ITU-T M.3702] is supported. The alarm service defined in [ITU-T M.3703] is supported.	

Use case stage	Evolution/Specification	<<Uses>> Related use
Begins when	The number of log records reaches the threshold of log record capacity.	
Step 1	The agent automatically maintains the number of log records. It will detect: If the number of log records increases above the threshold of log record capacity, go to step 2. If the number of log records decreases beneath the threshold of log record capacity, go to step 3.	
Step 2	The agent will construct the alarm information data (see clause 7.2.3.1 of [ITU-T M.3703]) with the probable cause set to Log Capacity and alarmType set to QoS Alarm. Follow the alarm reporting use case in clause 6.3.4.2 of [ITU-T M.3703]. Go to step 4.	
Step 3	The agent will construct the alarm information data (see clause 7.2.3.1 of [ITU-T M.3703]) with the probable cause set to Log Capacity and alarmType set to QoS Alarm. Follow the alarm clear use case in clause 6.3.4.4 of [ITU-T M.3703].	
Step 4	The notification will also be logged if it satisfies the logging criteria.	
Ends when	The notification has been sent.	
Exceptions	Agent processing error Communication error	
Post-conditions	A new notification log record is generated if the notification satisfies the logging criteria.	
Traceability	REQ-LM-FUN-18	

7 Analysis

According to [ITU-T M.3020], the "Analysis" phase will include information object class definitions and interface definitions.

7.1 Concepts and background

The log management service makes use of the following common management services as shown in the two diagrams below.

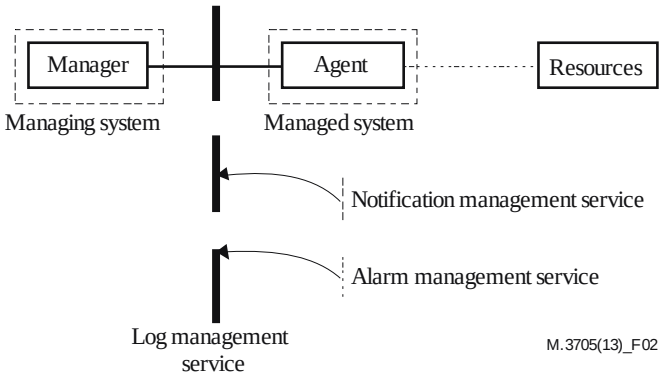

Figure 2 – System context

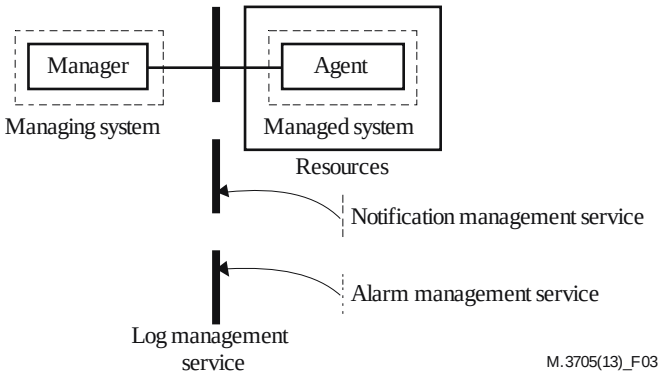

Figure 3 – System context B

7.2 Information object classes

7.2.1 Information entities imported and local labels

Label reference	Local label
[ITU-T M.3160], information object class, Top	Top
[ITU-T M.3160], information object class, Network	Network

7.2.2 Class diagram

7.2.2.1 Attributes and relationships

This clause introduces the set of information object classes (IOCs) that encapsulate information within the agent. The intent is to identify the information required for operations and notification. This clause provides the overview of all support object classes in UML. Subsequent clauses provide more detailed specifications of the various aspects of these support object classes.

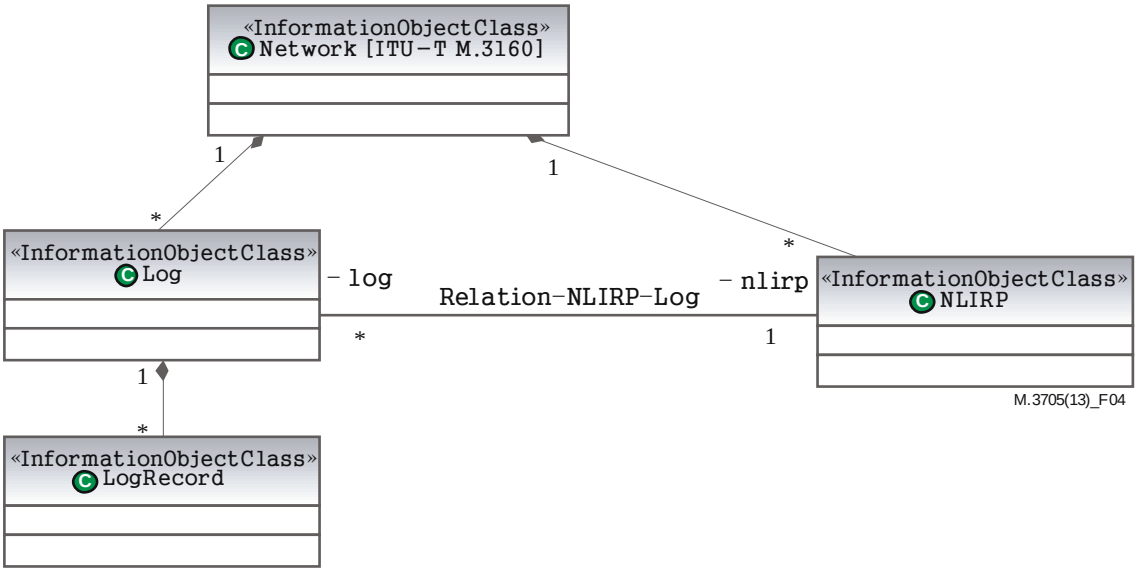

Figure 4 – Information object class relationships

7.2.2.2 Inheritance

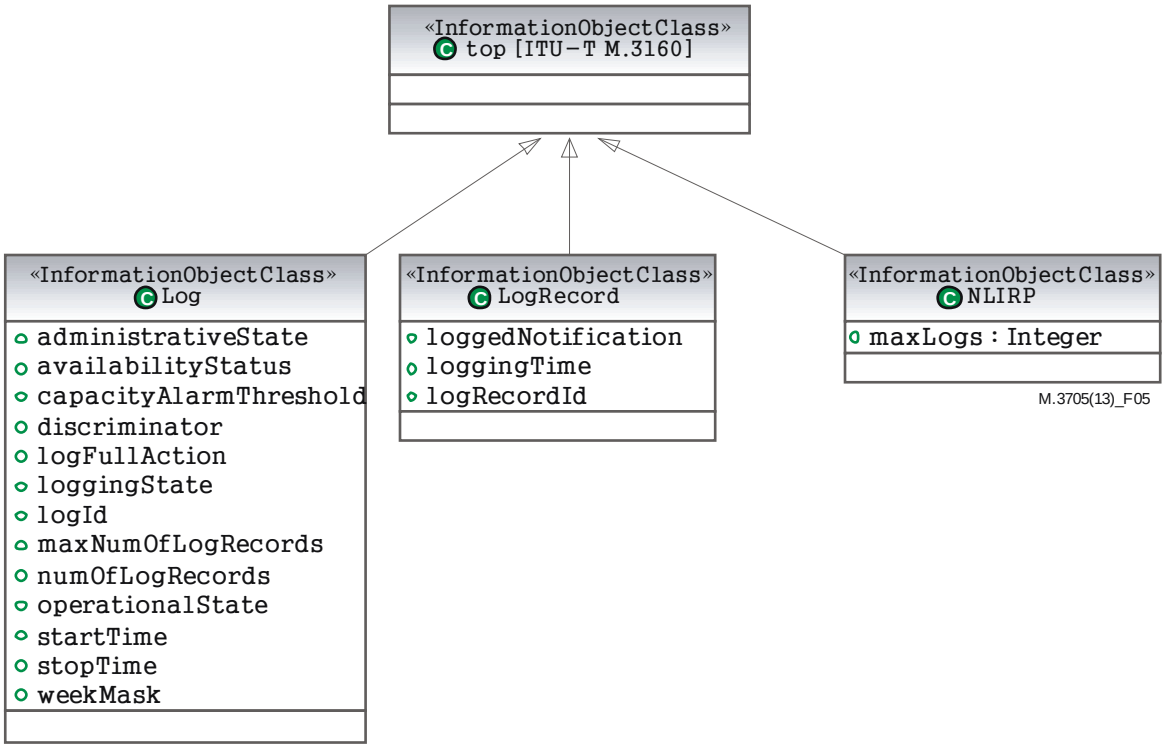

Figure 5 – Information object class inheritance

7.2.3 Information object class definitions

Class name	Qualifier	Requirement IDs
NLIRP	O	
Log	M	REQ-LM-FUN-07
LogRecord	M	REQ-LM-FUN-06

7.2.3.1 NLIRP(M)

7.2.3.1.1 Definition

NLIRP is the representation of the notification log management capabilities specified by this Recommendation. This object is provisioned by Agent.

7.2.3.1.2 Attributes

Attribute name	Support qualifier	Read qualifier	Write qualifier	Requirement IDs
maxLogs	O	O	–	

7.2.3.2 Log

7.2.3.2.1 Definition

The Log IOC is the representation of a notification log.

7.2.3.2.2 Attributes

Attribute name	Support qualifier	Read qualifier	Write qualifier	Requirement IDs
logId*	M	M	O	REQ-LM-FUN-10
discriminator	M	M	M	REQ-LM-FUN-02 REQ-LM-FUN-04
administrativeState	M	M	M	REQ-LM-FUN-05 REQ-LM-FUN-16
operationalState	M	M	–	REQ-LM-FUN-16
logFullAction	O	O	O	REQ-LM-FUN-21
availabilityStatus	O	O	–	REQ-LM-FUN-16
maxNumOfLogRecords	M	M	M	REQ-LM-FUN-18
numOfLogRecords	M	M	–	REQ-LM-FUN-18
capacityAlarmThreshold	O	O	O	REQ-LM-FUN-18
startTime	O	O	O	REQ-LM-FUN-03
stopTime	O	O	O	REQ-LM-FUN-03
weekMask	O	O	O	REQ-LM-FUN-03
loggingState	O	O	–	REQ-LM-FUN-16
NOTE – * indicates it is the naming attribute of this IOC.				

7.2.3.2.3 State diagram

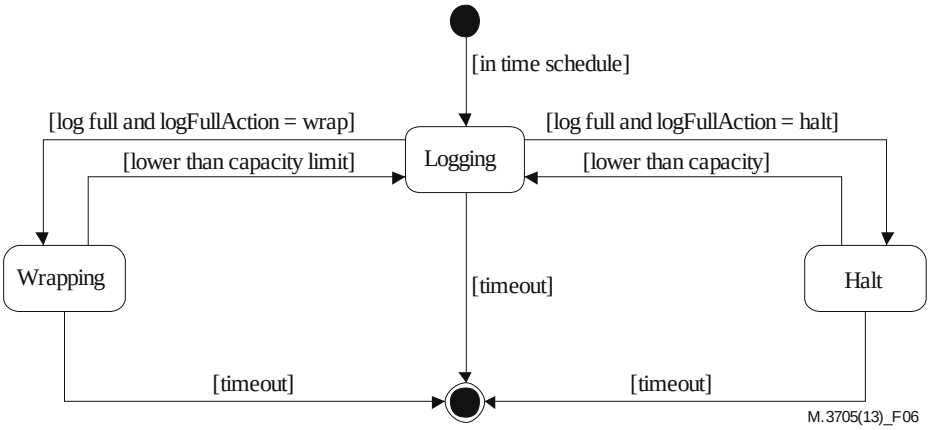

Figure 6 – State diagram for logging

It is up to a vendor-specific functionality whether a log that has been stopped shall remain visible across the interface or not. The deletion time of logs is vendor specific.

7.2.3.2.2 Notifications

Name	Qualifier	Requirement IDs	Notes
Object Create Notification [ITU-T M.3700]	M	REQ-LM-FUN-07 REQ-LM-FUN-17	
Object Delete Notification [ITU-T M.3700]	M	REQ-LM-FUN-07 REQ-LM-FUN-17	
Attribute Value Change Notification [ITU-T M.3700]	M	REQ-LM-FUN-02 REQ-LM-FUN-15 REQ-LM-FUN-16	Notification will be generated in case the following attribute is changed: discriminator, logFullAction, maxNumOfLogRecords, capacityAlarmThreshold, startTime, stopTime, interval
State Change Notification [ITU-T M.3700]	M	REQ-LM-FUN-02 REQ-LM-FUN-15 REQ-LM-FUN-16	Notification will be generated in case the following attribute is changed: administrativeState operationalState availabilityStatus loggingState
Alarm Notification [ITU-T M.3703]	O	REQ-LM-FUN-18	If capacityAlarmThreshold is not zero, in case numOfLogRecords reaches or is greater than capacityAlarmThreshold, an alarm is generated with probable cause " log capacity ". After numOfLogRecords is lower than capacityAlarmThreshold, the alarm disappeared.

7.2.3.3 LogRecord

7.2.3.3.1 Definition

The LogRecord IOC is the representation of an individual notification log record.

7.2.3.3.2 Attributes

Attribute name	Support qualifier	Read qualifier	Write qualifier	Requirement IDs
logRecordId*	M	M	–	REQ-LM-FUN-13 REQ-LM-FUN-15
loggingTime	M	M	–	REQ-LM-FUN-13
loggedNotification	M	M	–	REQ-LM-FUN-01 REQ-LM-FUN-08 REQ-LM-FUN-12
NOTE – * indicates it is the naming attribute of this IOC.				

7.2.3.3.3 Notifications (O)

Name	Qualifier	Requirement IDs	Notes
Object Created Notification[ITU-T M.3700]	M	REQ-LM-FUN-19	
Object Deleted Notification[ITU-T M.3700]	M	REQ-LM-FUN-19	

7.2.4 Information relationship definitions

Relationship	Support qualifier	Requirement IDs
Relation-nLIRP-log	M	

7.2.4.1 Relation-NLIRP-Log (M)

7.2.4.1.1 Definition

This represents the relationship between NLIRP and the log.

7.2.4.1.2 Role

Name	Definition
nLIRP	It represents the NLIRP.
Log	It represents the log.

7.2.4.1.3 Constraint

Name	Definition
maxlog	The number of log object instances no greater than the maxlogs attribute value in NLIRP
uniqueLogId	The logId must be unique within Agent.

7.2.5 Information attribute definitions

7.2.5.1 Definition and legal values

Attribute name	Definition	Legal values
administrativeState	See [ITU-T M.3701]	
availabilityStatus	See [ITU-T M.3701]	
capacityAlarmThreshold	This attribute defines the threshold number of log records in a log. When numOfLogRecords reaches the threshold, it will generate a capacity alarm.	INTEGER Integer greater or equal to 0, but smaller or equal to numOfLogRecords; 0 means no threshold.
discriminator	It specifies a filter constraint that Agent shall use to filter notifications; parameters in a notification can be used for filtering. The support of a time-based filter is mandatory. Support of other filter constraints is optional.	Filter constraint grammar is protocol dependent
weekMask	This attribute defines the interval of logging. It may indicate the interval in each week or each day etc. to do logging.	WeekMask [ITU-T M.3160]
logFullAction	Indicate the action that will be taken by this instance of Log when the maxNumOfLogRecords has been reached.	LogFullActionType ::= ENUMERATED { wrap, halt } • wrap: The oldest LogRecord(s) in the Log, based on the log time, will be deleted to free resources for the logging of new LogRecord(s). • halt: No more LogRecord(s) will be logged and all incoming events are discarded. LogRecord/s already in the log will be retained.
logRecordId	This attribute contains the id of a log record within a given log, assigned by the agent.	Name [ITU-T M.3020] The value of this attribute must be unique amongst all log record contained by a given log.
loggingState	Provides an indication of the current state of a specific log.	LoggingStateType::= ENUMERATED { logging, wrapping, halt, idle } • logging • wrapping • halt • idle (either not started or stopped)
loggingTime	This attribute defines the time that logged the notification.	GeneralizedTime [ITU-T X.680]
loggedNotification	This attribute defines the logged notification.	ANY, it can contain part of or all of the information of the logged notification.

Attribute name	Definition	Legal values
maxNumOfLogRecords	This attribute defines the max number of log records supported in a log. (Note)	INTEGER Integer greater than 0
numOfLogRecords	This attribute defines the current number of log records in a log.	INTEGER Integer greater than or equal to 0.
operationalState	See [ITU-T M.3701]	
startTime	This attribute defines the time to start logging. It works with stopTime to mean the validated period of the log.	GeneralizedTime [ITU-T X.680]
stopTime	This attribute defines the time to end logging.	GeneralizedTime [ITU-T X.680]
NOTE – In [ITU-T X.735] it is indicated by bytes, but bytes are protocol related, so here use the number of records instead.		

7.2.5.2 Constraints

Name	Definition
inv_logRecordCount	numOfLogRecords shall be less than or equal to maxNumOfLogRecords, and greater than or equal to zero.
Inv_logThreshold	capacityAlarmThreshold shall be less than or equal to maxNumOfLogRecords, and greater than zero.

7.3 Interface definition

The common object management operations have been defined in [ITU-T M.3700], the creation, deletion and modification of log object can reuse the "create object", "delete object" and "modify object" operations in [ITU-T M.3700]. So there is no need to define create/delete/modify log operations in this Recommendation.

There is an operation "getAttributes" defined in clause 7.3.1.1 of [ITU-T M.3700], which can be reused to retrieve log object with part or all of its attributes, so there is no need to define the "retrieve log object" operation in this Recommendation.

This is the same for the deleting and retrieval of LogRecord object operations.

7.3.1 Class diagram

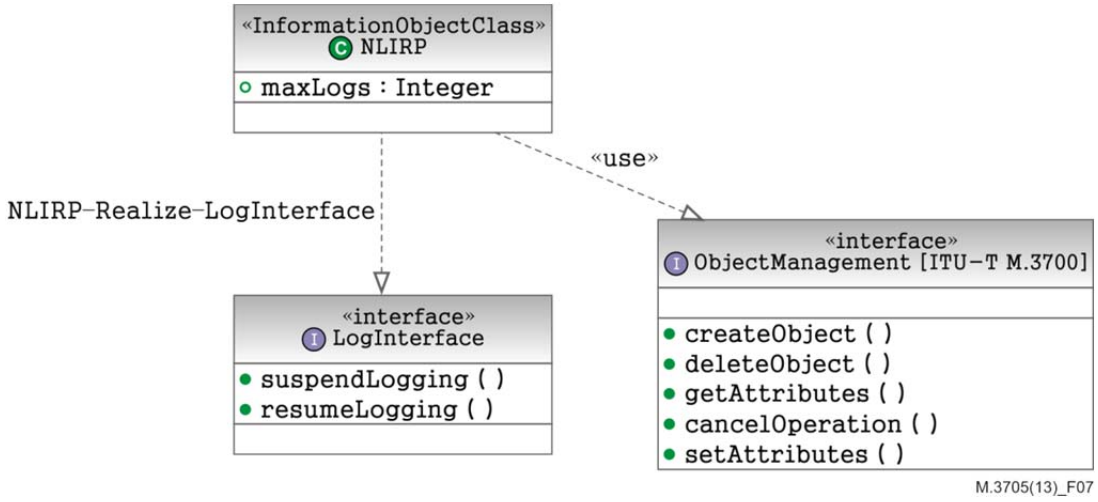

Figure 7 – Interface class diagram

7.3.2 Generic rules

This Recommendation follows the generic rules in clause B.2.3.2 of [ITU-T M.3020].

7.3.3 LogInterface interface(M)

7.3.3.1 Operation suspendLogging (M)

7.3.3.1.1 Definition

Manager invokes this operation to suspend a log object. Thus, the log pauses logging and can be resumed later.

7.3.3.1.2 Input parameters

The input parameters include the following:

Parameter name	Support qualifier	Information type/ Legal values	Comment
invokeIdentifierIn	CM	INTEGER A unique identifier that is Solution Set dependent.	This parameter identifies the current invocation. This parameter is used in the 'cancelOperation' operation [ITU-T M.3700] to cancel an on-going 'getMOAttributes' operation.
logObjectInstance	M	Name	It identifies the log object instance to be suspended.

7.3.3.1.3 Output parameters

Parameter name	Support qualifier	Matching information/ Information type/ Legal values	Comment
InvokeIdentifierOut	CM (Note)	INTEGER invokeIdentifierIn from the input parameters of this operation	This parameter identifies the current invocation in both IRPManager and IRPAgent. This parameter can be used together with the 'cancelOperation' operation to cancel an on-going 'getMOAttributes' operation.

Status	M	ENUMERATED {
		operationSucceeded,
		operationFailed
		}
			An operation may fail because of a specified or unspecified reason.

7.3.3.1.4 Pre-condition

Assertion name	Definition
logSuspendAssert	Log must not be suspended before suspend.

7.3.3.1.5 Post-condition

Assertion name	Definition
logSuspended	The administrativeState attribute is set to locked.
stateChangeNotification Emitted	A state change notification is sent after the administrativeState attribute in the log object is updated.

7.3.3.1.6 Exceptions

Assertion name	Definition
logIsAlreadySuspended	Condition: the requested log object is "Already" suspended. Returned information: The output parameter status. Exit state: Entry state.

7.3.3.2 Operation resumeLogging (M)

7.3.3.2.1 Definition

Manager invokes this operation to resume a log object instance, so that the paused logging can be resumed.

7.3.3.2.2 Input parameters

Parameter name	Support qualifier	Information type/ Legal values	Comment
invokeIdentifierIn	CM	INTEGER A unique identifier that is Solution Set dependent.	This parameter identifies the current invocation. This parameter is used in the 'cancelOperation' operation [ITU-T M.3700] to cancel an on-going 'getMOAttributes' operation.
logObjectInstance	M	Name	It identifies the log object instance to be suspended.

7.3.3.2.3 Output parameters

Parameter name	Support qualifier	Matching information/ Information type/ Legal values	Comment
InvokeIdentifierOut	CM (Note)	INTEGER invokeIdentifierIn from the input parameters of this operation.	This parameter identifies the current invocation in both IRPManager and IRPAgent. This parameter can be used together with the 'cancelOperation' operation to cancel an on-going 'getMOAttributes' operation.

Status	M	ENUMERATED {
		operationSucceeded,
		operationFailed
		}
			An operation may fail because of a specified or unspecified reason.

7.3.3.2.4 Pre-condition

Assertion name	Definition
logResumeAssert	Log must be suspended before resume.

7.3.3.2.5 Post-condition

Assertion name	Definition
logResumed	The administrativeState attribute is set to unlocked.
stateChangeNotificationEmitted	A state change notification is sent after the state attribute in the log object is updated.

7.3.3.2.6 Exceptions

Assertion name	Definition
logIsNotSuspended	**Condition**: the requested log object is not suspended. **Returned information**: The output parameter status. **Exit state**: Entry state.

Bibliography

[b-ITU-T Q.827.1] Recommendation ITU-T Q.827.1 (2004), *Requirements and analysis for the common management functions of NMS-EMS interfaces*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	**Telecommunication management, including TMN and network maintenance**
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2013