International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Q.834.3

(06/2004)

SERIES Q: SWITCHING AND SIGNALLING

Q3 interface

A UML description for management interface requirements for Broadband Passive Optical Networks

ITU-T Recommendation Q.834.3

ITU-T Q-SERIES RECOMMENDATIONS

SWITCHING AND SIGNALLING

SIGNALLING IN THE INTERNATIONAL MANUAL SERVICE	Q.1–Q.3
INTERNATIONAL AUTOMATIC AND SEMI-AUTOMATIC WORKING	Q.4–Q.59
FUNCTIONS AND INFORMATION FLOWS FOR SERVICES IN THE ISDN	Q.60–Q.99
CLAUSES APPLICABLE TO ITU-T STANDARD SYSTEMS	Q.100–Q.119
SPECIFICATIONS OF SIGNALLING SYSTEMS No. 4, 5, 6, R1 AND R2	Q.120–Q.499
DIGITAL EXCHANGES	Q.500–Q.599
INTERWORKING OF SIGNALLING SYSTEMS	Q.600–Q.699
SPECIFICATIONS OF SIGNALLING SYSTEM No. 7	Q.700–Q.799
Q3 INTERFACE	**Q.800–Q.849**
DIGITAL SUBSCRIBER SIGNALLING SYSTEM No. 1	Q.850–Q.999
PUBLIC LAND MOBILE NETWORK	Q.1000–Q.1099
INTERWORKING WITH SATELLITE MOBILE SYSTEMS	Q.1100–Q.1199
INTELLIGENT NETWORK	Q.1200–Q.1699
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR IMT-2000	Q.1700–Q.1799
SPECIFICATIONS OF SIGNALLING RELATED TO BEARER INDEPENDENT CALL CONTROL (BICC)	Q.1900–Q.1999
BROADBAND ISDN	Q.2000–Q.2999
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR THE NGN	Q.3000–Q.3999

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

ITU-T Recommendation Q.834.3

A UML description for management interface requirements for Broadband Passive Optical Networks

Summary

This Recommendation provides a UML description for the management interface between a supplier management system and an operator management system. This work defines part of the management aspects for network resources defined by the G.983-series of Recommendations for Broadband Passive Optical Network (BPON) equipment.

Generally speaking, the supplier management system is an element management system (EMS) and the operator management system is a network management system (NMS). However, the supplier management system is required to present a "network view" of connection management to the operator management system. Therefore, it was deemed necessary for the sake of clarity to use the terminology adopted in naming the systems involved.

Source

ITU-T Recommendation Q.834.3 was approved on 13 June 2004 by ITU-T Study Group 4 (2001-2004) under the ITU-T Recommendation A.8 procedure.

Keywords

APON, BPON, UML.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. 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/.

CONTENTS

ITU-T Recommendation Q.834.3

A UML description for management interface requirements for Broadband Passive Optical Networks

1 Scope

This Recommendation provides a UML description of a management interface between a supplier management system, provided to manage network resources conforming to specifications found in the G.983-series of Recommendations, and a network owner operation management system. It follows the process proposed in ITU-T Rec. M.3020 with alternations in order of presentation of material. Behaviour for real time and non-real time interfacing is addressed. All aspects of TMN management functional areas are addressed except for accounting management since usage data collection is outside the scope of the BPON equipment reference architecture.

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 G.983.1] ITU-T Recommendation G.983.1 (1998), *Broadband optical access systems based on Passive Optical Networks (PON).*

[ITU-T G.983.2] ITU-T Recommendation G.983.2 (2002), *ONT management and control interface specification for B-PON.*

[ITU-T G.983.3] ITU-T Recommendation G.983.3 (2001), *A broadband optical access system with increased service capability by wavelength allocation*.

[ITU-T G.983.4] ITU-T Recommendation G.983.4 (2001), *A broadband optical access system with increased service capability using dynamic bandwidth assignment*.

[ITU-T G.983.5] ITU-T Recommendation G.983.5 (2002), *A broadband optical access system with enhanced survivability*.

[ITU-T G.983.6] ITU-T Recommendation G.983.6 (2002), *ONT management and control interface specifications for B-PON system with protection features*.

[ITU-T G.983.7] ITU-T Recommendation G.983.7 (2001), *ONT management and control interface specification for Dynamic Bandwidth Assignment (DBA) B-PON system*.

[ITU-T M.2140] ITU-T Recommendation M.2140 (2000), *Transport network event correlation*.

[ITU-T M.3010] ITU-T Recommendation M.3010 (2000), *Principles for a telecommunications management network*.

[ITU-T M.3200] ITU-T Recommendation M.3200 (1997), *TMN management services and telecommunications managed areas: overview*.

[ITU-T M.3400] ITU-T Recommendation M.3400 (2000), *TMN management functions*.

[ITU-T Q.816.1] ITU-T Recommendation Q.816.1 (2001), *CORBA-based TMN services*: *Extensions to support coarse-grained interfaces*.

[ITU-T Q.834.1] ITU-T Recommendation Q.834.1 (2004), *ATM-PON requirements and managed entities for the network and network element view*.

[ITU-T Q.834.2] ITU-T Recommendation Q.834.2 (2001), *ATM-PON requirements and managed entities for the network view*.

[ITU-T X.720] ITU-T Recommendation X.720 (1992), *Information technology – Open Systems Interconnection – Structure of management information: Management information model*.

[ITU-T X.722] ITU-T Recommendation X.722 (1992), *Information technology – Open Systems Interconnection – Structure of management information: Guidelines for the definition of managed objects*.

[ITU-T X.734] ITU-T Recommendation X.734 (1992), *Information technology – Open Systems Interconnection – Systems Management: Event report management function*.

[ITU-T X.735] ITU-T Recommendation X.735 (1992), *Information technology – Open Systems Interconnection – Systems Management: Log control function*.

[ITU-T X.741] ITU-T Recommendation X.741 (1995), *Information technology – Open Systems Interconnection – Systems Management: Objects and attributes for access control*.

[ITU-T X.744] ITU-T Recommendation X.744 (1996), *Information technology – Open Systems Interconnection – Systems Management: Software management function*.

[ITU-T X.745] ITU-T Recommendation X.745 (1993), *Information technology – Open Systems Interconnection – Systems Management: Test management function*.

[ITU-T X.746] ITU-T Recommendation X.746 (2000), *Information technology – Open Systems Interconnection – Systems Management: Scheduling function*.

[ITU-T X.780.1] ITU-T Recommendation X.780.1 (2001), *TMN guidelines for defining coarse-grained CORBA managed object interfaces*.

3 Definitions

This Recommendation uses the following terms:

3.1 Terms defined in [ITU-T M.3010]

- user
- TMN management service
- TMN management function set

3.2 Terms defined in [b-OMG 99-06-01]

- activity diagram
- actor
- class
- class diagram
- collaboration diagram
- sequence diagram
- state diagram

– stereotype

– use case

3.3 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.3.1 activate: Execute installed software. Normally implies the switch of installed software from being secondary to primary.

3.3.2 assign: The outcome of service provisioning.

3.3.3 autodiscovery: The autonomous messaging to an OMS of creation or deletion notifications for equipment inventory data.

3.3.4 BPON resource: BPON network resources that need to be managed. These resources can be physical and logical.

3.3.5 build: The construction of a fragment of a management model based on containment rules and defined relationships, i.e., the provisioning of the parameters of a BPON managed resource, resulting from a discovery or autodiscovery process of installed equipment or through a pre-provisioning process prior to physical installation.

3.3.6 data warehouse: Long-term archival system, normally implemented as a database management system.

3.3.7 dispatch: To send personnel to a particular location where telecommunications equipment or facilities are or will be installed.

3.3.8 factory: Functionality that manufactures and deletes managed entities.

3.3.9 filtering: Criteria used for selection purposes.

3.3.10 includes: An include relationship from use case A to use case B indicates that an instance of the use case A will also contain the behaviour as specified by use case B (see [ITU-T M.3400]).

3.3.11 install: Physical placement of equipment. This means that shelves have been installed and powered. All common equipment is inserted. Management communication has been established. Interface cards may be inserted.

3.3.12 management model: Formal description of managed entities and relationships between them.

3.3.13 range: Ranging is a function used to measure the round-trip delay between the OLT and each ONU or ONT in order to determine the transmission timing for the subtending ONT or ONU. The process also involves establishing of security mechanisms (churning key algorithm) and the embedded operations channel. Ranging may be initiated manually by supplying the OLT with the serial number of the ONT or ONU. If supported by the implementation, ranging can also be initiated automatically by the OLT.

3.3.14 register: The process used to bring a network resource into the management jurisdiction of the supplier management system. The management communication link is established to a physically installed NE, and the NE is included in the management domain for the supplier management system.

3.3.15 reserve: The setting aside of network resources before provisioning of service.

3.3.16 service instance: A service instance is a connection between a UNI endpoint on an ONT or NT and an NNI endpoint at an OLT, or between UNI endpoints on two ONTs or NTs.

3.3.17 transfer function: This function implies the use of a non-real time protocol.

3.3.18 user label: Indicates an identifier that is created and provided by the operator or operator management system to associate with a managed resource by the supplier management system.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AAL	ATM Adaptation Layer
APON	ATM Passive Optical Network
ATM	Asynchronous Transfer Mode
BICI	Broadband Inter-Carrier Interface
BISSI	Broadband Inter-Switching System Interface
BPON	Broadband Passive Optical Network
CAC	Call Admission Control
CES	Circuit Emulation Service
CORBA	Common Object Request Broker Architecture
CTP	Connection Termination Point
DCN	Data Communications Network
DSx	Digital Signal x
EM-OSF	Element Management Layer Operations System Function
EMS	Element Management System
EOC	Embedded Operations Channel
Ex	European digital signal x
FSAN	Full Service Access Network
GDMI	Guidelines for the Definition of Management Information
GUI	Graphical User Interface
IP	Internet Protocol
ME	Managed Entity
MIB	Management Information Base
NE	Network Element
NM-OSF	Network Management layer Operations System Function
NMS	Network Management System
NT	Network Terminal
ODN	Optical Distribution Network
OLT	Optical Line Terminal
OMG	Object Management Group
OMS	Operator Management System
ONT	Optical Network Terminal
ONU	Optical Network Unit

OS	Operations System
OSF	Operations System Function
PON	Passive Optical Network
PVC	Permanent Virtual Circuit
QoS	Quality of Service
RCAA	Root Cause Alarm Analysis
RCIA	Root Cause Impairment Analysis
SM-OSF	Service Management layer Operations System Function
TCA	Threshold Crossing Alert
TMN	Telecommunication Management Network
TP	Termination Point
TTP	Trail Termination Point
UML	Unified Modelling Language
UNI	User Network Interface
VC	Virtual Channel
VCC	Virtual Channel Connection
VCI	Virtual Channel Identifier
VCL	Virtual channel link
VDSL	Very high speed Digital Subscriber Line
VP	Virtual Path
VPC	Virtual Path Connection
VPI	Virtual Path Identifier
VPL	Virtual Path Link

5 Conventions

Any "communicates" association between an actor and use case in the requirements clause (see clause 6.2), refers to the Q interface addressed in this Recommendation when the actor is any one of the following: OMS, privileged user, external event channel, profile object repository, data warehouse or secure file server. Figure 5-1 illustrates this diagrammatic reference.

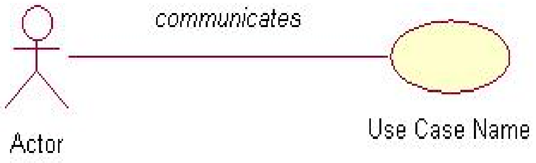


Figure 5-1 – Q interface reference in use case diagram

Any association between an actor and an object class in the analysis clause (see clause 6.3) refers to the Q interface addressed in this Recommendation when the actor is any one of the following: OMS, privileged user, external event channel, profile object repository, data warehouse or secure file server. Figure 5-2 illustrates this diagrammatic reference.

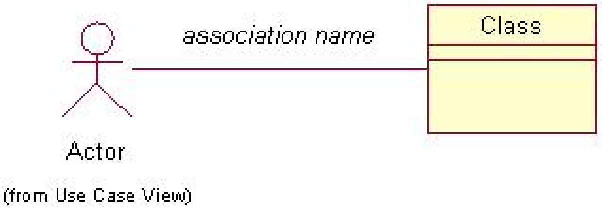


Figure 5-2 – Q interface reference in class diagram

All other associations, as well as other object classes not possessing such an association to these actors in the analysis clause are provided in this clause in order to complete the description of expected behaviour of the supplier management system and the BPON NEs within its management jurisdiction when fulfilling the TMN management needs of the operator and operator management systems. In general, it is not required that the supplier management system explicitly implement these associations, or object classes, provided that the implementation possesses the same behaviour. However, when an object class appears in the Analysis clause, and this class is one of the managed entities of [ITU-T Q.834.1] or [ITU-T Q.834.2], the class shall be implemented within the supplier management system as part of its logical schema. In general, the managed entities of [ITU-T Q.834.1] and [ITU-T Q.834.2] provide management data that is present on the mechanized interface.

6 GDMI template

6.1 Scope

The scope of this Recommendation includes management aspects for a BPON system as described by the G.983-series of Recommendations. The BPON system can be classified as an access and terminal equipment network [ITU-T G.983.1]. The management services covered by this Recommendation include aspects of network and service provisioning management, network performance management, traffic management, maintenance management and security administration. Figure 6-1 below shows the Q interface addressed in this Recommendation.

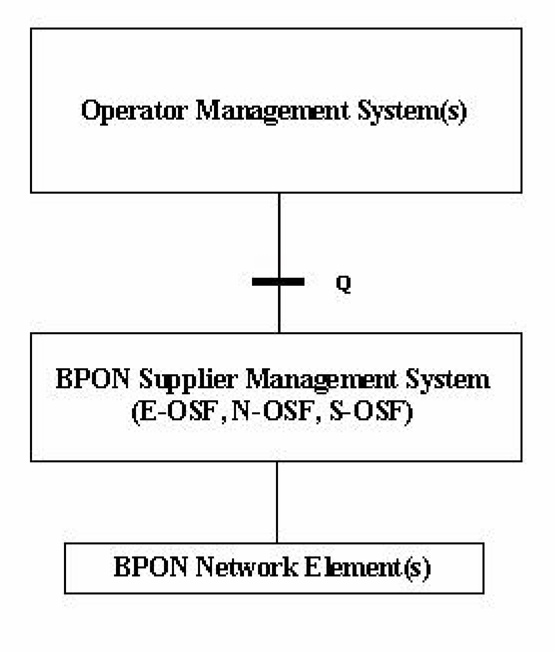

Operator Management System(s)
Q
BPON Supplier Management System
(E-OSF, N-OSF, S-OSF)
BPON Network Element(s)

Figure 6-1 – Reference interface

6.2 Requirements

6.2.1 Business level requirements

Major business requirements concerning the functionality of the supplier management system are documented in [ITU-T Q.834.1]. Services performed by the supplier management system on behalf of the operator management system(s) and operator users are controlled by the interfaces supported by the supplier management and described by the requirements provided in [ITU-T Q.834.1].

6.2.1.1 Actor roles

There are several actors mentioned in the high-level use case diagrams provided in clause 6.2.1.3. These actors include the following: operator, privileged user, operator management system (OMS), external event channel, white pages, data warehouse, BPON NE, profile object repository and secure file server. Figure 6-2 provides a brief definition of the roles that these actors play.

Actor	Roles
Operator	User interacting with the supplier management system via a graphical user interface.
Privileged user	User with administrative access to the supplier management system. Can be a system or operator.
Operator management system (OMS)	Separate management systems supporting operator TMN management requirements.
External event channel	Consumer of BPON events supplied by the supplier management system. This channel acts as a conduit of event information to interested client applications.
White pages	Directory service for resolving names of objects referenced by interface method invocations.
Data warehouse	Long-term archive of records maintained by the operator.
BPON NE	Equipment that is a network element.
Profile object repository	External OMS where profile objects reside.
Secure file server	Secure and centralized repository of network element configuration data and software generics.

Figure 6-2 – Actors and roles

6.2.1.2 Telecommunications resources

Figure 6-3 illustrates the BPON system architecture. The operation system linked to the OLT in this figure is the supplier management system. This system is provided, along with the equipment, to a network owner operator. There is no specification concerning the management communications interface between the OLT and the supplier management system. Consequently, both the supplier management system and the managed BPON equipment are viewed as relevant telecommunications resources in this Recommendation.

The optical line terminal (OLT) is a head-end digital terminal commonly located in the central office or some controlled environment structure. The optical distribution network (ODN) is a point-to-multipoint fibre infrastructure employing a passive splitter or coupler device for the fan out. The ONU provides the access network line termination function and the ATM multiplexing and de-multiplexing function. The NT provides the user network interface line termination function. The reference point, indicated by the term UNI, denotes the user network interface. It is used in the most abstract sense and is meant to indicate any type of service interface. The ONT combines the functions of the ONU and NT in one piece of equipment. In some cases, the UNIs from one ONT may belong to different users.

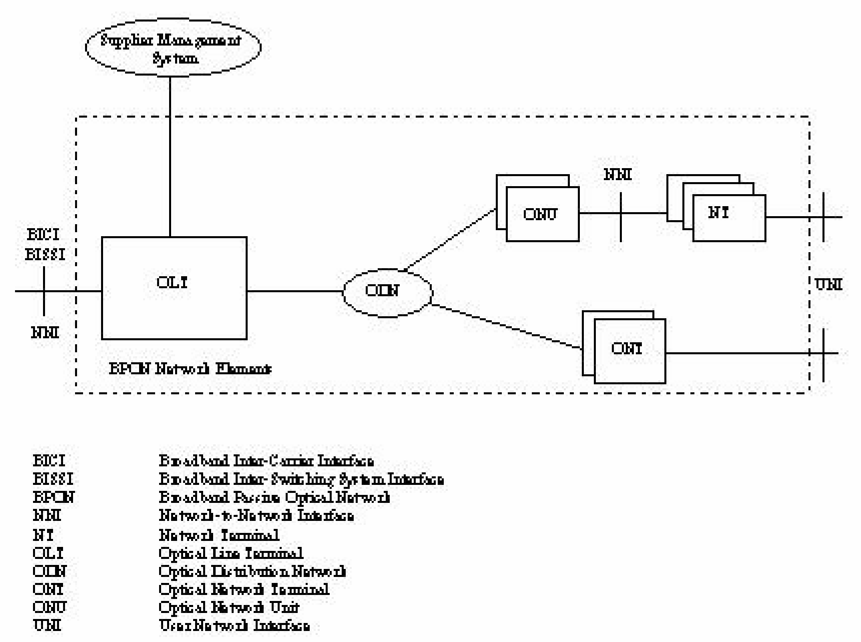

Supplier Management System
BICI
BISSI
NNI
OLT
ODN
ONU
NNI
NT
ONT
UNI
BPON Network Element
BICI Broadband Inter-Carrier Interface
BISSI Broadband Inter-Switching System Interface
BPON Broadband Passive Optical Network
NNI Network-to-Network Interface
NT Network Terminal
OLT Optical Line Terminal
ODN Optical Distribution Network
ONT Optical Network Terminal
ONU Optical Network Unit
UNI User Network Interface

Figure 6-3 – BPON system architecture

6.2.1.3 High-level use case diagrams

This clause contains high-level use case diagrams that summarize the functionality and interfaces of the supplier management system. Use cases are shown in these diagrams even when they do not have a "communicates" association to an external actor. The internal functionality described by these use cases serves an important purpose in that the behaviour of the supplier management system would be incompletely characterized without it. In some cases there are specific use cases mentioned on more than one high-level diagram. Again, the reason for this duplication is to aid in completing the characterization of behaviour and functionality. Use case descriptions are provided for every use case pictured in these high-level diagrams.

The interfacing to BPON technology domain objects through a façade object or through a fine-grain mechanism is defined and described in ITU-T Rec. X.780 and [ITU-T X.780.1] with key services defined in ITU-T Rec. Q.816 and [ITU-T Q.816.1].

The first overview use case diagram shows the interactions involved administering user access to the supplier management system.

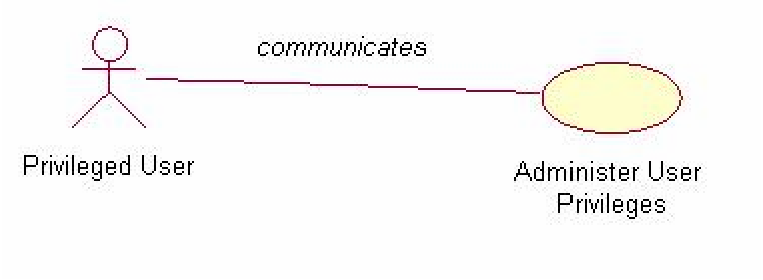


Figure 6-4 – Access control

The second overview use case diagram shows the external interactions involved in event handling activities of the supplier management system. It includes both real time and non-real time activities.

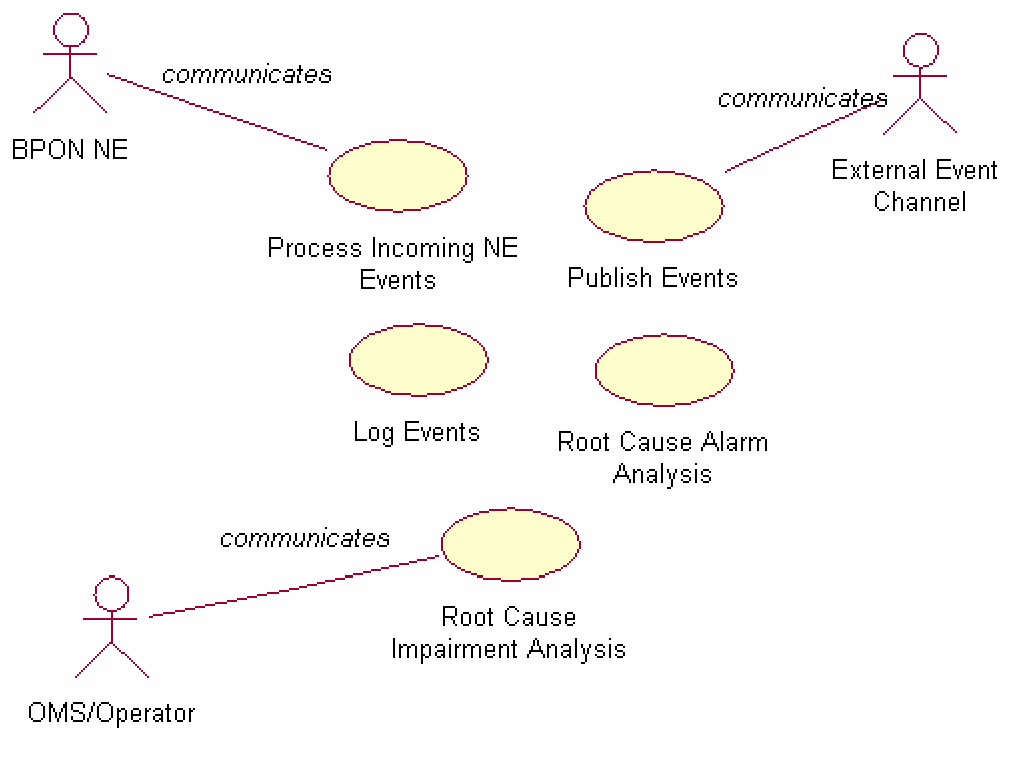


Figure 6-5 – Event handling

The third overview use case diagram covers the external interactions involving software and configuration data management by the supplier management system.

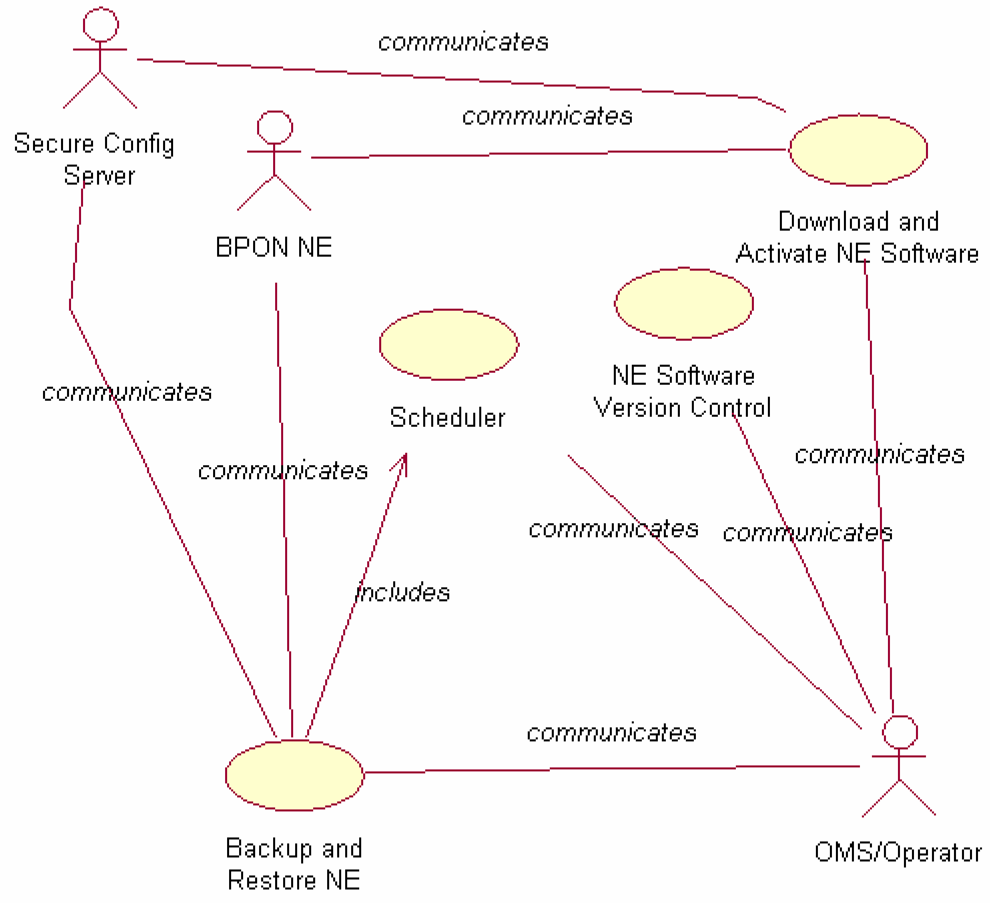


Figure 6-6 – Software and configuration data management[1]

[1] Backup and restore NE use case only communicates with the actor Secure Config Server when the MIB data is stewarded by the EMS.

The fourth overview use case diagram shows the interactions for testing functionality through the support of the supplier management system.

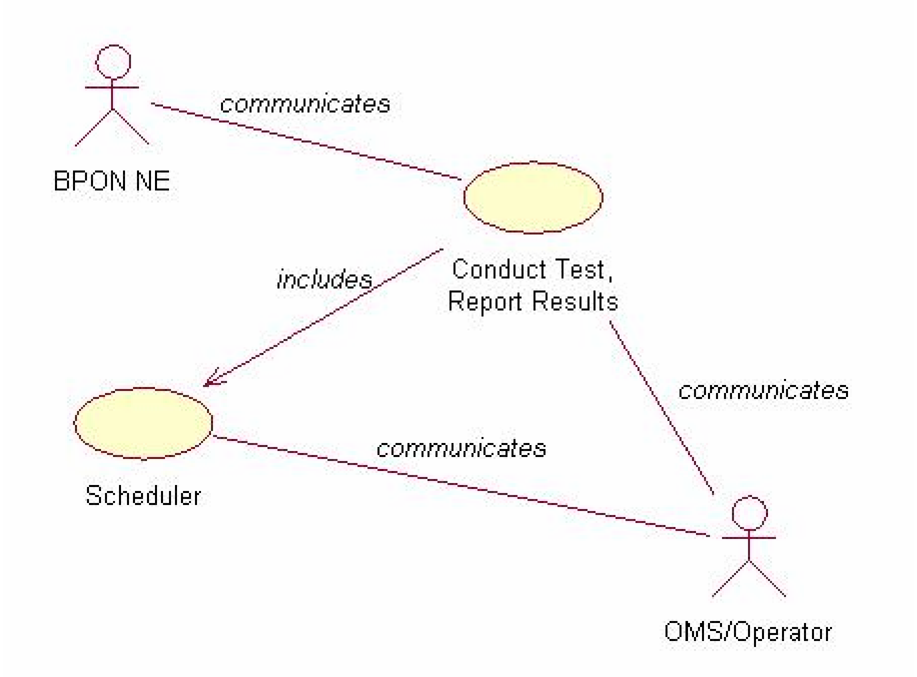


Figure 6-7 – Testing

The fifth overview use case diagram presents the internal functionality and external interactions of the supplier management system associated with the installation of BPON equipment.

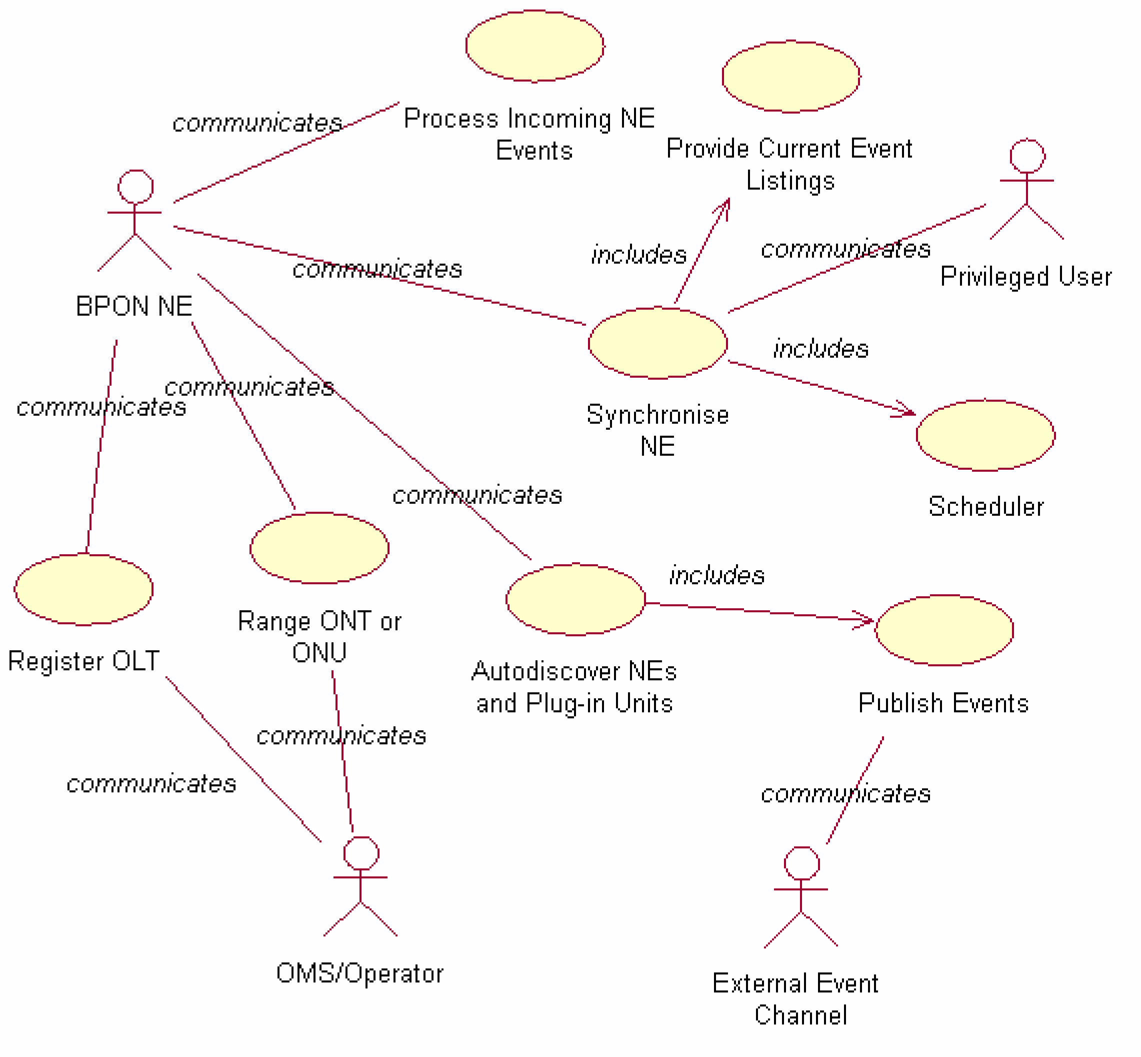


Figure 6-8 – Installation

The sixth overview use case diagram presents the internal functionality and external interactions of the supplier management system associated with provisioning of BPON network elements and BPON services.

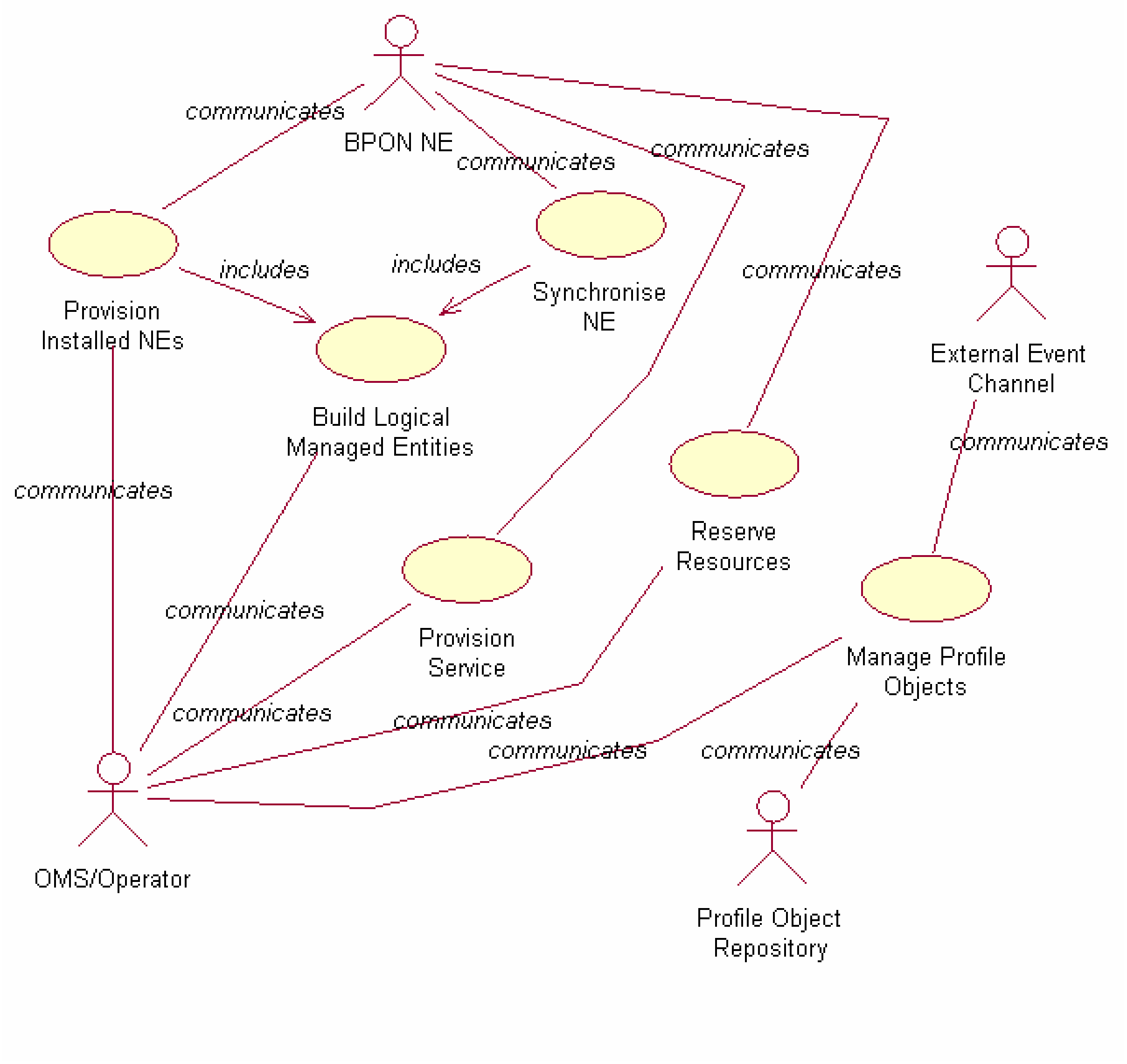


Figure 6-9 – Provisioning

The seventh and final overview use case diagram presents the external interactions of the supplier management system associated with collection of statistics and bulk transfer of large amounts of data stored in short-term archives within the supplier management system.

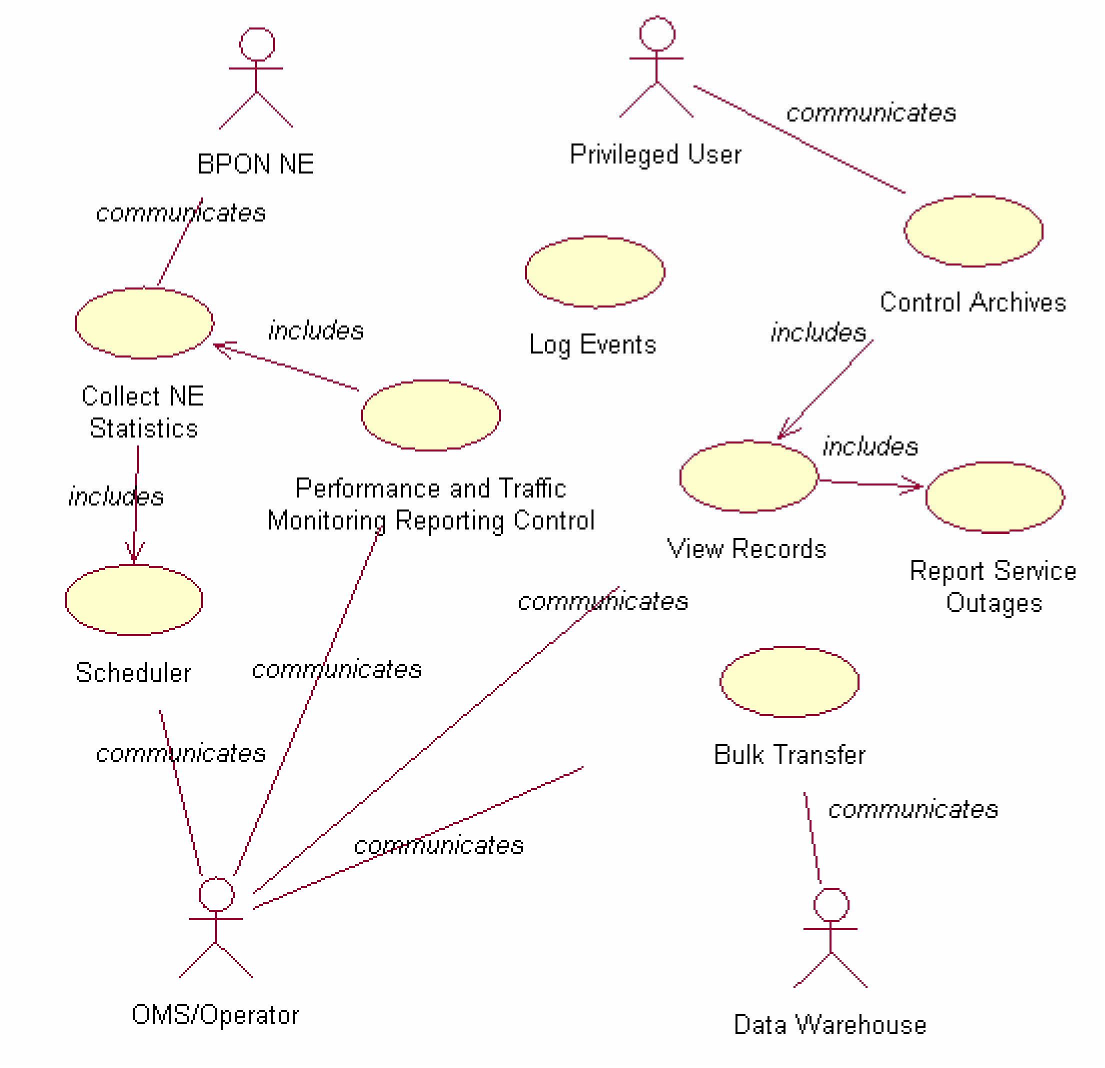


Figure 6-10 – Archiving and bulk transfer

6.2.2 Specification level requirements

This clause contains textual details for each of the use cases shown in the high-level use case diagrams of the previous clause. The details are provided to clarify the roles of external actors and telecommunications resources, to establish the basis for interactive diagrams in the analysis clause, and to refine the previous high level use case diagrams to a specification level. Use case details include the following components:

– Summary: Short summary of use case functionality referencing TMN functionality as needed.

– Assumptions: Listing of requirements surrounding the use case that would affect the design of the application code of the supplier management system.

– Actors: Actors are listed as shown in Figure 6-2 followed by parenthetical role characteristic as needed.

– Preconditions: Identifies the trigger for the use case commencement.

– Description: Detailed textual rendition of the functionality of the use case including stops where exceptions can occur.

– Exceptions: Identifies unsuccessful completion circumstances for the use case.

– Post-conditions: Identifies the conditions that will hold if the use case ends successfully.

The use case details are listed alphabetically by the use case title shown in the diagrams of the previous clause.

6.2.2.1 Administer user privileges

Summary: This use case describes functionality for creating, deleting, assigning and using access control information for users of the supplier management system.[2]

Assumptions: Authentication is accomplished through use of an external authentication service for operator or OMS access and this function is outside the scope of the use case. The supplier management system has authenticated the requesting operator or OMS. Control of human user access to the supplier management system via the OMS is controlled by the OMS and is outside the scope of this use case. Access to the supplier management system via an OMS by any human user of the OMS is viewed to have the same privileges as the OMS. The supplier management system supports an administrative privileged user. Default logins and passwords have been provided to this user for initial login. Target activities are defined previously and known to the supplier management system.

Actors: Privileged user.

Preconditions: The supplier management system has been installed. Connectivity between the supplier management application, OMSs, and all required GUI client applications has been provided.

Description: This use case begins when the supplier management system is first installed and the privileged user is required to establish access permission for any users of the supplier management system. The privileged user retrieves the default password policy of the supplier management system and determines whether or not to change the settings. If changes are needed, the privileged user makes them. Next, the privileged user checks the target activities and permission levels for any system-provided user group and determines whether or not these user groups will meet operational needs [unknown user group]. The privileged user will create new user groups if necessary based on this analysis [duplicate user group, unknown targets].

With a list of current operators in hand, the privileged user then creates new users and assigns them to user groups or establishes special target activities on an individual case basis [unknown user group, duplicate user Id, unknown targets, user login policy violation]. Settings for activity level for each activity for each user Id or group of users have values including "monitor only", "allowed to execute" or "no-access", to designate allowable operations on an individual activity basis.

As operator assignments change, the privileged user maintains access control for these changes by any of the following means:

– adding new operators to existing user groups [unknown user group];

– retrieving the permission listing for any existing user [unknown user Id], and making modifications to the listing according to operational needs either through membership to different user groups or by individual assignment [unknown targets, unknown user Id, unknown user group];

– deleting users who have left the company or whose assignments have changed so as to no longer require access to the supplier management system [unknown user Id].

[2] This use case description makes use of management functionality described in [ITU-T X.741].

Additionally, as high-level network administrative changes occur, the privileged user can re-define the management scope of groups of users. The privileged user can examine existing operator assignments to specific user groups or can examine the access limitations established for the user group [unknown user group]. The privileged user can perform broad reassignments as well as make modifications to the access limitations defined. This includes adding, deleting or modifying the level of accessibility to any activity [unknown user group, duplicate user group, unknown targets]. It may also include the elimination of existing user groups [unknown user group, user group not empty].

Subsequently, operators attempting to log onto the supplier management system experience the following verification process. The access control manager of the supplier management system verifies the user Id and password of the operator and grants the operator GUI access to the functionality allowed in the permission list. At any time after establishing access permission levels, the user may forget their password. The user Id – password relationship can be re-established by the privileged user [user login policy violation, unknown user Id].

This use case ends when the privileged user has updated permissions as needed.

Exceptions: Unknown user Id, unknown targets, duplicate user Id, unknown user group, duplicate user group, user group not empty.

Post-conditions: Operator access to the supplier management system is restricted to the activities and items that are allowed by permission and privilege listings. As the supplier management system software is upgraded, operator access control settings are preserved.

6.2.2.2 Autodiscover NEs and plug-in units

Summary: The supplier management system publishes changes in inventory management information to the operator or OMS. Changes in inventory management information are discovered by the supplier management system as a result of establishing management communications to an installed NE, or through the insertion or removal of a plug-in unit.

Assumptions: Communications between the supplier management system and the OLT are in place. Inventory data modelled in the supplier management system for an NE (including contained equipment holders) and plug-in units may be overwritten based on discovered data. The "to be discovered" equipment is in a stable condition. Embedded NE software is able to detect actual plug-in units present and act accordingly (in the case of the ONT or ONU, this implies that the default setting for any slot must be "plug and play"). Inventory management data refers to the type of information normally tracked by a capital asset system concerning physically installed equipment.

Actors: No external actors.

Preconditions: An OLT is installed.

Description: This use case begins when any one of the following events takes place:

– an OLT is registered;

– an ONT or ONU is ranged;

– an NT is installed and connected to a port of the ONU;

– a plug-in unit is installed in or removed from a slot of an installed NE having an available management communications channel to the supplier management system.

Registration of an OLT is an event triggering the synchronization of provisioned or modelled inventory management data for the OLT with the same inventory properties discovered through direct communications with the OLT. The supplier management system uses a set of managed entity creation records to format information about discovered properties of the OLT, the shelves contained within the OLT (equipmentHolderF), the slots within the shelves (equipmentHolderF), and the plug-in units inserted in the slots (plugInUnitF), including information concerning embedded software for the OLT or plug-in unit.

The ranging of an ONU or ONT, whether on demand by the supplier management system or through the automatic ranging function described by [ITU-T G.983.1] for a newly installed ONT or ONU, is an event that also triggers the synchronization of provisioned or modelled inventory management data for the ONU or ONT with the same inventory properties discovered through direct communications with the ONU or ONT. The supplier management system uses a set of managed entity creation records to format information about discovered properties of the ONU or ONT, the shelves contained within the ONU or ONT (equipmentHolderF), the slots within the shelves (equipmentHolderF), the plug-in units inserted in the slots (plugInUnitF), and the embedded software for the ONU or ONT or of any plug-in unit present.

If any port of the ONT is integrated to the ONT (meaning not the port of a plug-in unit), then this port relationship is known through recognition of the hardware version of the ONT.

The installation of an NT with connection to a port on the ONU is an event that triggers the synchronization of provisioned or modelled inventory management data for the NT with the same inventory properties discovered through supplier management system discovery of this network element. The supplier management system uses a set of managed entity creation records to format information about the discovered properties of the NT, the slots of the NT if any (equipmentHolderF), and any plug-in units that may be inserted in the slots (plugInUnitF) including information concerning embedded software loads for the NT or plug-in units.

The manipulation of a plug-in unit in a slot is an event that triggers either the formatting of a managed entity creation record for the plug-in unit in the case of insertion, or the formatting of a managed entity deletion record for the plug-in unit in the case of removal. Embedded software of the plug-in unit is also discovered.

If any of these synchronization activities indicates a difference between what had been planned and what is actually present, then the supplier management system will form an alarm event record indicating the mismatch.

This use case ends when the supplier management system formats the inventory change and/or provisioned versus installed alarm information into a form appropriate for publication to the external event channel.

Exceptions: None specified since this use case does not describe an IF1 communications mechanism.

Post-conditions: The newly discovered data is made available to the OMS and operators responsible for inventory management.

6.2.2.3 Backup and restore NE

Summary: The supplier management system provides the operator with capabilities for backing up and subsequent restoring of BPON system configuration data in the case of catastrophic failure of the OLT.

Assumptions: The supplier management system has authenticated the requesting operator or OMS. Stewardship of the OLT system MIB[3] may be in the OLT, may be in the supplier management system or may be spread between the two. OLT system refers to the OLT and all its subtending BPON NEs. The OLT has the current copy of MIB data for its subtending BPON NEs. When required, the restoring of system configuration data to the OLT and its return to normal functioning

[3] Here system MIB (or Management Information Base) is used generally to mean all configuration data held within the system.

must be accomplished as soon as possible. Backup versions of the OLT system MIB information are available on a secure file server.

Before the restore or backup processes can start, DCN communications between the OLT and supplier management system and between the OLT and the secure file server must be available. Before the restore process begins, the OLT equipment must be repaired.

Actors: Operator, OMS, BPON NE (OLT), secure file server.

Preconditions: The BPON OLT is installed, registered and not experiencing a catastrophic failure.

Description: This user case begins when an operator or OMS wishes to establish the routine backup of system configuration data found in a newly installed BPON system. The operator or OMS formulates a request that identifies the OLT system, provides the DCN address for the destination server and user Id and password to access the destination server, gives the full directory location for the backup file and a flag indicates whether the backup should overwrite the existing file or not, and specifies a schedule to be followed when backing up the configuration data [unknown destination server, unknown scheduler, invalid scheduler, unknown NE].

The supplier management system returns a tracking object Id to the request that can be used to cancel, abort, monitor the progress of, or change the schedule for, the back up activities [unknown backup process, unknown scheduler, invalid scheduler, comm failure, equipment failure]. Subsequently, the scheduling utility launches the actual backup activity according to a time trigger.

The master of the OLT system MIB data may be the supplier management system, may be the OLT, or the responsibility may be shared between the two. As a result, OLT system MIB data may have to be uploaded from several locations at the same time. If the information comes from two locations (OLT and supplier management system) the backup data must be held in the same destination server directory.

The server retains multiple versions of backup data. If need be, this server uses tape device backup itself to archive sufficient versions for operator requirements of security and reliability. The supplier management system maintains a log of successful and unsuccessful backups.

Occasionally, due to DCN communications failures, NE software upgrade safeguards or other factors, it may be necessary to request a backup on-demand. In this case, the OMS or operator formulates a backup request specifying the OLT, the DCN address for the destination server, the user Id and password to access the destination server, the full directory location for the backup file and a flag indicates whether the backup should overwrite the existing file [unknown destination server, comm failure, equipment failure, unknown NE].

If an OLT needs to be restored, maintenance activities may be required (including replacement of plug-in units) before the operator can request a restore of the OLT system. The operator accesses the log of successful uploads and chooses a version to use to restore the OLT. The operator forms a restore request. This request includes the identity of the OLT and the version of archived MIB data to be used, as well as the location of the archived file and user Id and password for supplier management system access to the archived file. The operator may also let the supplier management system make the "best possible" version choice.

The supplier management system checks the requested version against current equipment and software versions and determines if the version can be downloaded for the purposes of restoring the NE [software load hardware mismatch, unknown NE, denied access, unknown source file, unknown source server, comm failure, equipment failure]. In the case that the OLT is the master of the data, the supplier management system causes the OLT to pull the correct MIB version from the server. In the case that the supplier management system is the master of the data, the supplier management system pulls the version of MIB data from the server. In both cases, the configuration data eventually is downloaded and installed in the OLT.

The operator may monitor the progress of the restore activity [unknown restore process]. The operator may also view the final disposition of the activity by examining a log reporting on the success or failure of the restore process.

The use case ends when the restored OLT establishes management communication with the supplier management system.

Exceptions: Unknown NE, software load hardware mismatch, unknown destination server, unknown scheduler, comm failure, equipment failure, unknown backup process, unknown restore process, unknown source server, unknown source file.

Post-conditions: The successful download of MIB data triggers an NE synchronization process between the NE and the supplier management system.

6.2.2.4 Build logical managed entities

Summary: The supplier management system builds and/or modifies management model groupings for planned or installed BPON equipment on request of an OMS or operator, or builds management model groupings as a result of discovery. The constructed resources (consisting potentially of many managed entities) include but are not limited to NEs, plug-in units and logical resources such as TCONTs and MACBridges.

Assumptions: The supplier management system has authenticated the requesting operator or OMS. The OLT must be registered with the supplier management system if discovery triggers this use case. If the OLT is already registered, the DCN connection between the supplier management system and the OLT must be available to build subtending managed entities. The DCN connection between the supplier management system and the operator or provisioning OMS is available. The supplier management system is responsible for providing unique identifiers for managed entities that are contained within the context of an OLT system that are created by execution of this use case. As result of some external process outside the scope of this use case, the OMS or operator will have knowledge of the equipment hierarchy and naming conventions of the supplier management system.

Actors: OMS, operator.

Preconditions: The supplier management system is installed.

Description: This use case begins when the operator plans for the installation of all or part of the BPON equipment, needs to modify parameters that have been automatically applied to newly installed BPON equipment, or needs to provision infrastructure aspects of BPON equipment that are not automatically established by installation of the equipment.

When the operator plans for the installation of an NE, the operator or OMS formulates a request identifying the type of node, indicating versions of hardware and software, providing various configuration profiles to be associated with the node, and supplying several operator labels. A similar request is formulated for construction of plug-in units that also includes slot assignment [unrecognized version, invalid serial num syntax, duplicate serial number, unknown profiles, parameter violation, unknown managed entity, duplicate user label, invalid external time, unknown system timing source, profile suspended, unknown NE, invalid equipment code, slot already assigned, unknown slot, invalid slot assignment list].

The build process within the supplier management system follows containment relationships and other obvious restrictions (e.g., a plug-in unit is not built until the containing node has been constructed, or a protection grouping of ports is not built until the ports exist, or the construction of a subtending ONT or ONU is not possible unless the serving PON interface card port on the OLT exists). The construction of all managed entities within the supplier management system that is the consequence of a single request follows the schema for configuration managed entities described in [ITU-T Q.834.1]. The supplier management system follows the equipment hierarchy rules for the supplier's equipment, assigning identifiers to the managed entities it builds. The supplier management system returns with a unique identifier for the constructed item.

The operator proceeds with provisioning activities such as modifications to port attributes, construction of protection groupings of ports, construction of MACBridges (if required), and construction of TCONTs. In each case, a request is formulated that identifies previously built managed entities, supplying configuration profiles and parameters, providing operator labels and, in some cases providing some control logic [unknown NE, insufficient PON BW, unsupported TCONT type, duplicate user label, unknown managed entity, unknown profiles, parameter violation, profile suspended, invalid protection scheme, interface speed not changeable]. As before, the logical schema for configuration managed entities described in [ITU-T Q.834.1] is followed. These activities can occur before or after the equipment is installed. The provisioning request results in configuration changes in any installed NE. The supplier management system returns with a unique identifier for any constructed item.

If NEs and plug-in units are installed prior to operator or OMS provisioning activities, then the supplier management system shall support the augmentation of discovered equipment configuration information with profile assignments and user label assignments. In this case, the operator or OMS will formulate configuration requests identifying managed entities whose existence and identity have been provided to the OMS through installation notification reports, supplying configuration profiles and parameters, providing operator labels and, in some cases, providing some control logic [unknown NE, insufficient PON BW, unsupported TCONT type, duplicate user label, unknown managed entity, unknown profiles, parameter violation, profile suspended, invalid protection scheme, interface speed not changeable, invalid slot assignment list, invalid external time]. As before, the logical schema for configuration managed entities described in [ITU-T Q.834.1] is followed. The provisioning request results in configuration changes in the installed NE.

Eventually it may become necessary to remove a BPON network resource. In this case, the operator or OMS requests that the administrative state of the resource be locked and then that it be deleted [unknown NE, remaining contained managed entities, remaining reservations, remaining subnetwork connections, unknown managed entity].

This use case ends when infrastructure provisioning information has been successfully conveyed to the supplier management system and transfer to any pertinent installed BPON NE.

Exceptions: Unknown managed entity, unknown NE, unknown system timing source, unknown profiles, unknown slot, unrecognized version, remaining contained managed entities, remaining reservations, remaining subnetwork connections, duplicate user label, duplicate serial number, invalid parameter value, invalid slot assignment list, invalid external time, invalid equipment code, invalid user label syntax, invalid protection scheme, profile suspended, invalid serial number syntax, interface speed not changeable, slot already assigned, insufficient PONBW, profile suspended.

Post-conditions: The resource is built within the supplier management system management model and is available for activities such as service provisioning.

6.2.2.5 Bulk transfer

Summary: Based on a timer (scheduler) or explicit request, the supplier management system transfers archived data through non-real time transfer mechanisms to a separate server known as a data warehouse. Archived data includes the contents of logs or record sets of statistics. This functionality includes monitoring and tracking of the transfer procedure.

Assumptions: The supplier management system has authenticated the requesting operator or OMS. A communication link exists and is available between the operator or OMS and the supplier management system when making an explicit request. A communication link exists between the data warehouse and the supplier management system exists and is available. The supplier management system has authenticated the requesting operator or OMS. Archived data is accessible to the supplier management system. The data warehouse is able to store the new files (no obvious memory limitations). The supplier management system supports a scheduling function. Every record transferred in a single execution of bulk transfer function shall have the same data structure. After export, all exported data may or may not be deleted from the source location. If deletion of log records is expected, operator requested export should be possible only for special operator groups (authenticated) and this is handled by the OMS. If a scheduled transfer is desired, a schedule to be used in conjunction with the transfer has been established. Details of the file format are outside the scope of this use case.

Actors: Data warehouse, operator, BPON NE, OMS.

Preconditions: Archives have been established within the supplier management system and data has been stored in the archives.

Description: This use case begins when the operator or OMS schedules the routine retrieval of archived data within the supplier management system on the BPON NE. The request includes reference to a previously determined schedule, identifies the archive and provides security credentials to the data warehouse and a file name to be used when the supplier management system transfers the data within the archive [unknown record set, unknown scheduler, unknown destination server, invalid scheduler]. At the trigger of the clock, the file transfer process is initiated.

The operator or OMS may also make a request for the immediate file transfer of records within an archive of the supplier management system supplying the same reference material as before but without mention of the schedule [unknown record set, unknown destination server].

The supplier management system performs the following sequence of activities as part of the file transfer process:

– The data records are grouped together into a file following a data transfer format pre-defined by operator and supplier agreement. The format conventions cover the use of delimiters, file header structure, file trailer structure. If the transfer data is found within a BPON NE, this step is accomplished within the BPON NE by request of the supplier management system. This file is created at the time trigger, whether or not this time trigger is derived from a schedule or on-demand by the OMS.

– The supplier management system uses file transfer protocol mechanisms to establish a connection with the data warehouse using the supplied security credentials.

– The supplier management system then writes the file to the file name provided [comm failure].

– The supplier management system determines when the transfer is complete. It relies on file transfer protocol mechanisms to confirm that the transfer was successful.

– Throughout, the supplier management system records the status of the transfer process by providing updates to the transfer tracking object that was created within the supplier management system with the original transfer request.

– The supplier management system forms an activity completion record and logs the success or failure of the transfer in an activity completion log.

At any time before completion of this process, the operator or OMS may check on the status of the transfer [unknown transfer process]. It is also possible for the operator or OMS to investigate the history of all file transfer requested or scheduled.

Later, the OMS or operator may modify the schedule for the transfer of data from a particular archive. The OMS or operator formulates a request including reference to the existing scheduled activity and the new schedule to be applied [unknown transfer process, unknown scheduler, invalid scheduler]. The OMS or operator may also cancel the routine transfer of data from an archive [unknown transfer process]. If the activity is in progress, it shall be allowed to complete prior to cancelling of subsequent file transfer from that archive. The transfer tracking object is deleted from the supplier management system automatically upon cancellation of the scheduled process or with completion of an on-demand file transfer.

This use case ends when all immediate file transfers have been completed and the OMS or operator has cancelled all scheduled file transfers.

Exceptions: Unknown record set, unknown scheduler, unknown destination server, unknown transfer process, invalid scheduler.

Post-conditions: The supplier management system no longer routinely transfers archived data to the data warehouse and no transfer tracking objects exist within the supplier management system.

6.2.2.6 Collect NE statistics

Summary: The supplier management system shall provide for the collection of history data records from the BPON NEs, including both performance and traffic monitoring statistics. This collection shall be timely and occur before requested records can be over-written by the BPON NE. This function supports OMS or operator data collection from the supplier management system.

Assumptions: Performance or traffic monitoring and reporting has been activated by the operator or OMS for at least one monitoring point on a BPON NE within the management jurisdiction of the supplier management system. Monitoring on the BPON NE is accomplished through a register for every monitoring point. All registers for the same interval are initialized at the same time throughout the BPON NE (intervals may be 5 minutes, 15 minutes or 24 hours in length).

Each type of collectable history data record is defined by the operator and associated with a specific monitoring interval length and monitoring point. Interval start times are determined by the supplier management system. A statistics archive has been created and initialized by the operator (or via supplier management system default setting) to hold each type of collectable history data record. Archives are constructed to only accept records of the same type (e.g., DS1PMHistoryData or DS3PMHistoryData) involving the same monitoring window length.

If performance reporting has been requested by the operator for a particular monitoring point (via the use case called "performance and traffic monitoring reporting control"), a record showing the values for the counters or gauges is created at the end of the monitoring interval in the BPON NE and is available for collection.

If the collection of history data records is triggered by a customer complaint, then the supplier management system executes the retrieval of pertinent history data records as a separate process in order to tag each record with the service instance Id.

Actors: BPON NE.

Preconditions: All required history data records have been formed on the BPON NE.

Description: This use case begins when the clock indicates that another collection interval has been begun. The supplier management system systematically communicates with each BPON NE and retrieves all available history data records for the monitoring points and time interval specified by the operator or OMS. In the case of collection triggered by a customer complaint, the service instance Id is added to the history data records collected because of the customer complaint.

If the communication channel between the supplier management system and the BPON NE is interrupted, the supplier management system attempts several times to re-establish communications and complete the retrieval of all history data records [comm failure]. The supplier management system classifies and stores the records in the short-term archive that holds the same record type. The supplier management system forms an activity completion record and logs the success or failure of the transfer in an activity completion log.

This use case ends when the scheduled collection interval is ended.

Exceptions: Comm failure.

Post-conditions: BPON NE historical performance information is available for subsequent viewing by the operator and for bulk transfer to other file servers. The supplier management system archives the resulting information with other records of the same type awaiting the bulk transfer to the operator data warehouse.

6.2.2.7 Conduct test and report results

Summary: The supplier management system shall participate as required in any operator or OMS directed testing procedure including, but not limited to, ATM OAM cell loopback testing, interface loopback set-up on subscriber cards or OLT network interface cards, self test, metallic drop test, MAC layer test, draw dialtone break dialtone, and ATM continuity checks.

Assumptions: The supplier management system has authenticated the requesting operator or OMS. The supplier management system communications channel to the NE is working. The supplier management system is ready to receive commands from an operator or OMS. Supplier management system communications channel to operator or OMS is working. The test performer or test device of the NE is working. Tests are sequential. The NE has capabilities to conduct the test. This use case can conduct tests to assess hardware functioning. This use case can also conduct test scenarios in order to address customer complaints of service failures. The OMS or operator constructs various test sequences to address diagnostics for specific detected or reported failure conditions.

Actors: Operator, BPON NE, OMS.

Preconditions: BPON network resources tested by this functionality have been installed and provisioned. In the case of service level testing, service has been provisioned and activated as well.

Description: This use case begins when an operator or OMS receives a customer complaint or detects the failure of a BPON network resource. The operator or OMS constructs a test request. Types of tests requested include physical level tests, logical level tests and service level tests.

Physical level tests include the following: voice frequency, quality of data transmission, multimeter test, signalling test, loop test, wideband test, power on self-test and on demand self-test. Logical level tests include the following: ATM cell continuity check and ATM cell loop back. Service level tests include protocol tests, MAC layer test, metallic drop test, draw dialtone break dialtone test and service level loopback.

The supplier management system executes the following steps:

– identifies the tests requested [unknown test, invalid test operations, invalid timeout period];

– identifies the BPON resource to be tested and ancillary BPON resources that must participate in the test [unknown NE, unknown managed entity, not available for test, unknown service instance];

– prepares the resources for the test (engages the test performer or device of the NE);

– executes the test sequence in collaboration with the NEs [comm failure, invalid test operations, invalid start time, invalid stop time, invalid direction, invalid location Id, invalid timeout period];

– collects the results of the test; and

– reports the results of the testing promptly to the requester.

If the test is of sufficient duration (e.g., interface port loopback tests) and the test is viewed to be controlled, the supplier management system supports test interruption from the requesting party and reporting of interim test results [unknown test].

Tests may be triggered by the clock as a scheduled activity [unknown scheduler, invalid scheduler, invalid timeout period, invalid test operations]. In this case, the test reporting process retains test results, grouping it with other test results and logged for viewing by the operator at a later date. The OMS may modify the schedule for a test or even cancel a regularly scheduled test on a managed resource [unknown scheduler, invalid scheduler, unknown test, uncontrolled test in progress].

If the supplier management system receives test requests to occur on the same managed resource at about the same time, the first scheduled or requested test is executed and the others generate a conflict report that is logged [not available for test].

This use case ends when the test completes execution and results are reported to the requesting OMS and logged in an activity completion log. Operators can retrieve historical test result by managed entity or service instance [unknown managed entity, access denied, unknown test, unknown service instance].

Exceptions: Access denied, comm failure, invalid test operations, invalid start time, invalid stop time, invalid direction, invalid location Id, invalid scheduler, not available for test, unknown managed entity, unknown NE, unknown test, invalid timeout period, uncontrolled test in progress, unknown scheduler, unknown service instance, unknown test, invalid timeout period.

Post-conditions: An operator or OMS has more information with which to resolve the complaint of a customer or to support a maintenance activity.

6.2.2.8 Control archives

Summary: The supplier management system provides the functionality to manage logs for specific groups of events. The privileged user can create, initialize, suspend, resume, purge and remove event logs. The supplier management system also provides the functionality to query the status of a log.

Assumptions: The supplier management system has authenticated the requesting operator or OMS. The supplier management system supports logs and short-term statistics archives. Only a privileged user has permission to create, initialize, suspend or resume archiving. Access control for the user has been verified prior to this use case. There are memory resources available on the server hardware supporting the supplier management system. The supplier management system tracks the status of logs and archives and provides a notification if a threshold related to the fill status of the log or archive is crossed. A communication link exists between the privileged user and the supplier management system.

Actors: Privileged user.

Preconditions: The privileged user is authenticated and a working session is established with the supplier management system.

Description: This use case begins when the privileged user initiates a request to create a log or short-term archive that is not one of the standard archives installed with the supplier management system application.

In case of log creation, the creation request identifies a filter defining the entrance criterion for an event in the log, log maximum size, full action (wrap or stop recording), a threshold to determine log full condition and action to be performed in case of log full [record set exists, duplicate user label, access denied].

In the case of performance or traffic statistics recording, the creation request identifies the type of history data record, the maximum size (in terms of record count), and a user label for identification [archive exists, duplicate user label].

After the creation of the log or statistics archive record set, the operator can change the user label of the record set or query its status [unknown record set]. The user can also suspend recording of new records into a particular record set or resume recording that had been previously suspended [unknown record set]. At any time the privileged user can purge an archive [unknown record set]. The privileged user can also delete any record set that was not automatically installed with the supplier management system application [unknown record set].

This use case ends when an archive is created, modified or deleted.

Exceptions: Record set exists, unknown record set, duplicate user label.

Post-conditions: A record set is created, re-named or deleted. Recording to the record set may be active or suspended.

6.2.2.9 Download and activate NE software

Summary: The supplier management system provides for the download, distribution, installation (commit) and activation of software generic programs, software upgrades and software maintenance changes (patches) to BPON NEs based on request of the operator or OMS. The supplier management system can accept requests for one or multiple BPON NEs at once.

Assumptions: The supplier management system has authenticated the requesting operator or OMS. The destination within the BPON NE for software download is free to accept downloaded software (e.g., no backup in progress). There are no outstanding alarms on BPON NE components involved in software download (e.g., control card operational or other NE components involved in software propagation). Supplier management system supports software version control. The communication between supplier management system and OLT is functional at the beginning of the use case. The communication channel between the OLT and the secure software file server is functional at the beginning of the use case. Before establishing an NE software download activity, it is assumed that the software set is available and tested.

Until software is successfully loaded, propagated and activated, the formerly "active" version stays active. Software version control functionality is available. The supplier management system shall be able to support requests for software download, commitment and activation for a single instance and/or all instances of ONTs, ONUs or NTs subtending from one or all PON interfaces on one or more OLTs. The supplier management system shall be able to support requests for software download, commitment, and activation for a single instance and/or all instances of a particular card type for one or more OLTs. The activation of software on the OLT and ONU shall not be service affecting. If the activation of software on the ONT or NT is service affecting, the activation period is expected to last less than a few seconds.

Actors: Operator, OMS, BPON NEs, secure file server.

Preconditions: The software set is loaded onto the secure file server.

Description: This use case begins when the operator or OMS makes a request to the supplier management system to load (and eventually activate) new software for the BPON NEs. The request includes a reference to the location of the software set to be downloaded and the target destination(s) of the download. The target destination can be specified at the BPON NE group level, the BPON NE level or at the circuit pack level depending on supplier implementation and operator agreement. The request can include a reference to a start time for download and/or activation if the intent of the OMS or operator is to plan the NE software activity. The supplier management system verifies the use of the software through software version control [unrecognized target, insufficient memory, software load HW mismatch, unknown software load, timeout, invalid start time]. Any request for downloading software generics is accompanied by security credentials whereby the supplier management system is allowed to communicate with the source server.

The supplier management system then coordinates OLT access to the new software to be loaded, consulting the schedule or via on-demand request. The OLT downloads the software from the secure file server, applies the software to the target destination(s) and verifies that the delivery process has not introduced any errors to the software load [source unreachable, comm failure, insufficient memory, timeout, denied access, equipment failure].

The supplier management system returns a tracking object Id to the request that can be used to commit, activate, revert, get status, cancel and retrieve a list of software administration activities. The lifecycle of tracking object must extend until all associated activities are completed successfully or unsuccessfully. The object is only deleted after a pre-defined retention period and the length of time of the retention period is agreed outside the scope of this interface. The retention period for the tracking object should be generous enough to include any revert activity desired. If the tracking object has been automatically deleted by the supplier management system, then revert activity is viewed as download activity of a previous software load. The OMS can also delete this tracking object before its automatic termination if desired [unknown software download tracking object, software tracking object in use].

The software is not initially loaded to an active segment of the target destination. The software is then committed, i.e., made executable [installation failure, unknown software download tracking object, unrecognized target]. Then the software is activated by the operator or OMS [unknown software download tracking object, software not yet installed, activation failure, unrecognized target]. The supplier management system shall support both manual and automatic commitment and activation of successfully downloaded software.

At each step of the NE software download process, the supplier management system shall update the status information associated with the tracking object. The supplier management system shall also provide a real-time notification as well as log the success or failure of these procedures in an activity completion log. Whether the download is successful or not, the supplier management system supports operator and OMS queries concerning the status of the download, distribution, commitment and activation process.

The operator (or OMS) shall be able to cancel NE software download activities prior to their initiation [unknown software download tracking object, activity completed, activity in progress].

Exceptions: Software load/hardware mismatch, installation failure, activation failure, unknown software load, source unreachable, unrecognized target, comm failure, equipment failure, software not yet installed, insufficient memory, activity completed, timeout, activity in progress, denied access, unknown software download tracking object, invalid start time, software tracking object in use.

Post-conditions: The BPON NE shall function using its new software load.

6.2.2.10 Log events

Summary: The supplier management system stores event information in a log based on the filter defining the log. It makes the contents of a log available to a transfer function for scheduled bulk transfer.

Assumptions: It is possible to construct filters to describe the contents of logs within the supplier management system. Operator can create these filters, modify the filters when needed and delete them when they are no longer needed. A set of default filters is attached to the individual log file and, when not defined, the default is no filtering. Log maintenance is handled by other use cases (control archiving and bulk transfer). In other words, logs are created, initialized, and cleared via other supplier management functionality. Only privileged users are allowed to create filters that define logs archived within the supplier management system.

Actors: There are no external actors.

Preconditions: An event has been processed by the supplier management system and a record formatted as result of that processing.

Description: This use case begins when the supplier management system has processed an incoming event and formatted the resulting event record. Important events include but are not limited to the following: alarms, alarm clearings, threshold-crossing alerts, protection switching events, circuit pack removals and insertions, creation or deletion of managed entities, changes to key state and status variables, and scheduled or time-consuming activity completions.

The processed event record is examined to see whether or not the record data matches any of the filter constructs defining the contents of any of the logs created and initialized for the supplier management system [event flood] (the filters determine which events are to be added to specific event logs). If the event record does not match any filter, the event information is discarded. If the event record does match a specific construct, the event record is stored in the relevant event log. If the log is not full, the event record is written at the end of the log. If the log has been configured as a "wrap around" log, and the log is full, the event record overwrites the oldest record in the log. If the writing of the event record causes a logFull condition, then a notification is prepared for forwarding to an external event channel [out of memory].

Exceptions: Out of memory, event flood.

Post-conditions: The log is available for viewing by the OMS or operator. The contents of the log are available for bulk transfer to another file server called a data warehouse.

6.2.2.11 Manage profile objects

Summary: Once a profile object has been created in the profile object repository, the supplier management system can process event information stating this fact and make the profile object settings available for use by any use case of the supplier management system. This functionality includes the ageing out and deletion of these profile settings.

Assumptions: The supplier management system has authenticated the requesting operator or OMS. The supplier management system maintains information on the syntax and permitted range of values for parameters for each profile type that it recognizes. Supplier management systems participating in this use case are instances of the same supplier application. The operator has determined which supplier management systems are interested consumers for event information. This assumes that the profile object type can be referenced and employed by the supplier management system. As required, management communications network links exist to support the publishing of profile object creation/deletion messages to the external event channel. Through an external specification process beyond the scope of this use case, the profile object repository is knowledgeable about valid values for profile object attributes. One or more profile object repositories may exist.

Actors: OMS, operator, external event channel, BPON NEs.

Preconditions: A supplier management system is installed and has registered as a consumer of profile object creation and deletion notifications.[4]

Description: This use case begins when a profile object is created in the profile object repository and published to the notification channel on external event channel. The message from the notification channel is consumed by the supplier management system. The message includes the name and type of the profile. It also includes the attribute value listing for the specific values of the profile object instance. The supplier management system stores the profile name and attribute values. In some circumstances, this may mean that the supplier management system writes this

[4] If creation of the profile object occurs prior to the instantiation of the supplier management system, then the supplier management system obtains its attribute values by query to the profile object repository [unknown profiles]. The supplier management system writes this profile name and attribute values to the NEs within its management jurisdiction. The profile object settings are now available for use by an operator or OMS when interfacing with supplier management system.

profile name and attribute values to the NEs within its management jurisdiction. The profile object settings are now available for use by an operator or OMS when interfacing with supplier management system.

The supplier management system supports the inquiry by an operator or OMS if a particular profile is in use in the management model under the jurisdiction of the supplier management system. The query includes the name of the profile object [unknown profiles]. The supplier management system supports the re-naming of any known profile [unknown profiles]. The supplier management system also supports the ageing out of use of a particular profile object by request of an operator or OMS [unknown profiles]. In this case, the supplier management system prevents subsequent use of the named profile object by any external or internal interaction. The operator or OMS can also request the resumption of use of a profile object [unknown profiles].

The supplier management system also supports deletion of all references to a particular profile object instance. A deletion request includes the name of the profile object [unknown profiles]. The supplier management system verifies that no use of the profile object is being made by any managed entity within its domain of management [profile in use]. This verification is accomplished by checking the management model. The supplier management system deletes all reference to the profile object within its application and on the network resources it is managing.

This use case ends when the profile object parameters have been created, aged out or deleted in the supplier management system.

Exceptions: Duplicate profile name, unknown profiles, profile in use.

Post-conditions: At the end of its lifecycle, the profile object is unavailable for use by any supplier management system. Prior to that point, the profile object is available for use by an operator or OMS when interfacing with the supplier management system provided it has not been discontinued from use by an ageing out request of the operator or OMS.

6.2.2.12 NE software version control

Summary: The supplier management system tracks the version and update status of BPON NE software and records this information in a repository accessible by the operator or NML system. The software version control validates the to-be-downloaded software version against the saved version number, and raises exception for invalid to-be-downloaded software version. The operator can view the software version information in the repository.

Assumptions: The supplier management system has authenticated the requesting operator or OMS. The supplier management system has a repository set up to store BPON NE software version information. The supplier management system has built-in algorithms, or rules for version control. The repository is large enough to hold hardware and software version information for all BPON NEs within its engineered management domain.

Actors: Operator, OMS and BPON NE.

Preconditions: A new version of NE software is due to be downloaded or a new BPON NE has been installed and registered with the supplier management system or a new plug-in unit has been inserted.

Description: This use case begins when an NE software download is requested or when a new BPON NE has been installed in the network and autodiscovery has taken place. In each case, the supplier management system retrieves the current software and hardware version information from the BPON NE and updates (if necessary) the information within the software control repository for the NE memory area(s) [comm failure]. It determines if the version of software in the download request matches the rules or algorithmic checks implemented within the supplier management system for the corresponding hardware version. It provides notification of mismatch or match to the requesting internal process. As the NE software download process continues, the supplier management system continues to update the software hardware version information in its inventory.

In the case of newly installed BPON hardware, the supplier management system determines if the current software load of newly installed hardware can be upgraded to the release being used throughout the administrative domain and automatically upgrades the new hardware with the current release and, again, updates its version release inventory.

In all cases the supplier management system can respond to OMS or operator queries concerning the current release of software installed on a BPON network resource as well as whether or not a specific BPON network resource can support a particular software release [unknown managed entity, unknown NE].

This use case ends when hardware and software release information has been updated in the supplier management system inventory.

Exceptions: Unknown managed entity, unknown NE, comm failure.

Post-conditions: The version information of BPON NE software is updated and accessible to the operator and OMS.

6.2.2.13 Performance and traffic monitoring reporting control

Summary: The supplier management system shall provide for the activation and deactivation of performance data or traffic measurements collection on individual termination points contained in the BPON NEs as required by the operator or OMS. This use case also includes the setting of threshold values and describes automatic reporting of performance measurements when thresholds have been crossed.

Assumptions: The supplier management system has authenticated the requesting operator or OMS. Hardware and software support for monitoring of all performance and traffic parameters defined in the current data and history data managed entities of [ITU-T Q.834.1] is available. Current data is not directly controlled by OMS. Hardware and firmware support for performance and/or traffic monitoring at all BPON NE monitoring points have been initialized and activated and counters and gauges are operational. The communications channels between the BPON NE and supplier management system and between the supplier management system and the operator or OMS are working. The supplier management system has verified that the operator or OMS has permission to establish threshold values and/or to request the collection of statistics from the BPON NEs.

The supplier management system can hold up to one week of history data records collected from the BPON NEs within its management domain. The BPON NE can retain historical parameter values for at least one collection period beyond the recording of the data. The ultimate short-term archiving capability for performance and traffic records in the BPON NE is a matter for determination through explicit operator requirements and is not in the scope of this use case. Performance monitoring points of BPON NEs support the raising of threshold crossings alerts based on the setting of threshold values.

Actors: Operator, OMS and BPON NE.

Preconditions: Based on customer complaints or other trouble-shooting or maintenance needs, the operator decides to change the setting of threshold data values or wishes to collect performance and traffic measurements from BPON NEs.

Description: This use case begins when the operator or OMS establishes or modifies values for thresholds for monitored performance or traffic measurements for certain termination points within a BPON NE. The operator or OMS sends a request to the supplier management system indicating the monitoring point(s) of the BPON NE, identification of the monitored parameters, and associated threshold values to be used in the detection of threshold crossing event [unknown NE, unknown managed entity, unknown profiles, invalid association, comm failure, profile suspended]. The supplier management system transfers each of the threshold values to the identified BPON NE for use at the associated monitoring point. The request process includes the opportunity for the operator to make a default setting assignment for a system-wide threshold value for each monitored parameter type within an entire BPON subnetwork [unknown NE, unknown managed entity, unknown profiles, invalid association, comm failure, profile suspended, unknown monitoring point types].

The BPON NE continues its constant monitoring of performance at each monitoring point for each counter, resetting each measurement to zero at the end of the monitoring interval associated with the counter. There can be 5-minute, 15-minute and 24-hour counters in the BPON NE. Monitoring intervals are automatically established and applied on a uniform basis across all monitoring points of the BPON NEs within the management domain of the supplier management system as each BPON NE is added to the management domain of the supplier management system.

The BPON NE uses the threshold value to autonomously alert the supplier management system whenever the counter associated with the performance parameter falls out of the acceptable performance range indicated by the threshold value. TCA event processing by the supplier management system triggers (in part) the automatic retrieval of the history data record associated with the TCA event by the supplier management system. The history data record is archived with other records of the same type associated with TCA events and awaits the bulk transfer to the operator data warehouse.

Based on a customer complaint, the operator or OMS can request the collection of history data records for a selection of monitoring points for limited periods of time. The request includes the identification of the BPON NE and monitoring points, the history data records to be collected, the start time for collection, the collection window length and the service instance Id associated with the complaint [unknown managed entity, collection period past, unknown service instance Id, unknown NE]. The supplier management system notes the monitoring points and monitoring collection intervals and collaborates with the containing BPON NE to enable the subsequent reporting of performance parameter values for each of the collection intervals for each monitoring point [collection limitation].

The operator or OMS may also request the routine collection of certain history data records from BPON NEs or may request the termination of routine collection. The request made to the supplier management system identifies the monitoring point type and history data type [unknown history data type, invalid association, unknown scheduler, invalid scheduler, unknown NE]. The supplier management system notes the monitoring points and collaborates with the containing BPON NE to enable the subsequent reporting of performance parameter values for every collection interval for each monitoring point, or to disable the subsequent reporting [collection limitation].

Based on trend analysis or traffic monitoring needs, the operator or OMS can also request the routine auditing (i.e., collection) of history data records. The request made to the supplier management system includes the BPON NE, monitoring point instance, history data record type and schedule to apply to the collection of the history data record identified [unknown managed entity, collection period past, unknown NE]. The supplier management system notes the monitoring points and monitoring collection intervals and collaborates with the containing BPON NE to enable the subsequent reporting of performance parameter values for each of the collection intervals for each monitoring point. In this case, reporting of zeroes is not suppressed [collection limitation].

The operator or OMS may query the supplier management system at any time to obtain a listing of reporting monitoring points and reporting intervals for each BPON NE.

This use case ends when threshold values have been established, modified or removed for all or selected monitoring points or when performance data collection schedules are established, modified or cancelled according to maintenance needs and service level agreement policies.

Exceptions: Collection limitation, unknown monitoring point, collection period past, unknown type, comm failure, unknown threshold data, invalid threshold data, unknown service instance Id, unknown BPON NE, reporting exists, unknown scheduler.

Post-conditions: The operator has set threshold data values for monitored parameters on the BPON NE and the NE will respond with a TCA if an impairment is detected. If the operator request involves the collection of history data records in the supplier management system, then these record sets are available for retrieval by the OMS or operator, or for bulk transfer to the data warehouses.

6.2.2.14 Process incoming NE events

Summary: The supplier management system processes event notifications from the BPON NEs within its management jurisdiction. The supplier management system identifies the event type and source, transforms and augments the data into an event record structure of potential benefit to upstream systems and users, and transfers the record into an internal repository accessible to other supplier management system functions.

Assumptions: The communications channels between the supplier management system and the NEs are working. The supplier management system is able to accept notification of all events from the BPON NEs within its domain of management. Events are time-stamped by the NEs with a consistent timing source. The supplier management system coordinates the time stamp mechanism between NEs.

Actors: BPON NE.

Preconditions: An event is detected by an installed BPON NE.

Description: This use case begins when an event notification arrives from a BPON NE at the supplier management system event channel. Upon receiving an NE event the supplier management system uses a soak period to screen event transients (e.g., toggling alarms). This is distinct from the soak period used by the NE to determine that the situation should be reported as an alarm. The supplier management system perceives the event (i.e., it screens the source of the event and verifies that it is interested in the event) [corrupted event data, incomplete event data, unauthorized source]. The supplier management system shall discard any event according to a set of business rules including, but not limited to, the elimination of "toggling" events and congestion conditions on the input event buffer (persistency analysis on the event may also have occurred on the NE). The supplier management system further identifies the event. The list of event types consists of alarms (including threshold crossing alerts), attribute value changes (including protection switching events and state changes), and network resource creation and deletion notifications.

The supplier management system may add data to the NE event information according to business requirements provided by the network operator [unable to add required enhancements]. For example, in the case of alarm events, the supplier management system may correlate alarm information to service instances supported by the managed entity in failure condition and add the identification of affected services to the event notification. The addition of the data could involve consultation with the management model in the supplier management system in order to determine if a service outage has occurred and the assignment of alarm severity, if this characteristic has not already been provided by the NE.

This use case ends when the supplier management system makes the enhanced information accessible to other internal functions by putting it in an event queue.

Exceptions: Corrupted event data, incomplete event data, unauthorized source, unable to add required enhancements.

Post-conditions: The functions "autodiscover NE and plug in units", "root cause alarm analysis", "root cause impairment analysis", "provide current event summary listings", "maintain management model" and "log events" are able to consume properly formatted event records.

6.2.2.15 Provide current event listings

Summary: The supplier management system will provide access to information showing the current value of key status and state parameters and group this information in a listing for perusal by the operator. The listings are continuously and autonomously updated by the supplier management system based upon ongoing events within the BPON NEs.

Assumptions: The supplier management system has authenticated the requesting operator or OMS. Lists are limited to information concerning failure conditions and trouble-shooting within the BPON NEs. This functionality includes, but is not limited to the following: current alarm summaries, listing of successful and unsuccessful protection switching events where the protected unit is no longer the active one, service instances currently experiencing a service outage, termination points in loopback mode, or managed entities whose administrative state is "locked".

The supplier management system can process incoming BPON NE and GUI interaction events. The supplier management system can correlate events and service information, can conclude that a service outage exists for a particular failure condition (considering all affecting conditions like protection switching events and that a service has indeed been provisioned), and can correlate protection group provisioning information with protection switching events. Events can come from BPON NEs or operator interaction. It is a matter for supplier implementation and operator requirements which current event listings are supported.

Actors: Operator, BPON NE, privileged user.

Preconditions: Current listings and event queues have been initialized as part of the installation of the supplier management system.

Description: This use case begins when events of interest are detected at the BPON NE and event information is set to the supplier management system. The supplier management system examines events indicating changes in state and status. If the variable is one tracked for a current summary event listing, the listing is consulted. If the event indicates the start of a tracked condition, information concerning the managed entity associated with the event and attribute is added to the listing along with a timestamp of the event, provided the condition is not outstanding already. If the event indicates the end of a tracked condition, the listing is consulted and the most recent listing entry concerning the start of the condition is removed. Listings summarize conditions on a BPON system basis.

The listing is always accessible to view by the operator through a graphical user interface. Changes to the listing happen autonomously without the need for operator refreshing of the screen. Desired modes of presentation of the listing are determined via operator system requirements.

Operators with privileged status are allowed to resynchronize current summary event listings. Based on operator request, the supplier management system retrieves the current value of the state, status or management attribute tracked by the current summary event listing for the BPON system for any managed entity contained in the system that possesses the characteristic attribute [comm failure, DCN timeout, unknown NE, equipment failure, timeout]. If the BPON system retrieval process shows that the listing is not up-to-date with the current conditions of the system, then the listing is modified (through deletion of an entry or insertion of a new entry) in order to correct the listing.

Listing entries are correlated with information retrieved from the system via the identifier of the managed entity. Deletion of an entry can occur if a listed managed entity no longer exists contained within the BPON system, or if a failure condition or test has ended and the system has reverted to normal functioning. If either of these situations occur, all entries concerning the same managed entity are removed from the listing. Insertion can occur when no listing entry exists for a managed entity now indicating a change in functioning.

This use case ends when the listing has been properly updated.

Exceptions: Comm failure, DCN timeout, unknown NE, equipment failure, timeout.

Post-conditions: Accurate current event list information is accessible to the operator and OMS.

6.2.2.16 Provision installed NEs

Summary: Installed BPON resources are provisioned with configuration settings in anticipation of service provisioning.

Assumptions: The supplier management system has authenticated the requesting operator or OMS. Management communications between the supplier management system and the installed BPON resource is operational. In the case of the OLT, this means that the OLT has been registered. In the case of an ONT or ONU, this means that the ONT or ONU has been ranged. In the case of an NT, this means that the upstream ONU has been ranged and that management communications exists between the NT and ONU. Configuration settings may (or may not) have been previously supplied to the supplier management system.

Actors: BPON NE, operator or OMS.

Preconditions: A BPON NE has been installed and is under the management jurisdiction of the supplier management system.

Description: This use case begins when the operator or OMS undertakes to provision the installed BPON network resource. BPON resources include BPON NEs (OLT, ONT, ONU, NT) and/or plug-in units. The autodiscovery function provides the supplier management system with inventory data describing the type of equipment installed. The supplier management system automatically "builds" the BPON resource in the management model.

If the information constructed in the management model matches inventory data supplied previously to the supplier management system (through a set of "pre-provisioning" build transactions from the operator or OMS), the supplier management system automatically applies to the installed resource any additional configuration settings supplied via the previous transactions. If the information constructed in the management model does not match inventory data supplied previously to the supplier management system, the supplier management system prepares one or more event records to notify interested consumers of the mismatch.

If no previous "pre-provisioning" build transactions have taken place, the operator or provisioning OMS formulates a set of provisioning build requests identifying the discovered BPON resource and providing configuration settings necessary to prepare the BPON resource for use in service provisioning.[5] The supplier management system applies these settings to the identified BPON resource and updates the management model appropriately.

This use case ends when provisioning information has been transferred (as needed) to the pertinent network resources by the supplier management system.

Exceptions: See clause 6.2.2.4 exceptions.

Post-conditions: The installed BPON resource is available for service provisioning and activation management operations.

6.2.2.17 Provision service

Summary: The supplier management system selects ports, facilities and bandwidth from BPON resources determined to be available in order to complete the design, selection and assignment process associated with a set of services for a particular customer. Activation of network resources occurs simultaneously provided immediate activation is required. A service is

[5] Details covered in clause 6.2.2.4.

defined as a connection between an UNI endpoint on an ONT and an NNI endpoint at an OLT, or between UNI endpoints on two ONTs subtending from the same OLT.

Assumptions: The supplier management system has authenticated the requesting operator or OMS. The OLT is registered with the supplier management system. The PON interface plug-in unit on the OLT may or may not be installed. In any case, the PON port has been provisioned. The ONT may or may not be installed. ONT resources have been provisioned if not installed. An operator or provisioning OMS selects the endpoints. The provisioning OMS or operator have access to the valid/permissible range of VPI/VCI values for the NNI and UNI interfaces. The communications channel between the supplier management system and OLT is up at the start of the use case. Resources may or may not have been reserved prior to this use case for the service connection.

Actors: OMS, operator, BPON NEs.

Preconditions: A service request has triggered the need for a connection between an UNI endpoint on an ONT or NT and an NNI endpoint on an OLT or between two UNI endpoints of ONTs subtending from the same OLT.

Description: This use case begins when the OMS or operator sends a service connection set up request to the supplier management system. The request includes a service instance identifier, identifiers and characteristics for the endpoints (i.e., VPI and VCI values for ATM endpoints), a reservation Id (if relevant), administrative state value, and profile pointers that characterize the service connection desired. The supplier management system validates existence of the end points, identifiers and profiles [unknown NE, unknown profiles, unknown port, profile suspended, connection already exists]. It checks to see if the VPI/VCI values are in use and are valid [parameter violation]. It checks to see if resources have already been reserved [unknown reservation Id]. The supplier management system also validates that required network resources exist to provision this service if resources have not been reserved and applies appropriate configuration requests to the BPON NEs if they are already installed [insufficient BW, connection count exceeded, comm failure, equipment failure, insufficient PON BW]. Whether or not the BPON NEs are installed, the supplier management system updates its own management information model following rules derived from [ITU-T Q.834.1]. The supplier management system generates a subnetwork connection Id to describe the service connection and returns this value to the OMS or operator.

At some later point, it might be necessary to modify the traffic or service characteristics describing the connection. In this case, a modification request is made from the operator or OMS to the supplier management system that includes the subnetwork connection Id [unknown connection], port A Id [unknown port] and a listing of service profile names and new network profile names [unknown profiles, profile suspended]. The supplier management system validates that required network resources exist to provision this service change (e.g., bandwidth over the PON and on the designated network interface) [insufficient BW] and applies the new traffic profile characteristics to the service connection [unknown profiles, profile suspended].

Based on customer request (extended absence) or failure to pay service charges, the OMS or operator may request the suspension of an existing service connection. In this case, the OMS or operator formulates a request including the service instance Id and the suspension time interval that is sent to the supplier management system for execution [unknown service instance, invalid start time, invalid stop time]. The supplier management system also supports the resumption of service based on the request of the OMS or operator if this is desired prior to the stop time of suspension or if the original connection request had administrative state set to the "locked" value [unknown service instance].

The operator or OMS may request the removal of a service connection. In this case, the deletion request includes the subnetwork connection Id. The supplier management system changes the configuration data on the BPON NEs [unknown connection, comm failure, equipment failure] as well as within its own management information model. The supplier management system also makes resources formerly assigned to the service available for use by any subsequent connection request, modifying managed entities tracking these resource values.

This use case ends when the service creation, modification, suspend, resume or disconnect request completes and relevant service provisioning information has been transferred to the pertinent NE(s) as they are installed.

Exceptions: Insufficient bandwidth, insufficient PON bandwidth, unknown port, unknown profiles, profile suspended, comm failure, equipment failure, unknown NE, connection already exists, connection count exceeded, parameter violation, invalid start time, invalid stop time, unknown service instance, unknown reservation Id.

Post-conditions: Connection information is available to be applied to installed BPON network resources, thus creating service availability for the requesting customer.

6.2.2.18 Publish event

Summary: On receipt of processed configuration, performance, or fault event information provided by other use cases within the supplier management system and based on rules concerning publication, the supplier management system queues and channels event information to all interested consumers.

Assumptions: Management communications channels are available between the supplier management system and interested consumers (users and systems) allowing the transfer of event information. The actual notification mechanisms are dependent on the communications protocol and can range from publishing, to specific event channels, to directing of event messages to individual consumers based on a discriminator construct filter. Details of the autonomous mechanisms are outside the scope of the use case. Operator business rules have been implemented in the supplier management system describing the event data that should be immediately transferred to upstream OMS(s) or operators. Relationships between event type and suitable notification channels have also been implemented.

Actors: External event channel.

Preconditions: The supplier management system is installed and is managing at least one BPON NE.

Description: This use case begins when, as part of its installation, the supplier management system establishes management communications mechanisms for the purpose of forwarding event information using agreed upon protocols [already connected]. Then the supplier management system becomes aware of the creation of an event record from an internal process. Event records can be created because of managed entity creation, managed entity deletion, alarms, threshold crossing alerts in performance monitoring, and attribute value changes, including, but not limited to, changes in state and status variables, circuit pack removal from slots, and protection switching occurrences.

The supplier management system applies business rules provided by operator requirements to determine whether or not the event record is of interest to any consumers. If the event record is not of interest to any consumers, it is discarded. If the event record is qualified for immediate transfer, the supplier management system provides the event record information to the notification forwarding mechanism implemented on the supplier management system that is specific to the communications protocol in use between the supplier management system and any interested event consumer [disconnected]. In some cases there may be multiple notification channels, in which case the supplier management system will also determine the channels to be used [invalid event type].

This use case ends when the event record has been successfully transferred to an external event channel.

Exceptions: Disconnected, already connected, invalid event type.

Post-conditions: The event information is available for use by the operator or OMS.

6.2.2.19 Range ONT or ONU

Summary: The supplier management system directs the OLT to range a subtending ONT or ONU.

Assumptions: The supplier management system has authenticated the requesting operator or OMS. The OLT has been installed and is equipped with a provisioned PON interface card. The DCN is working between the supplier management system and OLT. The OLT supports ranging as described in [ITU-T G.983.1]. The ONT or ONU has been installed and is equipped with power. There is an ODN connection between the OLT PON interface port and the ONT (or ONU). Ranging can be accomplished without required use of service demand information. The supplier's manufacturing process control prevents the possibility of duplicate serial numbers. The supplier management system may support rules concerning serial number syntax and the maximum number of subtending ONT or ONUs on any OLT PON interface card port.

Actors: Operator, OMS, BPON NE (OLT).

Preconditions: An ONT or ONU has been installed.

Description: This use case begins when the supplier management system obtains the serial number for a newly installed ONT or ONU. The serial number may be provided by a field installation technician or through an automatic protocol detection mechanism. If the serial number is provided by a technician, a ranging request for the ONT or ONU is formulated including identification of the OLT, the OLT PON port, the user label of the ONT or ONU, and the serial number itself. The supplier management system directs the OLT to range the new subtending ONT or ONU based on its serial number [comm failure, equipment failure, unknown NE, unknown port, max subtending nodes exceeded, insufficient PON BW, invalid serial num syntax, APON layer failure, duplicate user label, invalid user label syntax, backup in progress, synch in progress].

This ranging activity calculates the optical distance between the OLT and ONT/ONU, establishes security mechanisms, sets up the upstream time slot for the ONT/ONU, assigns an index number for the ONT/ONU, and establishes the VCC for the embedded operations channel between the OLT and ONT/ONU. The latter action establishes management communication between the supplier management system and the ONT/ONU. The supplier management system associates the ONT (or ONU) with an index number and returns the managed entity Id for the ONT. It also associates the user label supplied on the request with the index number and the ONT (or ONU) managed entity Id.

If the serial number is supplied through automatic ranging protocol mechanisms through the autodiscovery function of the supplier management system, then the OMS or operator either requests the association of pre-provisioned data to the freshly discovered ONT/ONU [unknown managed entity] or builds the ONT/ONU and then requests the association of provisioned data to the freshly discovered ONT/ONU [unknown managed entity]. In either case, the supplier management system associates the ONT (or ONU) with an index number, the user label, and the managed entity Id as before.

In case the ONT or ONU becomes defective, the supplier management system supports requests for replacement of ONTs/ONUs. In this case, the OMS or operator forms a request including the managed entity Id of the original NE, the new serial number for the replacement NE, and the new user label. The supplier management system processes the request, ranges the new ONT or ONU from the same PON port of the OLT, and applies existing service configuration data to the new ONT/ONU [comm failure, unknown NE, invalid serial num syntax, APON layer failure, equipment failure, invalid user label syntax, HW services mismatch, duplicate user label, backup in progress, synch in progress].

In case the service demand at the ONT or ONU location exceeds the capabilities of the existing NE, the supplier management system supports requests for the upgrading of the ONT or ONU. In this case, the OMS or operator forms a request including the managed entity Id of the original NE, a reference to pre-provisioning information for the new services, the new serial number for the replacement NE, and the new user label. The supplier management system processes the request, ranges the new ONT or ONU from the same PON port of the OLT, and applies existing and new service configuration data to the upgraded ONT/ONU [comm failure, unknown NE, invalid serial num syntax, APON layer failure, equipment failure, invalid user label syntax, HW services mismatch, duplicate user label, backup in progress, synch in progress, insufficient PON BW].

In case the service demand on a PON port reaches a threshold, then the supplier management system also supports requests for moving of the ONT/ONU from one PON port to another one. In this case, the OMS or operator forms a request including the managed entity Id of the original NE and the new PON port Id. The supplier management system processes the request, ranges the existing ONT or ONU from the new PON port of the OLT, and retains existing service configuration data associated with the ONT/ONU [comm failure, unknown NE, unknown port, APON layer failure, equipment failure, insufficient PON BW, backup in progress, synch in progress].

This use case ends when the ONT or ONU has been ranged successfully and all pertinent managed entities have been built in the supplier management system.

Exceptions: Comm failure, unknown NE, invalid serial num syntax, APON layer failure, equipment failure, invalid user label syntax, HW services mismatch, duplicate user label, backup in progress, synch in progress, insufficient PON BW, unknown port.

Post-conditions: The ONT or ONU is ready for further provisioning activities.

6.2.2.20 Register OLT

Summary: The management communications channel between the supplier management system and OLT is verified and the OLT is registered for management by the supplier management system.

Assumptions: The supplier management system has authenticated the requesting operator or OMS. The OLT is installed. The power supply is working. An operator-defined name (OLT user label) and DCN address (e.g., IP address) have been configured on the installed OLT via local craft interface or some factory provisioning mechanisms. Registration takes less than one minute. The DCN connection has been installed and configured. A check of DCN connectivity times-out from the supplier management system if no response from the remote end is received within 10 seconds. If privileged user status is required for the provisioner, access control mechanisms have been verified in advance of this use case.

Actors: Operator, OMS, BPON NE (OLT).

Preconditions: An OLT is installed, but not yet managed by the supplier management system.

Description: This use case begins when the OMS or operator requests that a supplier management system build a new OLT within its management domain. The request includes the DCN address associated with the OLT and an OLT user label. The request may also include references to operator administration domains. The supplier management system processes the request [duplicate user label, too many NEs, invalid user label syntax]. Invalid DCN address stores the address and label information and checks the DCN connection between itself and the OLT [DCN timeout, invalid DCN address]. The supplier management system establishes application layer to application layer communications between itself and the OLT and verifies this communication by retrieving the OLT user label [denied access, address label mismatch]. The supplier management system then assigns a globally unique OLTId (managed entity Id) to the OLT, thus exercising its role as manager of the OLT, and returns this assignment to the requesting OMS or operator.

Upon request of the OMS or operator, the supplier management system can change the DCN address of an OLT belonging to its management domain. In this situation, the request includes the managed entity Id for the OLT and the new DCN address. The supplier management system verifies the old DCN address, checks the DCN connection between itself and the OLT using the new DCN address, and verifies management capabilities by retrieving the OLT user label [denied access, address label mismatch, DCN timeout, comm failure, unknown NE, invalid DCN address, backup in progress].

It is also possible to remove an OLT from management jurisdiction of the supplier management system by making such a request [unknown NE].

This use case ends when the supplier management system has added the OLT to its domain of management and has established a management application association with the OLT.

Exceptions: Denied access, address label mismatch, DCN timeout, comm failure, unknown NE, invalid DCN address, backup in progress, duplicate user label, too many NEs, invalid user label syntax.

Post-conditions: As long as the OLT is registered with the supplier management system it is available for management by the OMS or operator through the supplier management system.

6.2.2.21 Report service outages

Summary: When a network outage occurs, the supplier management system should be able to detect it based on incoming alarms and events, identify affected services and BPON resources, generate service outage records and report the outage to the OMS or operator.

Assumptions: The supplier management system establishes a proper channel to receive incoming alarms/events. It also establishes the proper channel to the OMS to report possible outages. The supplier management system has the necessary information about the services and BPON resources that it manages. It also contains proper logic to detect outage and affected service/resources based on incoming alarms/events.

Actors: BPON NE.

Preconditions: The supplier management system is installed and maintains relationship information between network resources and service assignments.

Description: This use case begins when the supplier management system receives NE event information reflecting a possible network outage. The supplier management system proceeds with root cause analysis in an attempt to determine the fundamental cause of the failure. It also accesses events from the alarm event queue and protection switching event queue for the affected BPON NE in order to determine whether or not the failure condition is service affecting. If so, the supplier management system consults with the management model in order to identify the service instances that have been affected by the network outage and creates a service outage event record for each instance affected. Each service outage record shall include identification of the affected service, values of relevant state attributes, cause of outage, outage start time. The supplier management system posts the outage event record to a current event listing for such service outages. The OMS and operator can retrieve this information via an explicit request.

Later, when event information indicating the clearing of the network outage is received and processed by the supplier management system, the supplier management system removes the outage event information from the current listing, appends the outage stop time to the record, and records the enhanced record in a log on the supplier management system.

This use case ends when expanded outage record has been posted to the log.

Exceptions: None specified.

Post-conditions: Service outage records are available for retrieval by the OMS from the log.

6.2.2.22 Reserve resources

Summary: The supplier management system supports reservation of bandwidth pending installation of an ONT, ONU, NT or subscriber port in the ONT or NT for a particular OLT prior to the dispatch of personnel to the ONT, ONU or NT installation location. This function includes cancel and modification of resource reservation.

Assumptions: The supplier management system has authenticated the requesting operator or OMS. The supplier management system may support rules concerning the maximum number of subtending ONT on any OLT PON interface card port for the OLT. The supplier management system has an accurate view of current network resources for a specific OLT, including installed, assigned and reserved resources. CAC calculation capability is supported either by an installed OLT or by the supplier management system. Slot assignments do not change within this use case.

Appropriate DCN communications between the supplier management system, upstream OMS(s), and OLT are available as needed at the start of the use case. Reservation of bandwidth is supported on a per service instance basis (implying the eventual creation of a subnetwork connection).

Actors: Operator, OMS, BPON NE (OLT).

Preconditions: The OLT has been provisioned as well as the relevant PON interface slot and NNI slot and the OLT is under the management jurisdiction of the supplier management system.

Description: This use case begins when an operator or OMS receives a work order to install a new service where there is new ONT, a new ONU, a new NT or a new subscriber line card in an existing NT or ONT. The operator or OMS formulates a reservation of bandwidth request. The request includes a service instance identifier, identifiers and characteristics for the endpoints (i.e., VPI and VCI values for ATM endpoints), and profile pointers that characterize the service connection desired. The supplier management system validates existence of the end points, identifiers and profiles [unknown NE, unknown profiles, unknown port, profile suspended, connection already exists]. It checks to see if the VPI/VCI values are in use and are valid [parameter violation]. The supplier management system processes the information provided on the request and performs the following:

– accesses a CAC calculation mechanism to determine whether there is sufficient bandwidth in the OLT to admit the service [insufficient bandwidth];

– uses connection counts, grant bandwidth metrics and port line bit rate information to determine whether there is sufficient capacity on the OLT (includes ODN limitations) and on the prospective interfaces of the OLT to satisfy the service demand [max subtending nodes exceeded, connection count exceeded];

– reserves bandwidth, capacity and connections [comm failure] on the provisioned NEs;

– makes association of reserved resources to service instance Id;

– provides the reservation Id to the requesting operator (or provisioning system) as identification for the reserved resources.

The operator or OMS makes requests until reservation of all resources in the OLT required for the installation of services for the specific customer served by the ONT, NT or port/circuit pack is finished.

The supplier management system shall also support requests by the operator provisioning OMS to cancel reserved resources. The operator or OS references the reservation Id with the cancel request [unknown reservation Id]. The supplier management system releases all network resources whose reservation is tagged by the reservation Id.

The supplier management system shall also support retrieval of a reservation Id given a service instance Id value or the retrieval of a service instance Id given a reservation Id originally provided with a successfully completed reservation request [unknown service instance, unknown reservation Id].

The supplier management system can report on reserved, assigned and available bandwidth per port on request of the OMS or operator [unknown NE, comm failure]. The supplier management system can also report on the amount of bandwidth reserved for a particular reservation [unknown reservation Id].

This use case ends when reservation of bandwidth, connections and other capacity metrics is completed and reservation information has been transferred as needed to the pertinent NE(s).

Exceptions: Unknown NE, insufficient bandwidth, max subtending nodes exceeded, connection count exceeded, duplicate service instance Id, unknown service instance, unknown reservation Id, comm failure, unknown profiles, profile suspended.

Post-conditions: Bandwidth, connections and capacity are marked as "reserved" in any subsequent capacity inventory reporting and dedicated for future provisioning activities for the identified service instance.

6.2.2.23 Root cause alarm analysis

Summary: When there is an occurrence of a set of alarms associated with a single failure condition, the supplier management system shall analyse and correlate the alarm events within its domain to the best of its ability and determine the underlying root cause of the problem. It prepares an alarm record for the root cause failure condition for forwarding to OMS(s) and operators. If root cause is not determined, the supplier management system prepares a set of alarm records for publication to OMSs and operators.[6]

Assumptions: One failure condition in a BPON network resource may result in many alarm events from multiple managed entities. Multiple alarm events occurred at approximately the same time. These events were already evaluated and validated by the supplier management system ("process incoming NE events") and shown to possess enough information for alarm analysis purposes. The supplier management system maintains a management model containing (in part) dependency relationships between managed resources including unmonitored resources. Redundant alarm events are eliminated.

Actors: No external actors.

Preconditions: Multiple failure conditions have been detected by a BPON NE within a short period of time.

Description: This use case begins when multiple incoming alarm events have been processed by the supplier management system within a small period of time. The supplier management system groups together related alarm events into an event set for direct comparison or patterning. Event sets are created via rules determined by managed entity dependency relationships. The supplier management system engages in an event comparison process with the goal of finding one active, underlying, independent event for the event set. The process starts with the first alarm event in the event set and compares the next event to see if one of them may be eliminated through rules of event correlation. The process continues until all events in the event set have been processed. If the comparison process detects an event that cannot supersede or be superseded by a previous event, it will be combined with remaining previous events. The result of this comparison process is either determination of a single root cause failure condition or a filtered set of alarm events.

Dependencies are relationships between equipment components and/or transmission media determined by the topology of the network, client-server associations and cross connections.

[6] This use case description makes significant use of management functionality described in [ITU-T M.2140].

Patterning may be done recursively to infer trouble with a resource such as a conduit or power supply from indications in many indirectly supported resources. State change information also plays a role in alarm event correlation. There are several types of failure conditions: equipment failures, communications failures, processing errors, environmental concerns and security violations. There can be dependencies and causality relationships between different types of failure conditions.

Communication alarms may be triggered by an equipment fault. Therefore, if an equipment alarm is received, all communication alarms for termination points contained by the equipment component should be superseded. That is, communication alarms are only considered when they occur without related equipment alarms. If no equipment alarms related to the trail are received, but communication alarms are received, then the cause of the fault might be outside of the supplier management system management domain, might be due to some unmonitored equipment component within its domain, or might arise from the transmission medium that carries the characteristic signal between the BPON NEs. In this case, the upstream communication alarm might be considered the best root cause information within the supplier management system domain.

Environmental alarms should be given high priority in searching for root cause since they point to problems for entire BPON nodes or all NEs at a given location (i.e., they relate to many equipment components and many trails). State changes can also serve as a backup method of detecting faults. Administrative and operational state changes should be treated as equipment alarms, since they always indicate a change in the ability of a resource to fulfil its function. The details of alarm event correlation are left up to the individual supplier management system.

This use case ends when a root cause has been determined, or when an event set has been filtered to the greatest extent possible. The alarm information is formatted in records and made available to interested consumers.

Exceptions: None specified.

Post-conditions: Root cause alarm information has been formatted and these alarms can be raised to external event channels.

6.2.2.24 Root cause impairment analysis

Summary: When there is an occurrence of a set of threshold crossing alerts associated with a single performance degradation condition, the supplier management system shall analyse and correlate the alert events within its domain to the best of its ability, determine the underlying root cause of the problem, and store this information in a log. If several occurrences of the same root cause impairment are detected within a period of time, the supplier management system shall prepare a QoS alarm record for publication by any interested consumer (operator or OMS).

Assumptions: The supplier management system has authenticated the requesting operator or OMS. One impairment condition in a BPON network resource may result in the notification of multiple TCA events associated with multiple managed entities. Multiple TCA events occurred at approximately the same time. These events were already evaluated and validated by the supplier management system ("process incoming NE events") and shown to possess enough information for impairment analysis purposes. The supplier management system maintains a management model containing (in part) dependency relationships between managed resources including unmonitored resources. Redundant TCA events are eliminated. The supplier management system shall support the collection of performance monitored parameters including, but not limited to, those listed as history data managed entities.

Actors: Operator or OMS.

Preconditions: Multiple impairments have been detected on a BPON NE within a short time window.

Description: This use case begins when multiple incoming TCA events have been processed by the supplier management system within a small period of time. The supplier management system groups together related TCA events into an event set for direct comparison or patterning. Event sets are created via rules determined by managed entity dependency relationships. The supplier management system engages in an event comparison process with the goal of determining one active, underlying and independent priority impairment for the event set.

The process starts with the first TCA event in the event set and compares the next event to see if one of them may be eliminated through rules of event correlation (see below for some filtering rules). The process continues until all events in the event set have been processed. If the comparison process detects an event that cannot supersede, or be superseded by, a previous event, it will be combined with remaining previous events. The result of this comparison process is either determination of a single root cause impairment condition or a filtered set of TCAs.

Dependencies are relationships between equipment components and/or transmission media determined by the topology of the network, client-server associations, and cross connections. With the exception of physical interface termination points on the subscriber plug-ins, the supplier management system shall collect only near-end performance monitored parameters. The supplier management system shall suppress the processing and reporting of TCA on trails when the trails have an active failure condition. For each TCA, the supplier management system shall filter out any downstream near-end and far-end TCAs relating to the same direction of transmission for lower level trails served by the trail generating the TCA. For a set of TCAs involving the same parameter for the same trail, the supplier management system shall filter out all but the first TCA received during the interval of collection. TCAs may be further filtered according to precedence within each history data parameter category.

At the end of the precedence and comparison filtering process, the supplier management system shall support tagging of the remaining TCAs. If a particular TCA persists for X intervals within a window of Y collection intervals (where X and Y are settable), the TCA will be called a persistent root cause impairment. The supplier management system shall notify all interested clients of any such persistent filtered root cause impairments using a quality of service alarm and providing the necessary information including managed entity Id, performance parameter, threshold value and observed value.

The supplier management system also allows the setting of sliding window parameters (i.e., X TCAs within Y consecutive collection intervals) per monitored parameter type. [unknown NE, unknown parameters, interval count too large, comm failure, unknown managed entity, equipment failure]. The supplier management system also supports administrative functions of retrieval concerning settings of sliding window parameters [unknown managed entity, unknown NE, unknown parameters].

This use case ends when root cause impairment information has been logged and any suitable quality of service alarm notification has been prepared.

Exceptions: Unknown NE, unknown parameters, interval count too large, comm failure, unknown managed entity, equipment failure.

Post-conditions: Root cause impairment data is available for retrieval from the supplier management system and quality of service alarms can be raised to an external event channel.

6.2.2.25 Scheduler

Summary: The supplier management system provides a scheduler function for activities to be carried out at a later date. The operator or OMS can create a new schedule, suspend/resume a schedule, view a schedule and delete or modify an existing schedule if it is not in use.

Assumptions: The supplier management system has authenticated the requesting operator or OMS. A communication link exists between the operator or OMS and the supplier management system.

The supplier management system has authenticated the operator or OMS to access the scheduling function.

Actors: Operator or OMS.

Preconditions: The supplier management system is installed.

Description: This use case begins when the OMS or operator initiates a request to create a new schedule. To create a new schedule, the following parameters are included: schedule name, start and stop times for when the schedule can be applied, schedule trigger point times matrix, and the periodicity of the schedule [duplicate user label, matrix scheduler type mismatch, invalid start time, invalid stop time, invalid trigger].

Once the schedule is created, the OMS or operator can schedule an activity such as NE MIB uploading, bulk transfer, testing or synchronization activity simply by referencing the schedule name. The scheduled activity is in pending mode prior to the trigger time, and in progress mode until it is successfully (or unsuccessfully) completed.

The operator or OMS can retrieve information on the schedule. The returned information includes scheduler name, start time, stop time, trigger point times, matrix, operational state and administrative state [unknown scheduler]. The supplier management system also supports the operator's need to suspend or resume activities via reference to the schedule. The supplier management system is able to suspend/resume a scheduled activity by locking/unlocking the administrative state of the associated schedule [unknown scheduler]. The operator can also delete or modify an existing schedule that is not in use [unknown scheduler, schedule in use, invalid start time, invalid stop time, matrix scheduler type mismatch, invalid trigger, duplicate user label].

This use case ends when a schedule has been created, modified or deleted.

Exceptions: Unknown scheduler, schedule in use, duplicate user label, matrix scheduler type mismatch, invalid start time, invalid stop time, invalid trigger.

Post-conditions: Invocation of routine management activities can be supported by the supplier management system based on any established active schedulers.

6.2.2.26 Synchronize NE

Summary: The supplier management system is responsible for providing synchronization and consistency between all physical and logical BPON network resource data.

Assumptions: The supplier management system has authenticated the requesting operator or OMS. The management communications channel between the BPON resource is available. The supplier management system maintains an information model that captures the configuration data in a BPON system. This information model should reflect the current provisioned state of the BPON system. As provisioning changes are made in the network the information model is updated to reflect the latest changes. These changes may occur by the operator provisioning something through the supplier management system, or through a craftsperson provisioning changes in the field.

Actors: BPON NEs, privileged user.

Preconditions: The supplier management system is installed and is designed to normally remain in synch with the configuration of the BPON NEs within its management jurisdiction.

Description: This use case begins when the privileged user suspects that the supplier management system and BPON NE are out of synch with each other. The privileged user formulates a request for synchronization naming the BPON NE. The supplier management system responds to the request by updating its management information with the latest information obtained by retrieving all configuration data from the BPON NE [comm failure, unknown NE, equipment failure, backup in progress, synch in progress]. While this process is active it is assumed that other management activities involving the BPON NE are blocked.

If the synchronization proves to be disruptive to management operations (taking too long), then it is possible for the privileged user to abort the synchronization process. Any inconsistencies between the supplier management system and the NE that have been resolved before the abort are retained.

Similar functionality is invoked automatically whenever there is an event denoting a DCN connection establishment or recovery, a remote reset of a BPON NE, an ONT or ONU ranging, or a resynchronization of a current event listing. When an ONT is ranged, it is assumed that the OLT will automatically update its local ONT configuration to reflect the state of the ONT. This means that the supplier management system will use the range event to trigger an upload of the ONT data from the OLT.

Each time the process is initiated, an NE will be selected for synchronization. The process will initiate an upload of data from the NE. This will be a vendor-specific implementation.

The next step in the sequence is to reconcile the data retrieved from the NE with the current state of the information model. If there is any difference in any data stewarded by the NE, then the model will be updated and (if business rules apply) attribute value change information will be formatted and made available as published notifications to any interested operator or OMS. As updates are made to the information model, events will also be generated in the system. If there is any difference in any data stewarded by the supplier management system, then the supplier management system issues configuration change requests to the NE.

The process will conclude by returning a value to the initiator (internal procedure) that indicates that the synchronization process was successfully completed, and the information model was updated.

A privileged user can also request routine resynchronization of NE and supplier management system management information. The request includes the identification of the BPON NE and reference to the schedule [unknown NE, unknown scheduler, invalid scheduler]. The privileged user can modify the scheduled activity as well as cancel it [unknown NE, unknown scheduler, invalid scheduler].

This user case ends when supplier management system and the BPON NE are in synch.

Exceptions: Comm failure, unknown scheduler, unknown NE, equipment failure, backup in progress, synch in progress.

Post-conditions: Management information resident in installed BPON NEs is consistent with the same information resident in the supplier management system.

6.2.2.27 View records

Summary: The supplier management system will provide means to view all logged events or other records archived temporarily at the supplier management system. It will also provide a way to retrieve a subset of records on behalf of an OMS.

Assumptions: The supplier management system has authenticated the requesting operator or OMS. Selection filters have been specified and implemented.

Actors: Operator and OMS.

Preconditions: The supplier management system has been archiving performance and traffic measurements and recording event notifications in logs.

Description: This use case begins when the operator or OMS initiates a request to select records from a particular record set for further evaluation. The request identifies the record set and provides selection criteria. The selection criteria may include such parameters as:

- Managed entity Id.
- Time interval.
- Record type.

The supplier management system will process the retrieval request and find the records contained in the record set that meet the selection criterion. The listing of records will be returned to the requestor [unknown record set, timeout, no such records, too many records].

The OMS may query for the size of any existing record set [unknown record set].

This use case ends when the records or status of a record set information has been provided to the requesting operator or OMS.

Exceptions: Unknown record set, timeout, no such records, too many records.

Post-conditions: The records are available for reviewing by the operator, or for processing by the OMS.

6.3 Analysis

Detailed class, sequence and state change diagrams will be offered only for those situations where an interface to an external actor exists, or for those cases that these details are necessary to explain behaviour. Each section of the analysis begins with a high-level view of the classes involved in the high-level use case diagrams of clause 6.2.1.3 with details of specific use cases following this summary. This is followed by references to any managed entities (the management information data structures from [ITU-T Q.834.1] and [ITU-T Q.834.2]) that may be involved in the use case. In some cases, the references to managed entities is followed by a listing to "management support entities" referring to familiar entities from existing ITU-T Recommendations. Next follows signatures for any real time operations between an external actor and the supplier management system. This information is accompanied by a brief description of each exception raised by the operations listed. Finally, users of this Recommendation may assume that every operation is atomic except where indicated as "best effort".

6.3.1 Access control

The following class diagram show interactions between actors and classes internal to the supplier management system when administering user access to the supplier management system.

6.3.1.1 Administer user privileges

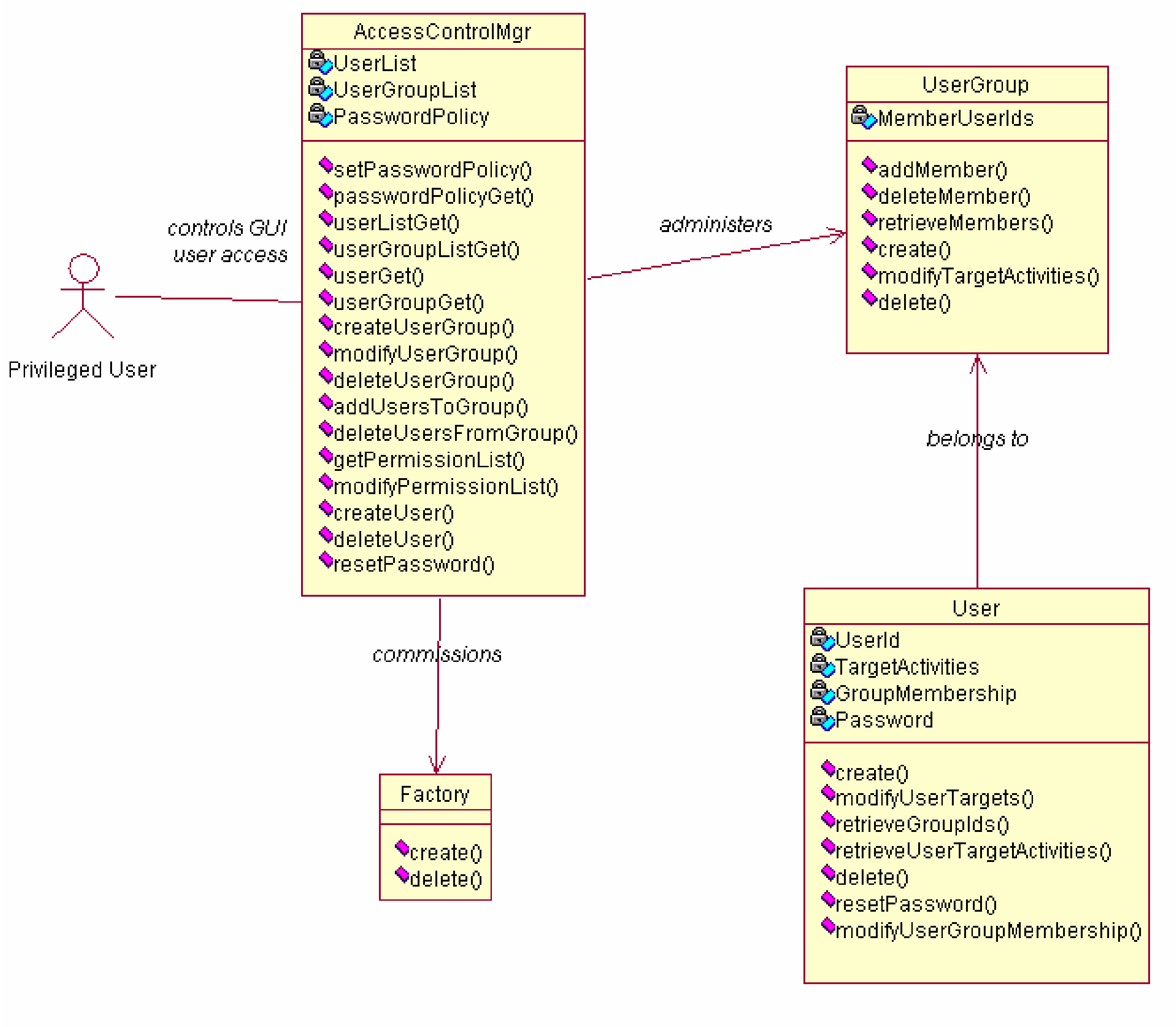


Figure 6-11 – Administer user privileges class diagram

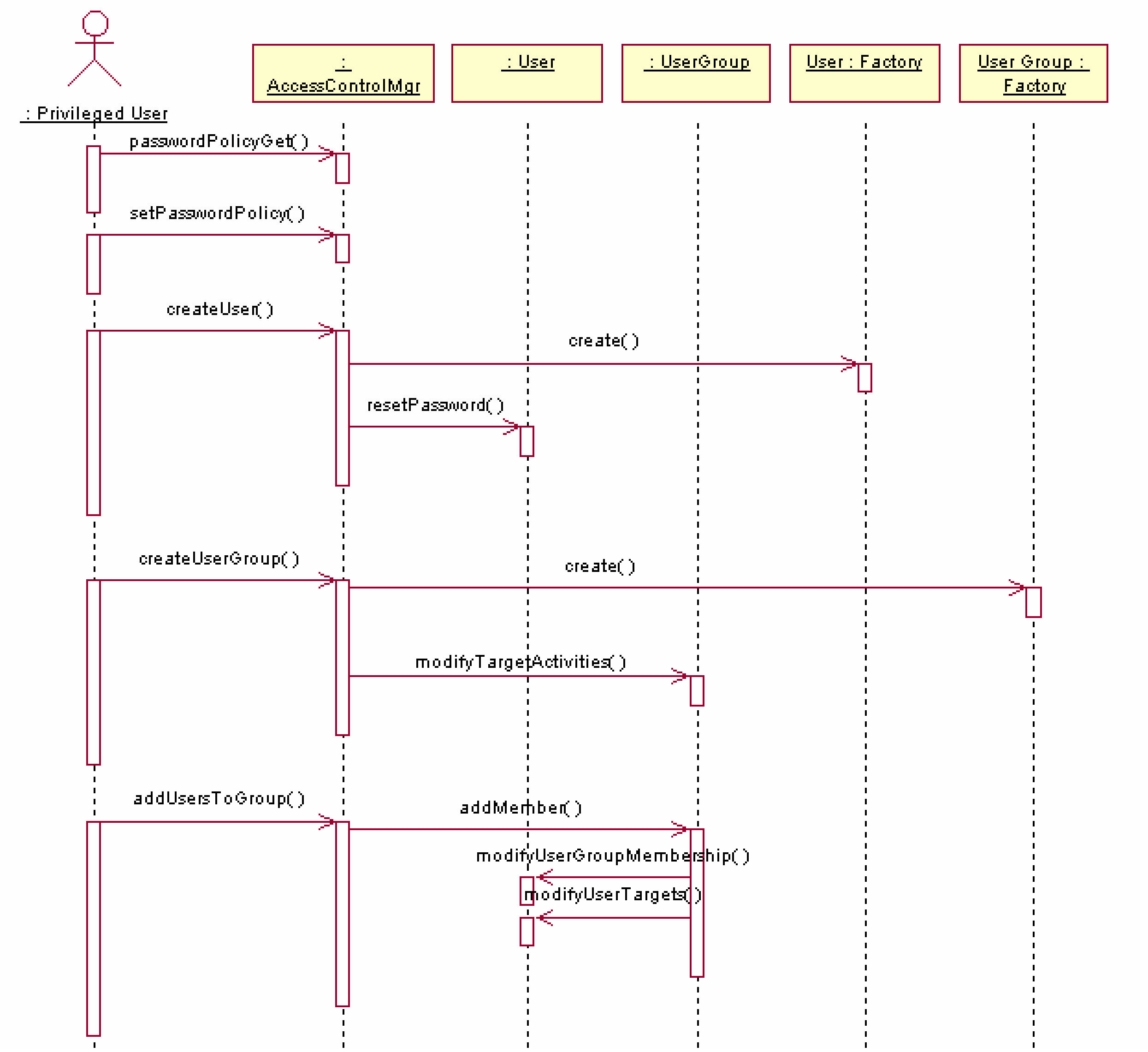


Figure 6-12 – Create user and user group sequence diagram

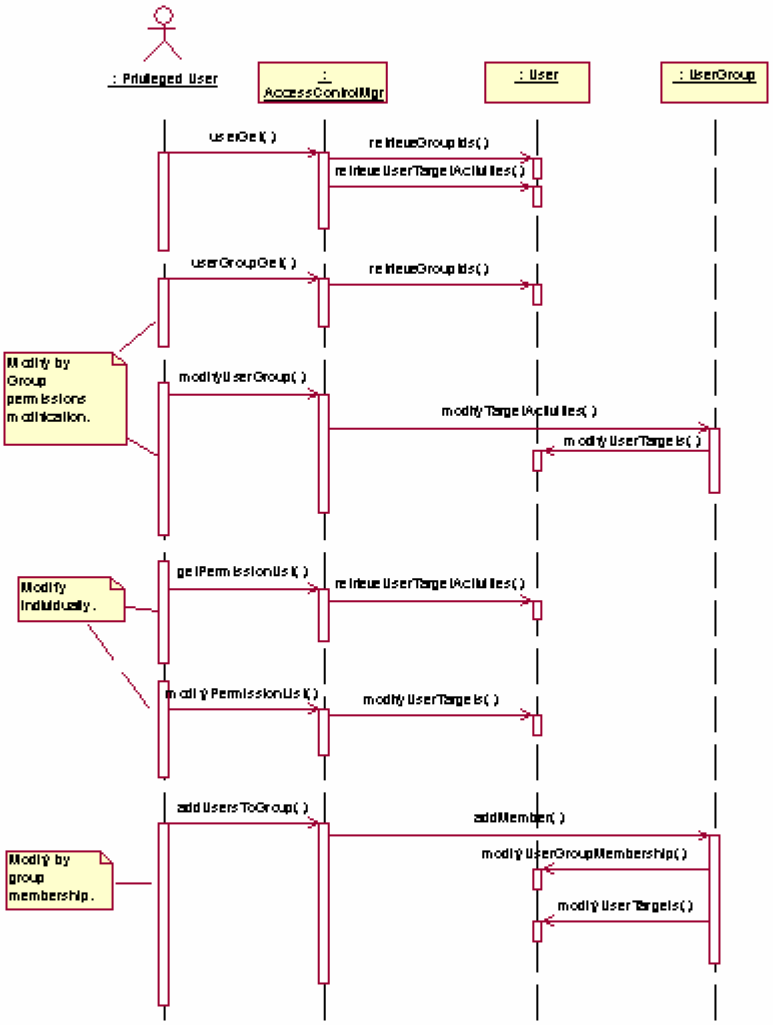


Figure 6-13 – Modify user permissions sequence diagram

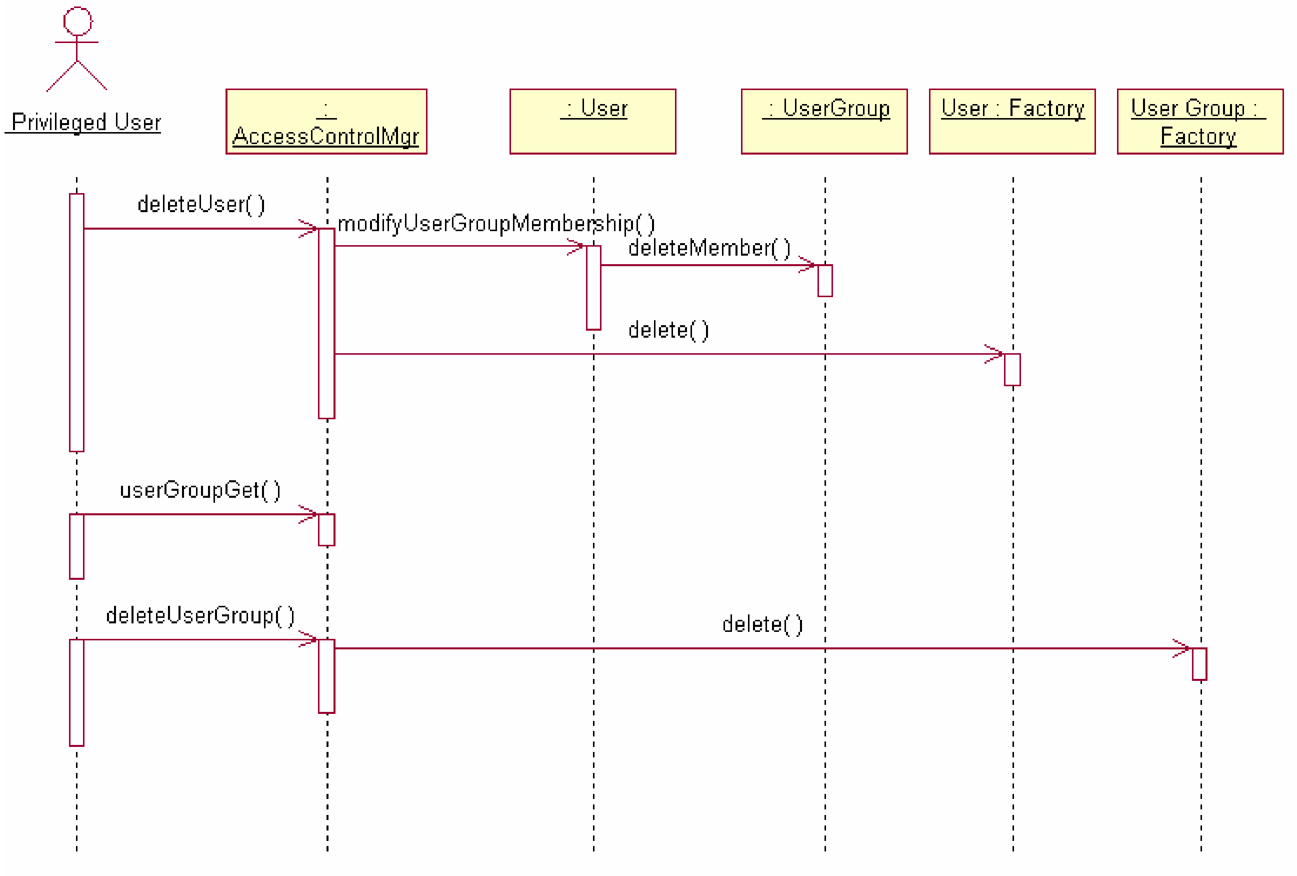


Figure 6-14 – Delete users and user groups sequence diagram

Operations

Operation name	Operation purpose
1) setPasswordPolicy	This operation allows the privileged users to manage the password policy.
2) passwordPolicyGet	This operation allows the privileged users to retrieve the policy concerning the syntax of data exchanged and timers used when logging into the supplier management system.
3) userListGet	This operation allows the privileged users to retrieve the list of user Ids having some form of access to the supplier management system as well as their target activities and group memberships.
4) userGroupListGet	This operation allows the privileged users to retrieve the user groups having access to the supplier management system with the members of the group and target activities identified.
5) userGet	This operation allows the privileged users to retrieve the user's group membership and target activities.
6) userGroupGet	This operation allows the privileged users to retrieve the member users of the group and their allowed target activities.
7) createUserGroup	This operation allows the privileged users to create a new user group.
8) modifyUserGroup	This operation allows the privileged users to add/delete the target activities of a user group.
9) deleteUserGroup	This operation allows the privileged users to delete an existing user group.
10) addUsersToGroup	This operation allows the privileged user to add new users to an existing user group.
11) deleteUsersFromGroup	This operation allows the privileged users to delete users from a user group.
12) getPermissionList	This operation allows the privileged users to obtain the list of the activities allowed to a specified user.
13) modifyPermissionList	This operation allows the privileged users to modify the list of the activities allowed to a user.
14) createUser	This operation allows the privileged users to create a new user.
15) deleteUser	This operation allows the privileged users to delete an existing user.
16) resetPassword	This operation allows the privileged users to reset the password for a user.

Figure 6-15 – Access control manager operations

Operation signatures

Operation name	Input parameters	Return value	Exceptions
1) setPasswordPolicy	PasswordPolicyType	void	AccessDenied
2) passwordPolicyGet		PasswordPolicyType	AccessDenied
3) userListGet		UserSeqType	AccessDenied
4) userGroupListGet		UserGroupSeqType	AccessDenied
5) userGet	UserIdType	UserType	AccessDenied, UnknownUserIds
6) userGroupGet	UserLabelType	UserGroupType	AccessDenied, UnknownUserGroupId
7) createUserGroup	UserLabelType, TargetActivitySeqType	void	DuplicateUserGroupId, UnknownTargets, AccessDenied
8) modifyUserGroup	UserLabelType, TargetActivitySeqType, TargetActivitySeqType	TargetActivitySeqType	UnknownUserGroupId, UnknownTargets, AccessDenied
9) deleteUserGroup	UserLabelType	void	AccessDenied, UserGroupNotEmpty, UnknownUserGroupId
10) addUsersToGroup	UserLabelType	void	AccessDenied, UnknownUserGroupId
11) deleteUsersFromGroup	UserLabelType, UserIdSeqType	void	AccessDenied, UnknownUserGroupId, UnknownUserIds
12) getPermissionList	UserIdType	TargetActivitySeqType	UnknownUserIds, AccessDenied
13) modifyPermissionList	UserIdType, TargetActivitySeqType, TargetActivitySeqType	TargetActivitySeqType	UnknownUserIds, UnknownTargets, AccessDenied
14) createUser	UserIdType, PasswordType, TargetActivitySeqType	void	DuplicateUserId, UnknownTargets, AccessDenied, UserLoginPolicyViolation
15) deleteUser	UserIdType	void	UnknownUserIds, AccessDenied
16) resetPassword	UserIdType, PasswordType	void	UnknownUserIds, UserLoginPolicyViolation, AccessDenied

Figure 6-16 – Access control manager signatures

Exceptions

Exception raised	Description
AccessDenied	System is not granted access to this interface object.
DuplicateUserGroupId	The Id is already used for another user group.
DuplicateUserId	Access control profile has already been established for this user Id.
UnknownTargets	List of unknown target activities.
UnknownUserGroupId	User group is unknown to the supplier management system.
UnknownUserIds	This exception is raised when any user Id is unrecognized.
UserLoginPolicyViolation	The specified assignment of a new password to a user violates the user login policy currently enforced by the supplier management system.
UserGroupNotEmpty	Non-empty user group cannot be deleted.

Figure 6-17 – Access control manager exceptions

6.3.2 Event handling

The following two clauses provide the analysis for the two use cases in Figure 6-5, having interactions with external actors provided by the operator or network owner.

6.3.2.1 Publish event

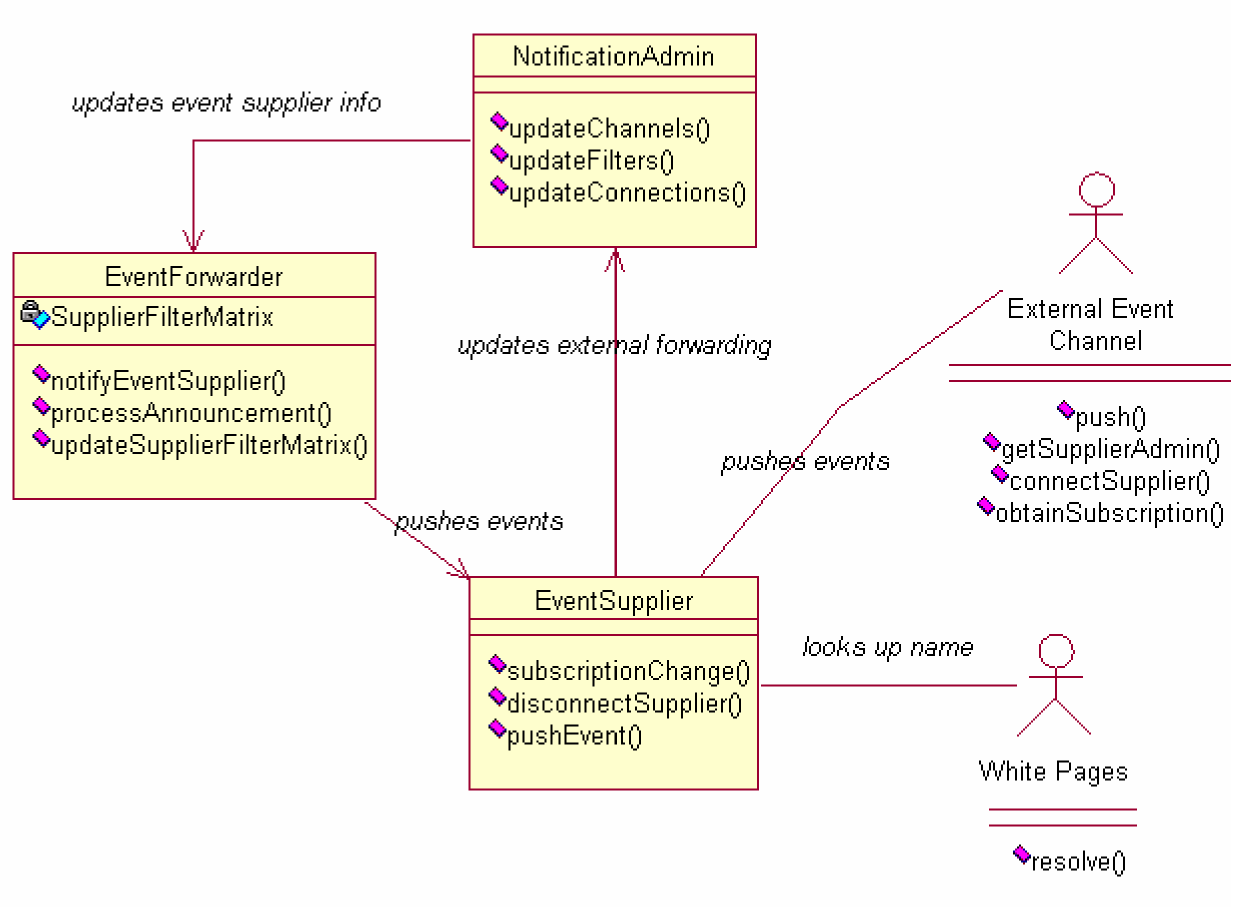


Figure 6-18 – Publish event class diagram

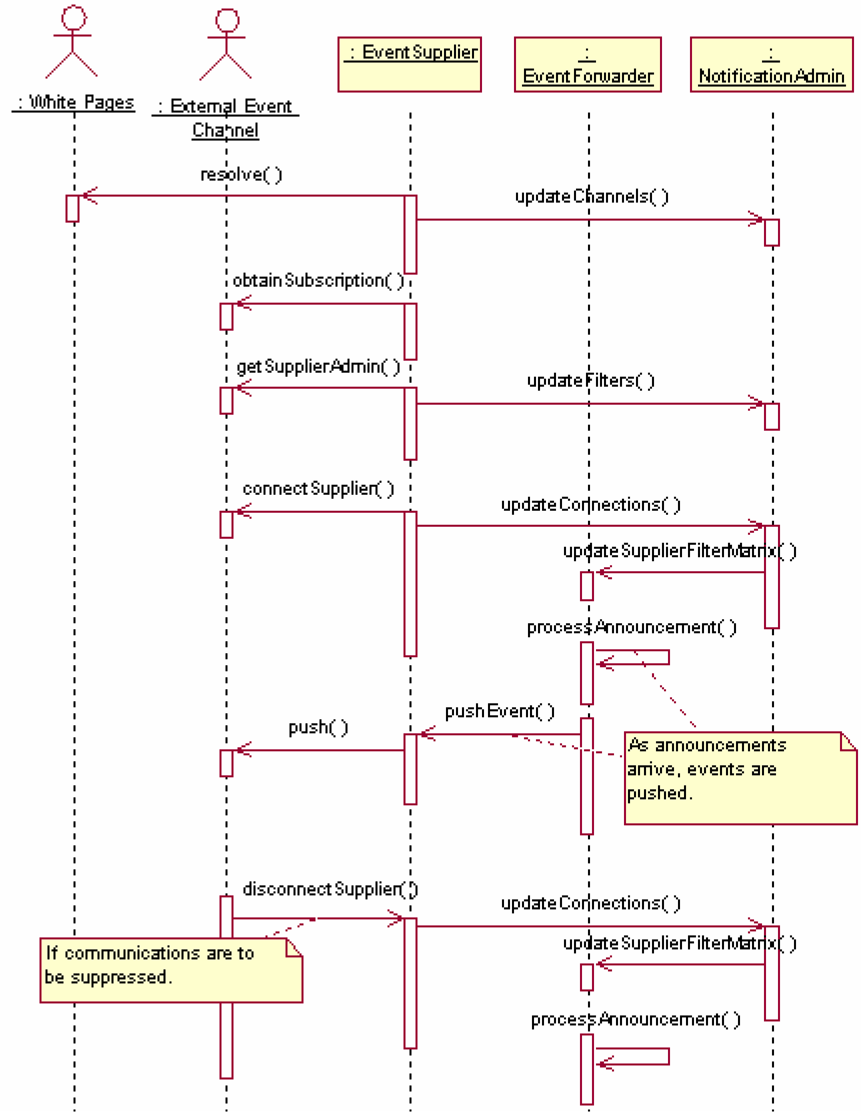


Figure 6-19 – Publish event sequence diagram

Operations

Operation name	Operation purpose
1) obtainConsumers	This operation allows the supplier management system to determine the names of the OMSs that consume event notifications.
2) connectSupplier	This operation allows the supplier management system to connect to the external event channel.
3) push	This operation allows the supplier management system to push an event notification to the external event channel.
4) obtainSubscription	This operation allows the supplier management system to determine the type of events to be pushed on the external event channel.
5) disconnectSupplier	This operation allows the supplier management system to be disconnected from the external event channel.
6) getSupplierAdmin	This operation allows the supplier management system to administer its event supplier function.

Figure 6-20 – Event publisher operations

Operation name	Input parameters	Return value	Exceptions
1) obtainConsumers		NameType	AccessDenied
2) connectSupplier	NameType		AccessDenied, AlreadyConnected
3) push	StructuredEventType	void	Disconnected, AccessDenied
4) obtainSubscription		StructuredEventSeqType	AccessDenied
5) disconnectSupplier	NameType	void	AccessDenied
6) getSupplierAdmin		sequence of long	AccessDenied

Figure 6-21 – Event publisher signatures

Exceptions

Exception raised	Description
AccessDenied	System is not granted access to this interface object.
AlreadyConnected	The communicating object is already connected to the event channel.
Disconnected	The object was disconnected from the event channel.
InvalidEventType	The subscription change identified an invalid event type.

Figure 6-22 – Event publisher exceptions

6.3.2.2 Root cause impairment analysis

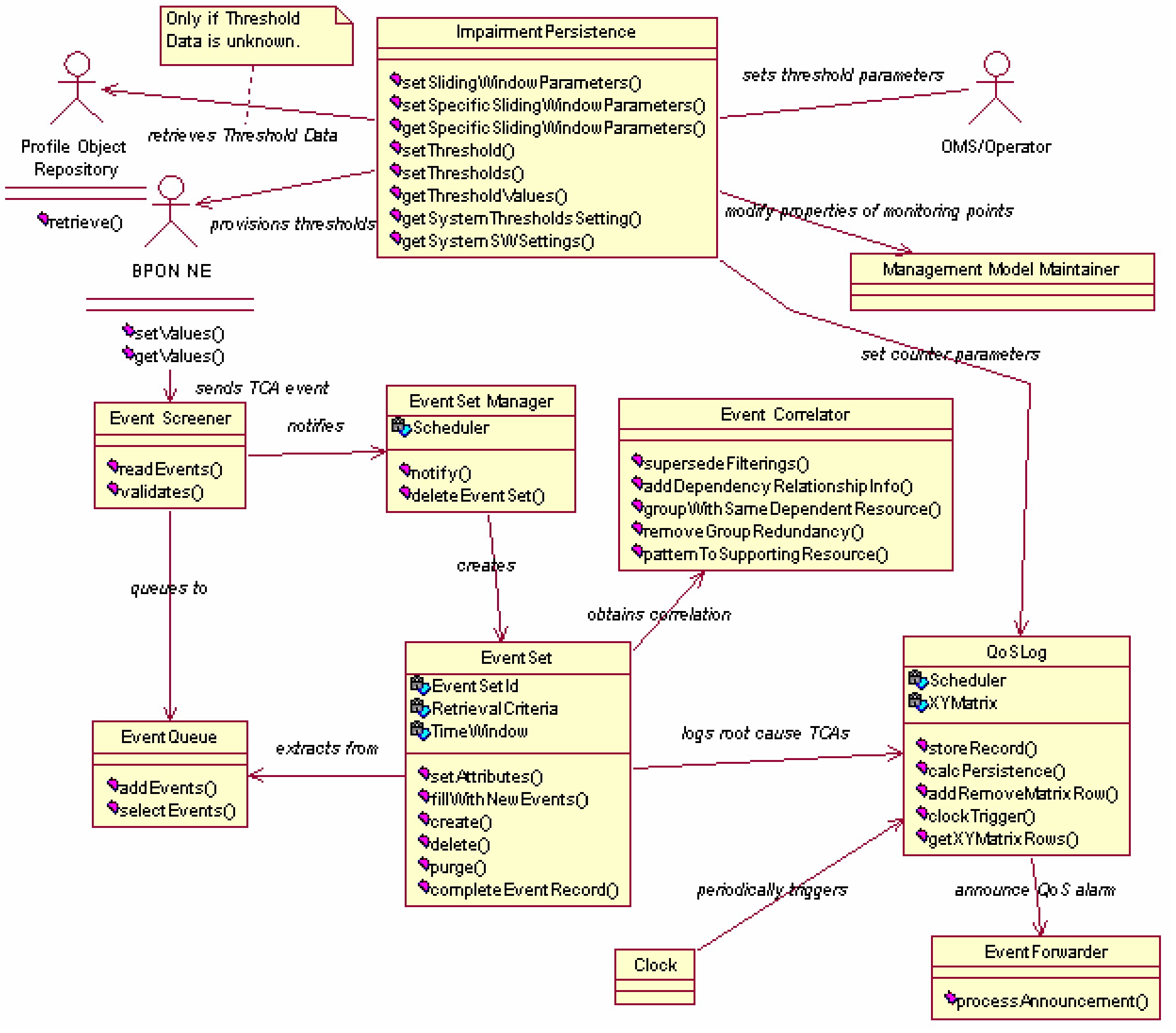


Figure 6-23 – Root cause impairment analysis class diagram

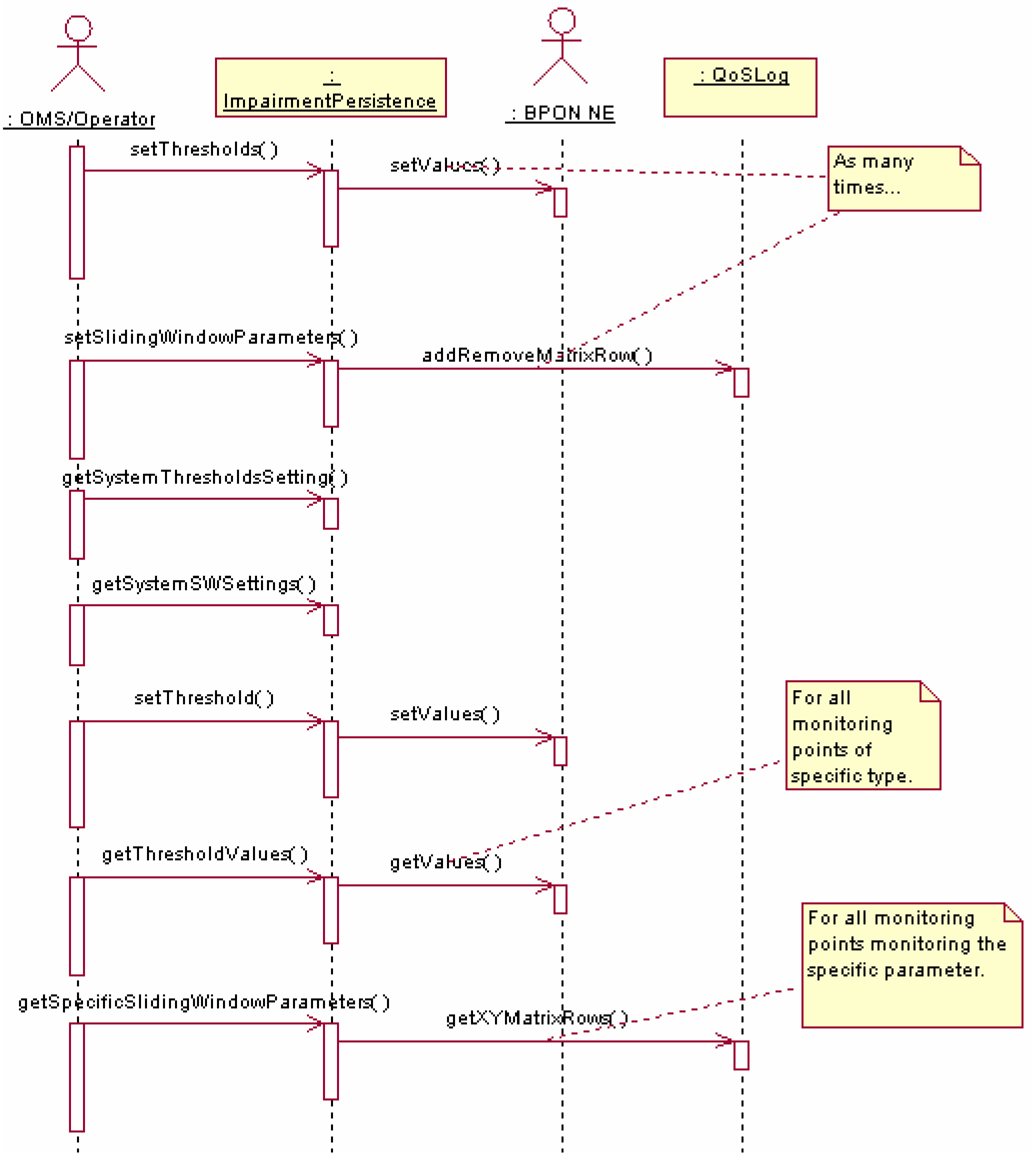


Figure 6-24 – Setting of parameters sequence diagram

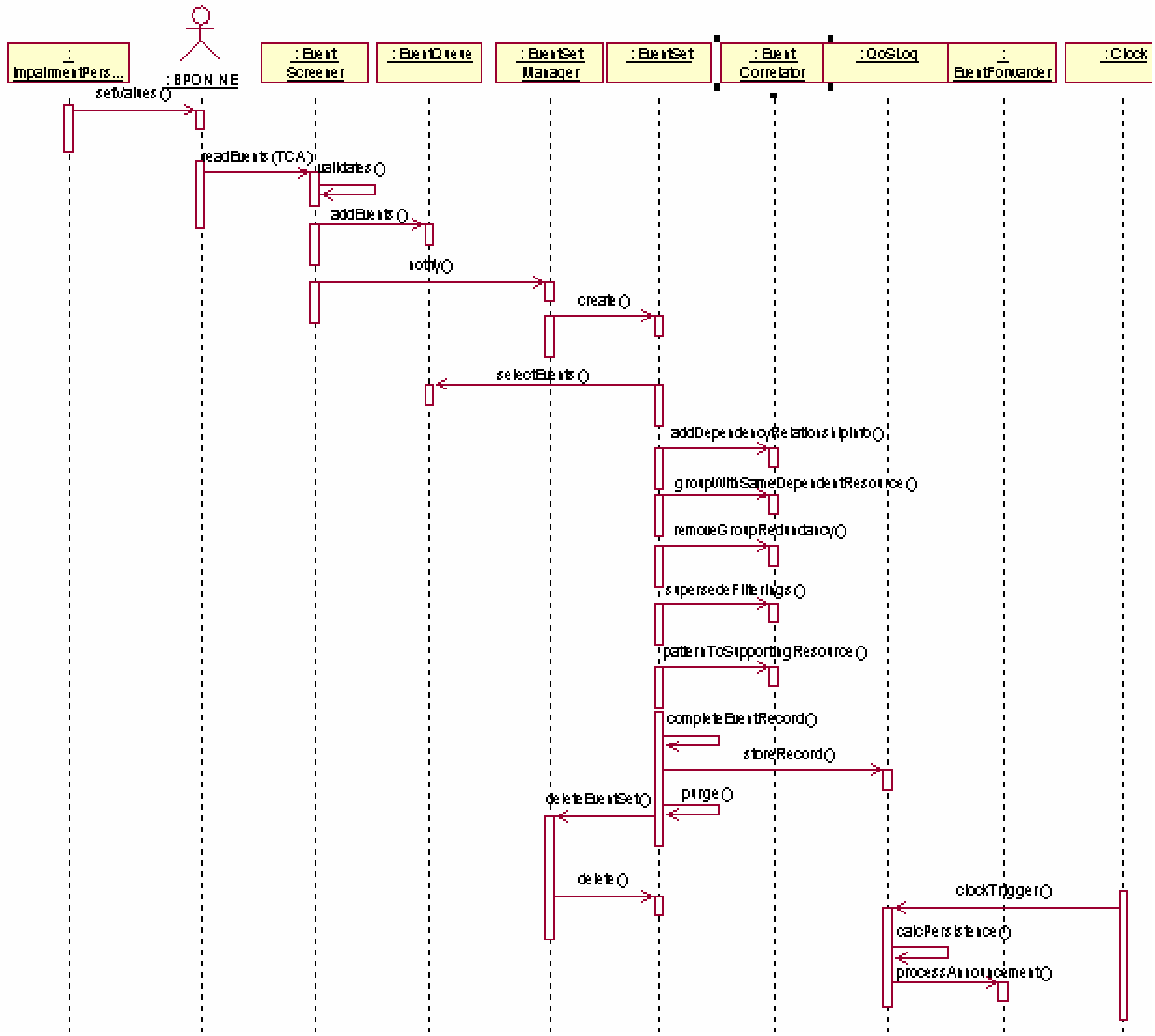


Figure 6-25 – RCIA sequence diagram

Operations

Operation name	Input parameters
1) setSlidingWindowParameters	This operation sets the sliding window parameters for one, some or all monitored parameters in an NE.
2) setSpecificSlidingWindowParameters	This operation is similar to the operation setSlidingWindowParameters except the scope of assignment of settings is limited to a specific monitoring point identified in the operation.
3) getSpecificSlidingWindowParameters	This operation provides a listing of monitoring points and their sliding window settings for a specified parameter.
4) setThreshold	This operation sets the threshold value identified by a profile to a monitoring point in a network element.
5) setThresholds	This operation allows the setting of a collection of threshold value, monitoringPointType pairs on a particular NE.
6) getThresholdValues	This operation provides a listing of monitoring points and their threshold data setting names for a specified monitoring point type.
7) getSystemThresholdsSetting	This operation retrieves the system default values for threshold data.
8) getSystemSWSettings	This operation retrieves the system default sliding window settings.

Figure 6-26(a) – Impairment persistence operations

Operation signatures[7]

Operation name	Input parameters	Return value	Exceptions
1) setSlidingWindowParameters	ManagedEntityIdType (NE), MonitoredParameterSeqType, short (total consecutive intervals), short (minimum persistence)	void	UnknownNE, UnknownParameters, IntervalCountTooLarge, AccessDenied, CommFailure
2) setSpecificSlidingWindowParameters	ManagedEntityIdType (NE), ManagedEntityIdType (Monitoring Point), MonitoredParameterSeqType, short (total consecutive intervals), short (minimum persistence)	void	UnknownNE, UnknownParameters, IntervalCountTooLarge, AccessDenied, UnknownManagedEntity, CommFailure, EquipmentFailure
3) getSpecificSlidingWindowParameters	ManagedEntityIdType (NE), MonitoredParameterType	SWPValueSeqType	UnknownNE, UnknownParameters, CommFailure
4) setThreshold	ManagedEntityIdType (NE), ManagedEntityIdType (monitoring point), NameType (threshold data profile)	void	UnknownNE, AccessDenied, UnknownManagedEntity, UnknownProfiles, InvalidAssociation, CommFailure, ProfileSuspended
5) setThresholds	ManagedEntityIdType (NE), boolean (system scope), ThresholdsSeqType	void	UnknownNE, UnknownProfiles, AccessDenied, UnknownMonitoringPoint Types, InvalidAssociation, CommFailure, ProfileSuspended
6) getThresholdValues	ManagedEntityIdType (NE), MonitoringKindType	MonitoringPoint ThresholdsSeqType	UnknownNE, UnknownMonitoringPoint Types, CommFailure
7) getSystemThresholdsSetting	ManagedEntityIdType (NE)	ThresholdsSeqType	AccessDenied, UnknownManagedEntity
8) getSystemSWSettings	ManagedEntityIdType (NE)	ParameterSetting SeqType	AccessDenied, UnknownManagedEntity

Figure 6-26(b) – Impairment persistence signatures

[7] The "set" operations listed above modify (overwrite) an existing X,Y sliding window specification. If no such specification exists for the monitored parameter, then the "set" operations are viewed to be additional specifications.

Exceptions

Exception raised	Description
AccessDenied	System is not granted access to this interface object.
CommFailure	There was a DCN link failure between the NE and the supplier management system.
EquipmentFailure	The NE currently has a failure condition preventing the requested transaction from being completed.
IntervalCountTooLarge	The exception is raised when the requested intervals exceeds the maximum supported by the supplier management system. The exception indicates the maximum allowed monitoring intervals supported by the supplier management system.
InvalidAssociation	The given profile cannot be applied to a monitoring point.
ProfileSuspended	This exception is raised if the profile name provided is unknown to the supplier management system and cannot be retrieved from the profile object repository.
UnknownManagedEntity	The specified managed entity is unknown to the supplier management system.
UnknownMonitoringPointTypes	The monitoring point instance provided on the request is unknown to the supplier management system.
UnknownNE	Identified NE is unknown to the supplier management system.
UnknownParameters	The given monitored parameter is unknown in the supplier management system.
UnknownProfiles	System is not granted access to this interface object.

Figure 6-27 – Impairment persistence exceptions

6.3.3 Software and configuration data

6.3.3.1 Download and activate NE software

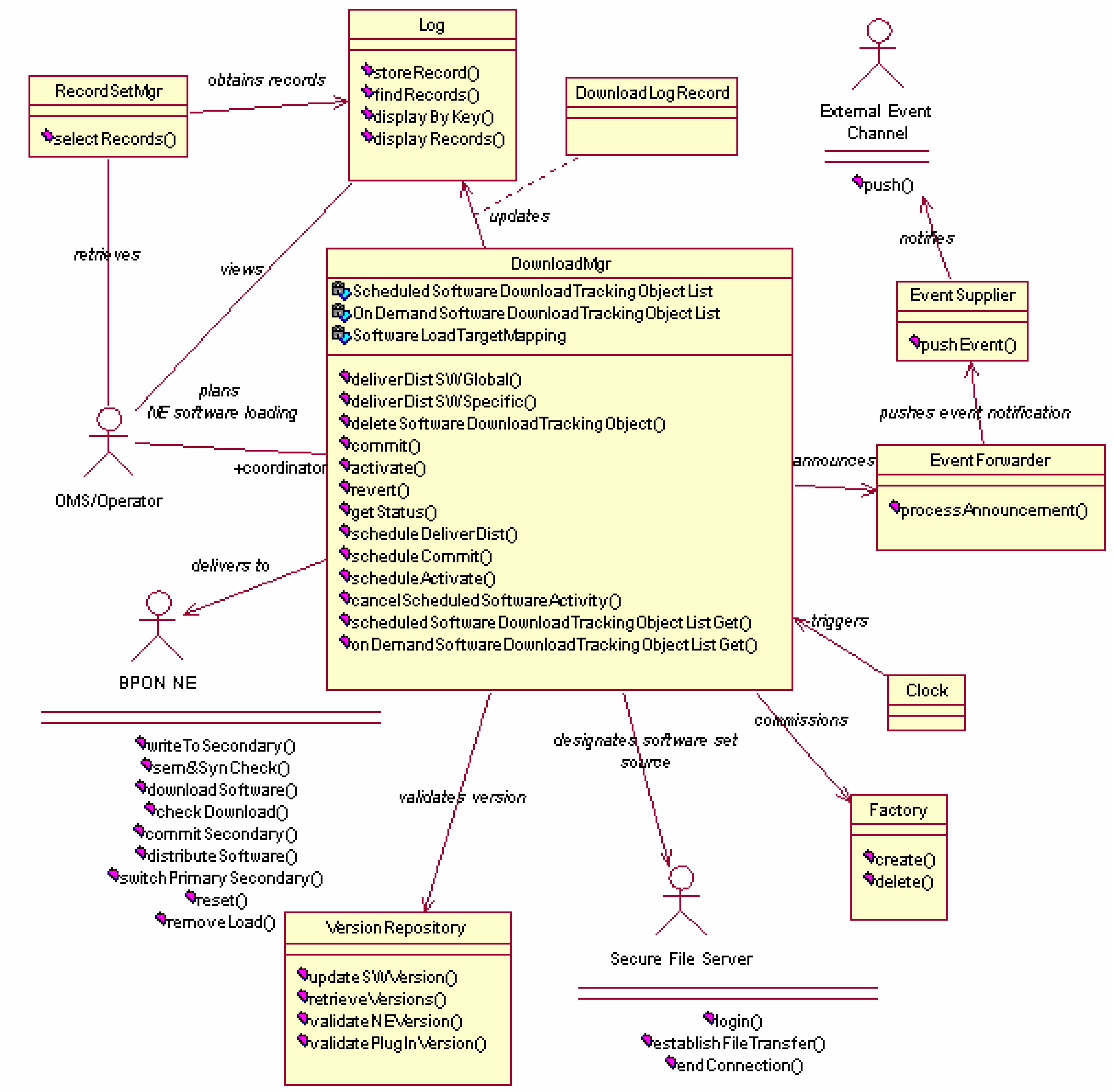


Figure 6-28 – Distribute NE software class diagram

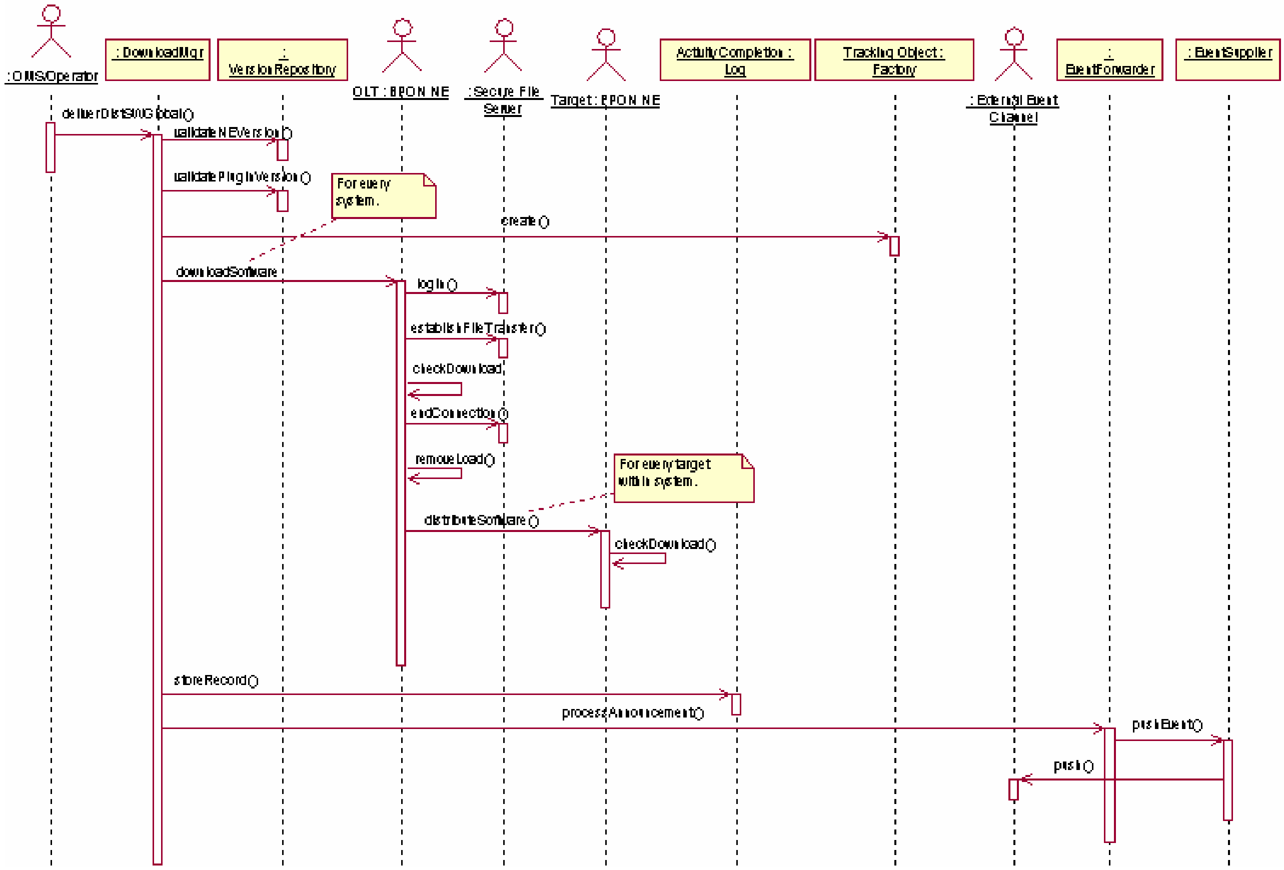


Figure 6-29 – Immediate NE software delivery sequence diagram

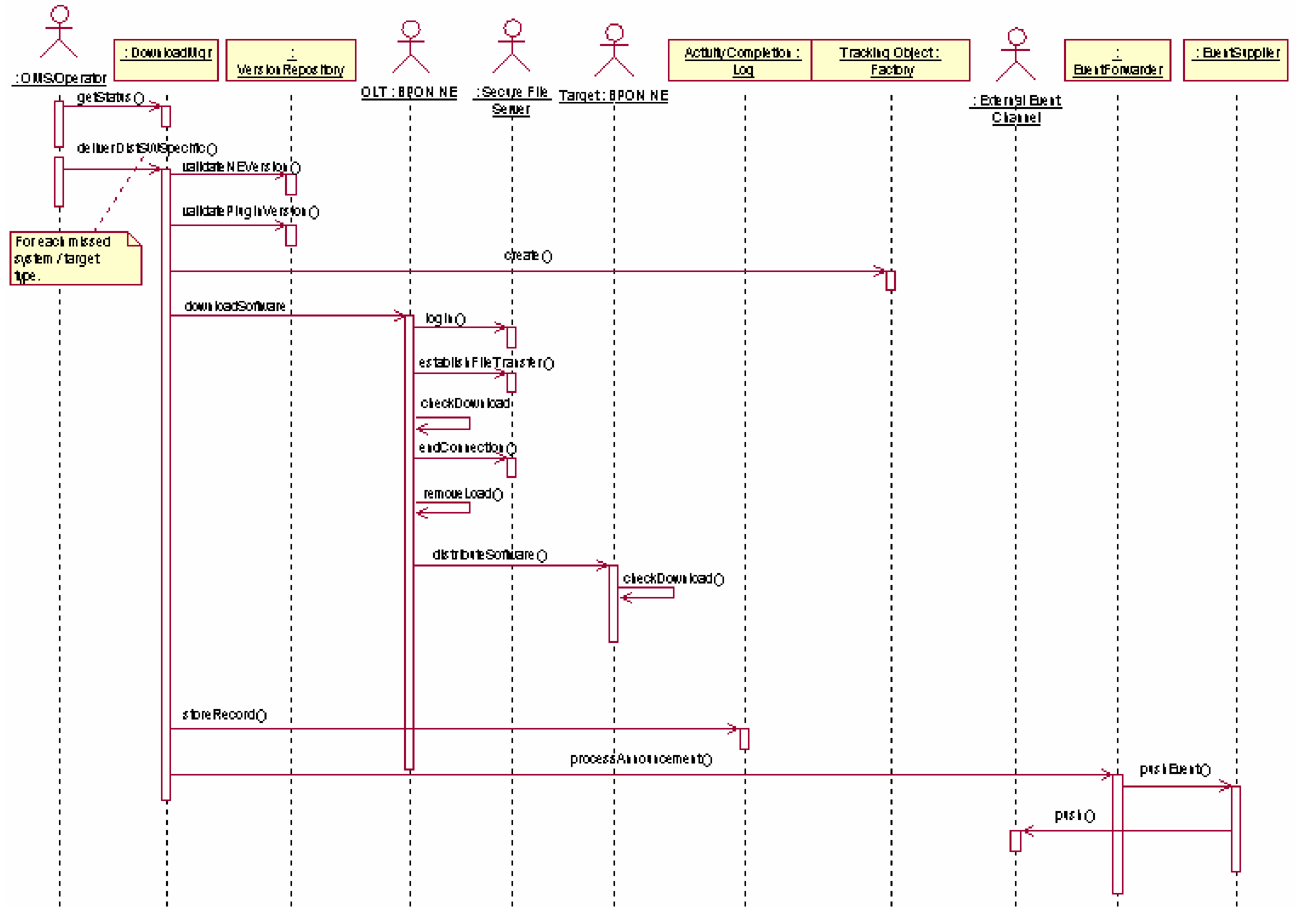


Figure 6-30 – Immediate specific NE software delivery sequence diagram

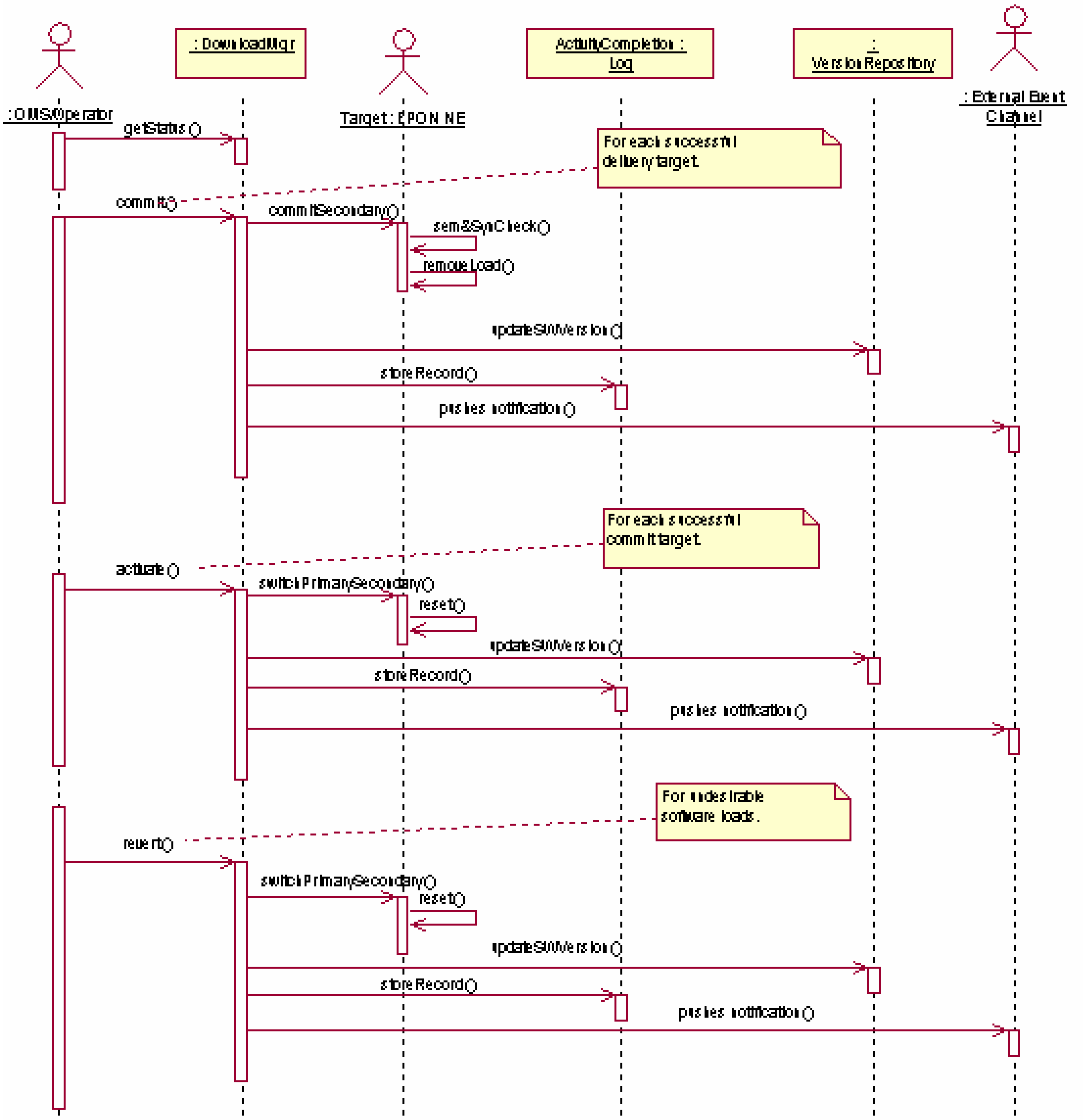


Figure 6-31 – Immediate NE software commit, activate or revert sequence diagram (for successful software delivery targets)[8]

[8] In this figure and subsequent software activity sequences diagrams, "pushes notification" to the external event channel refers to the same notification process that is detailed out in Figures 6-29 and 6-30 for on demand software delivery and distribution.

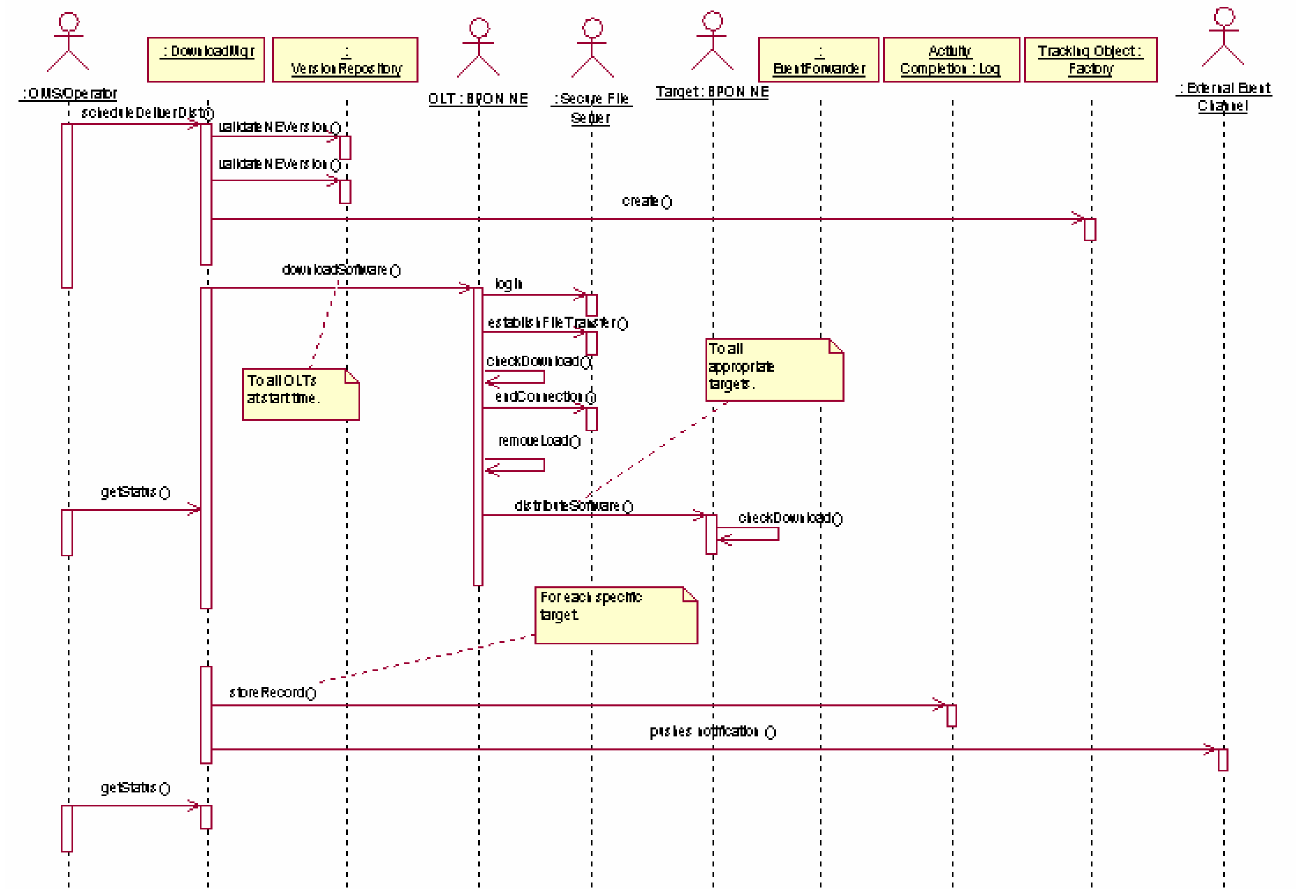


Figure 6-32 – Scheduled NE software download sequence diagram

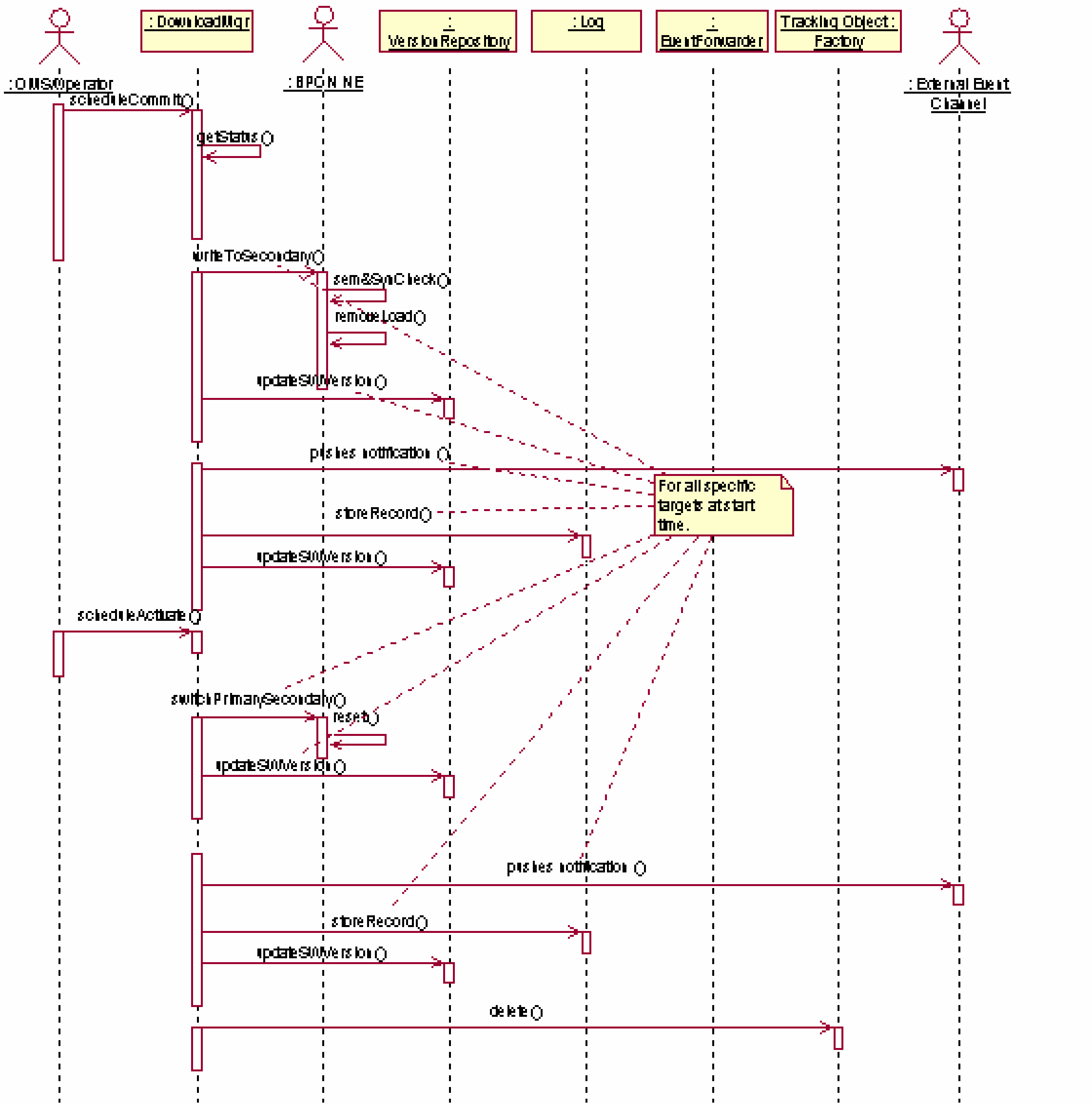


Figure 6-33 – Scheduled NE software commit or activate sequence diagram

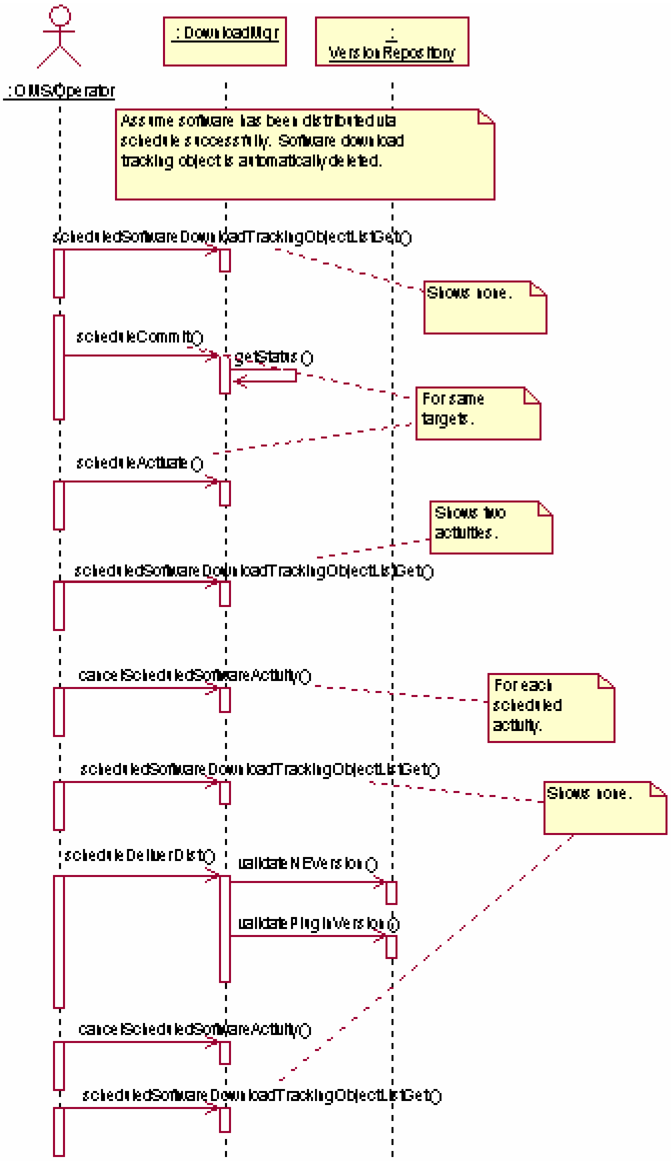

: OMSOperator
: DownloadMgr
: VersionRepository
Assume software has been distributed via schedule successfully. Software download tracking object is automatically deleted.
scheduledSoftwareDownloadTrackingObjectListGet()
Shows none.
scheduleCommit()
getStatus()
For same targets.
scheduleActivate()
Shows two activities.
scheduledSoftwareDownloadTrackingObjectListGet()
cancelScheduledSoftwareActivity()
For each scheduled activity.
scheduledSoftwareDownloadTrackingObjectListGet()
Shows none.
scheduleDeliverDist()
validateNEVersion()
validatePluginVersion()
cancelScheduledSoftwareActivity()
scheduledSoftwareDownloadTrackingObjectListGet()

Figure 6-34 – Cancel scheduled NE software delivery sequence diagram

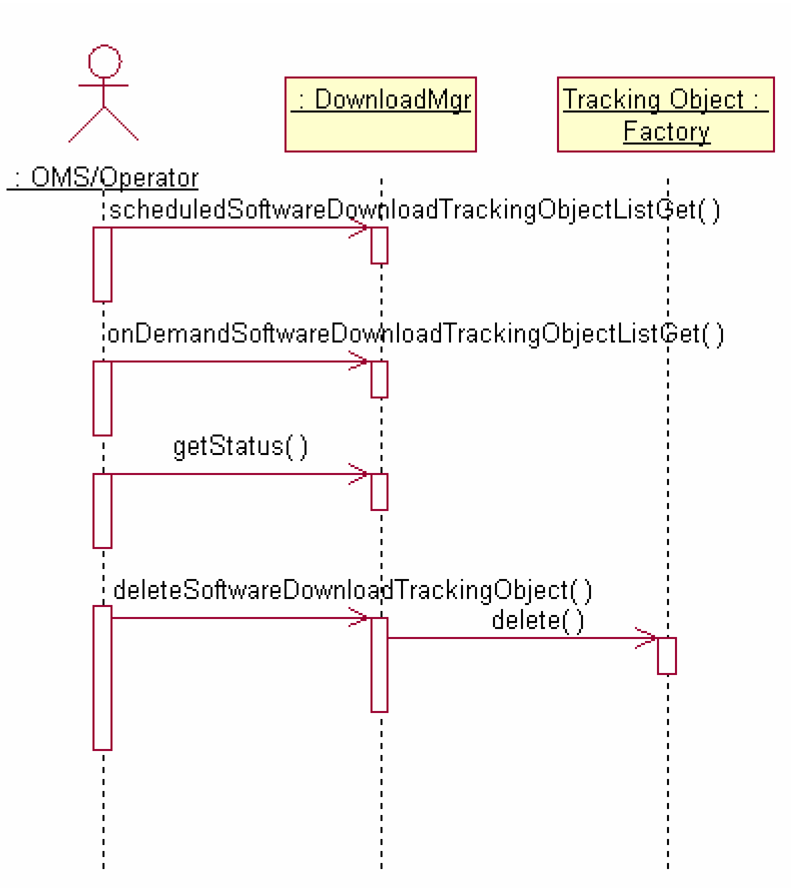

: OMS/Operator
: DownloadMgr
Tracking Object : Factory
scheduledSoftwareDownloadTrackingObjectListGet( )
onDemandSoftwareDownloadTrackingObjectListGet( )
getStatus( )
deleteSoftwareDownloadTrackingObject( )
delete( )

Figure 6-35 – Tracking object maintenance sequence diagram

Operations

Operation name	Operation purpose
1) deliverDistSWGlobal	This operation requests the supplier management system to download software generics from software source machine for the purpose of software upgrades and software maintenance changes (patches) to NEs.
2) deliverDistSWSpecific	This operation is same as deliverDistSWGlobal except the scope is within a single NE/PlugInUnit/slot as described in the input parameter distributionTarget.
3) deleteSoftwareDownloadTrackingObject	This operation allows the OMS to notify the supplier management system that the software tracking object specified is no longer needed.
4) commit	This operation requests the supplier management system to install (commit) the downloaded software to target locations.
5) activate	This operation activates installed software at target locations.
6) revert	This operation activates older installed software at target locations.
7) getStatus	This operation requests the status of software activities.
8) scheduleDeliverDist	This operation schedules the delivery and distribution of software to specified targets.
9) scheduleCommit	This operation schedules the installation (commit) of software to predetermined targets.
10) scheduleActivate	This operation schedules the activation of software to predetermined targets.
11) cancelScheduledSoftwareActivity	This operation cancels all subsequently scheduled software download activities associated with this tracking object.
12) scheduledSoftwareDownloadTrackingObjectListGet	This operation retrieves the list of outstanding scheduled activities for software download.
13) onDemandSoftwareDownloadTrackingObjectListGet	This operation retrieves the list of outstanding non-scheduled activities for software download.

Figure 6-36 – Download manager operations

Operation signatures

Operation name	Input parameters	Return value	Exceptions
1) deliverDistSWGlobal	FilenameSeqType, DCNAddressType, UserIdType, PasswordType, ManagedEntityIdSeqType	SoftwareDownload TrackingObjectId Type	CommFailure, UnrecognisedTarget, InsufficientMemory, SoftwareLoadHWMismatch, SourceUnreachable, UnknownSoftwareLoad, Timeout, AccessDenied, DeniedAccess
2) deliverDistSWSpecific	FilenameSeqType, DCNAddressType, UserIdType, PasswordType, TargetType	SoftwareDownload TrackingObjectId Type	CommFailure, UnrecognisedTarget, InsufficientMemory, SoftwareLoadHWMismatch, SourceUnreachable, UnknownSoftwareLoad, Timeout, AccessDenied, DeniedAccess
3) deleteSoftwareDownload TrackingObject	SoftwareDownloadTracking ObjectIdType	void	UnknownSoftwareDownload TrackingObject, AccessDenied, SoftwareTrackingObjectInUse
4) commit	SoftwareDownloadTracking ObjectIdType, TargetType	void	InstallationFailure, UnknownSoftwareDownload TrackingObject, AccessDenied, UnrecognisedTarget
5) activate	SoftwareDownloadTracking ObjectIdType, TargetType	void	UnknownSoftwareDownload TrackingObject, SoftwareNotYetInstalled, ActivationFailure, AccessDenied, UnrecognisedTarget
6) revert	SoftwareDownloadTracking ObjectIdType, TargetType	void	UnknownSoftwareDownload TrackingObject, SoftwareNotYetInstalled, ActivationFailure, AccessDenied, UnrecognisedTarget, InvalidSoftwareTrackingObject
7) getStatus	SoftwareDownloadTracking ObjectIdType	DownloadStatusSeq Type	UnknownSoftwareDownload TrackingObject, AccessDenied
8) scheduleDeliverDist	FilenameSeqType DCNAddressType UserIdType PasswordType ManagedEntityIdSeqType GeneralizedTimeType	SoftwareDownload TrackingObjectId Type	SoftwareLoadHWMismatch, AccessDenied, InvalidStartTime
9) scheduleCommit	SoftwareDownloadTracking ObjectIdType, GeneralizedTimeType	void	UnknownSoftwareDownload TrackingObject, SoftwareNotYetInstalled, AccessDenied, InvalidStartTime
10) scheduleActivate	SoftwareDownloadTracking ObjectIdType, GeneralizedTimeType	void	UnknownSoftwareDownload TrackingObject, SoftwareNotYetInstalled, AccessDenied, InvalidStartTime

Operation name	Input parameters	Return value	Exceptions
11) cancelScheduledSoftware Activity	SoftwareDownloadTracking ObjectIdType	void	UnknownSoftwareDownload TrackingObject, ActivityCompleted, ActivityInProgress, AccessDenied
12) scheduledSoftwareDownload TrackingObjectListGet		SoftwareDownload TrackingObjectIdSeq Type	AccessDenied
13) onDemandSoftwareDownload TrackingObjectListGet		SoftwareDownload TrackingObjectIdSeq Type	AccessDenied

Figure 6-37 – Download manager signatures

Exceptions

Exception raised	Description
AccessDenied	System is not granted access to this interface object.
ActivationFailure	This exception is raised if the software activation process failed.
ActivityCompleted	The software activity has been executed and cannot be cancelled.
ActivityInProgress	This exception is raised when the software activity has been initiated and cannot be cancelled.
CommFailure	There was a DCN link failure between the NE and the supplier management system.
DeniedAccess	System is not granted access to the NE.
InstallationFailure	Software installation process failed.
InsufficientMemory	There is insufficient memory on the NE to load the software unit.
InvalidSoftwareTrackingObject	The referenced software tracking object is not the most recent associated with the installation of a software load on the NE.
InvalidStartTime	The start time is inconsistent with the current time, the current trigger time matrix or the new stop time.
SoftwareLoadHWMismatch	The designated software may not be loaded onto the equipment hardware since the version of the hardware cannot accept the software load.
SoftwareNotYetInstalled	The software may not be activated since it has not been installed yet.
SoftwareTrackingObjectInUse	Indicates that software download has been completed so that the process cannot be cancelled.
SourceUnreachable	The server holding the software load to be downloaded could not be reached by the OLT.
Timeout	The process duration reached a system-defined timeout before the process could complete.
UnknownSoftwareLoad	The specified software unit cannot be found.
UnknownSoftwareDownloadTrackingObject	The named software activity is unknown to the supplier management system.
UnrecognisedTarget	The designated software in the secure file server is unknown to the supplier management system.

Figure 6-38 – Download manager exceptions

6.3.3.2 Backup and restore NE

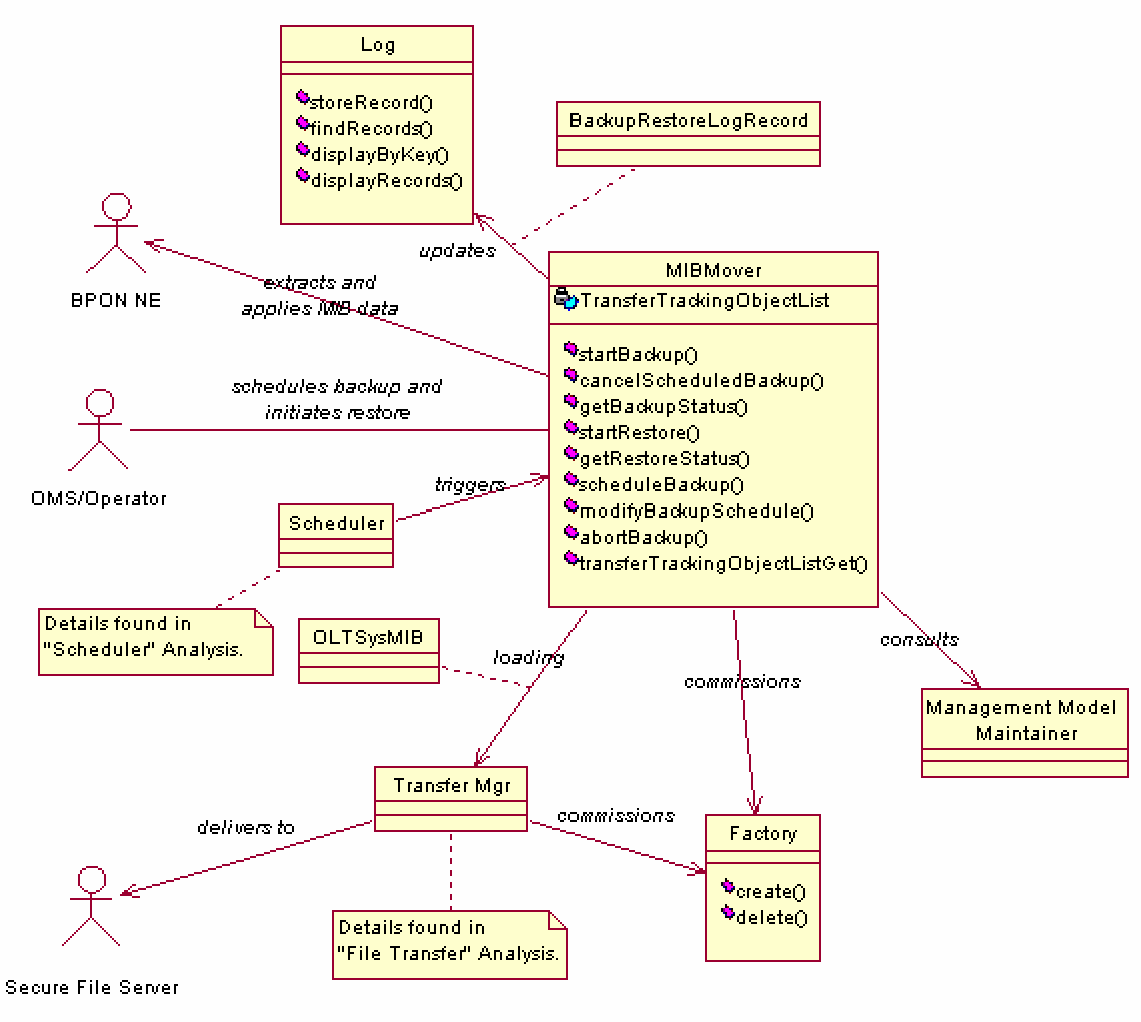


Figure 6-39 – NE data backup and restore class diagram

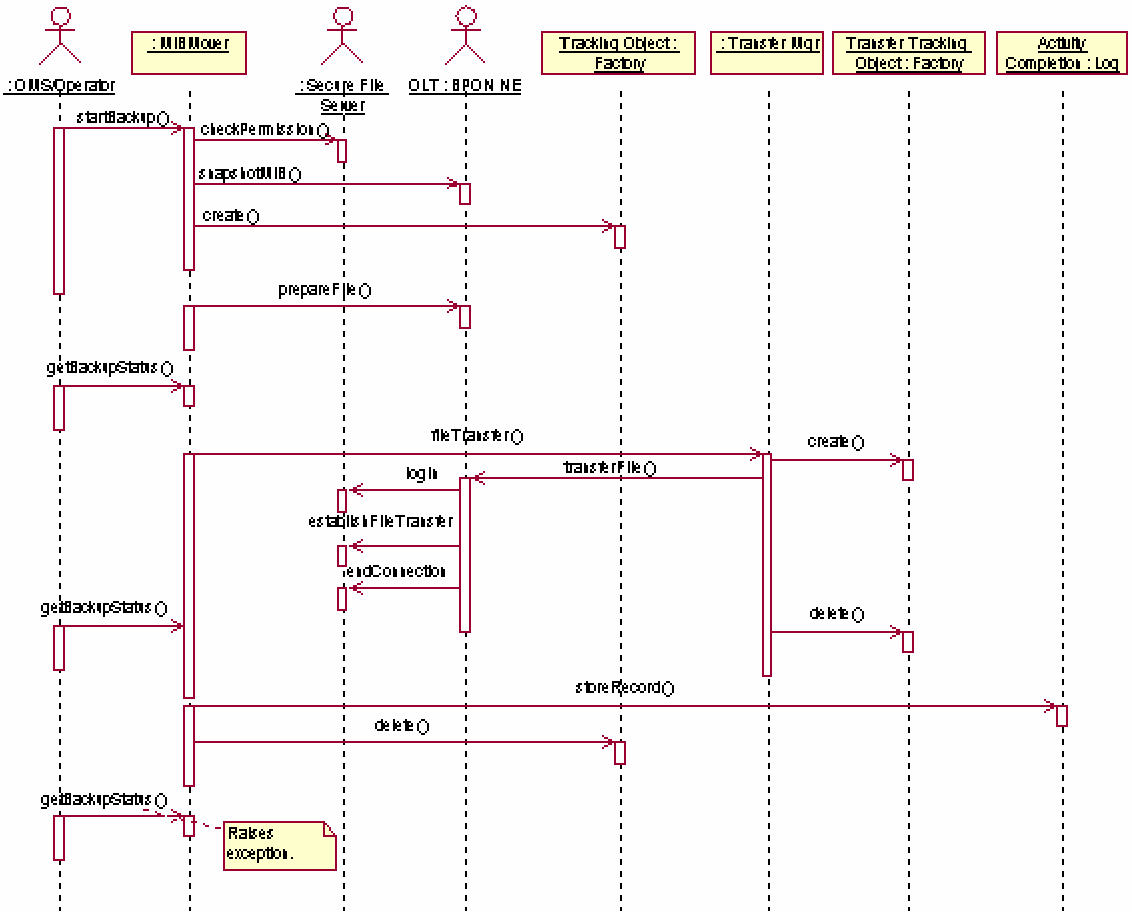


Figure 6-40 – Immediate NE backup sequence diagram[9]

[9] If the MIB is stewarded within the supplier management system, then the MIB snapshot, file creation and file transfer is accomplished within the supplier management system and not the OLT.

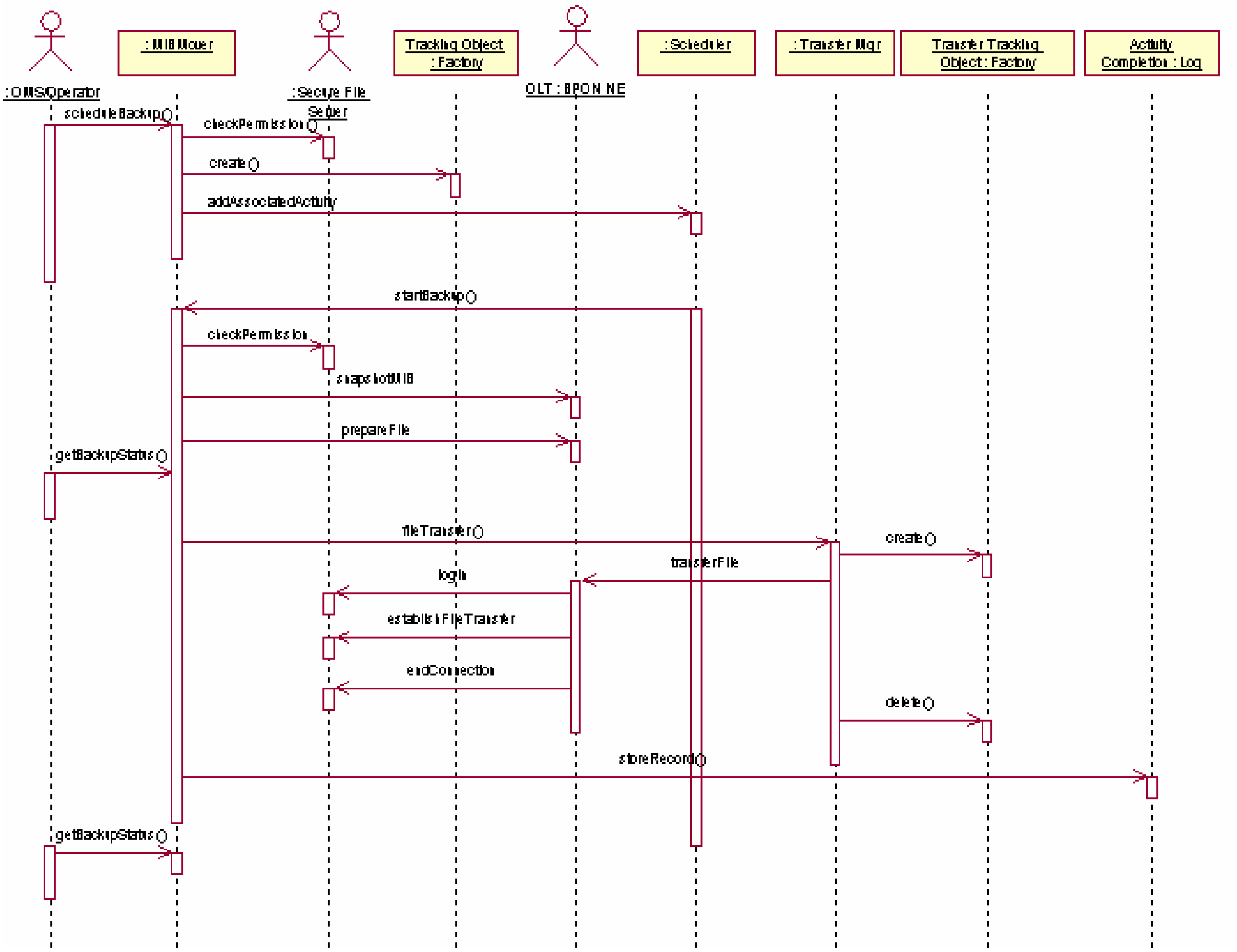


Figure 6-41 – Scheduled NE backup sequence diagram[10]

[10] If the MIB is stewarded within the supplier management system, then the MIB snapshot, file creation and file transfer is accomplished within the supplier management system and not the OLT.

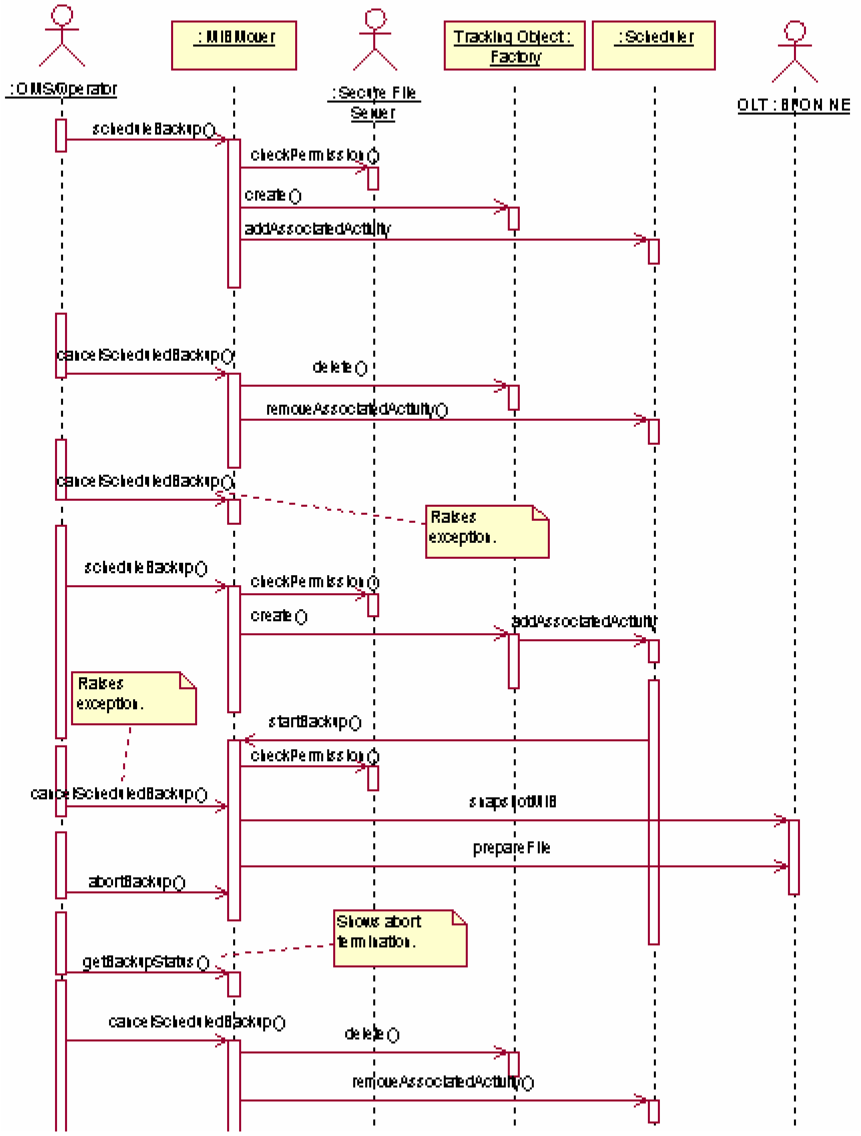


Figure 6-42 – Cancel scheduled NE backup sequence diagram

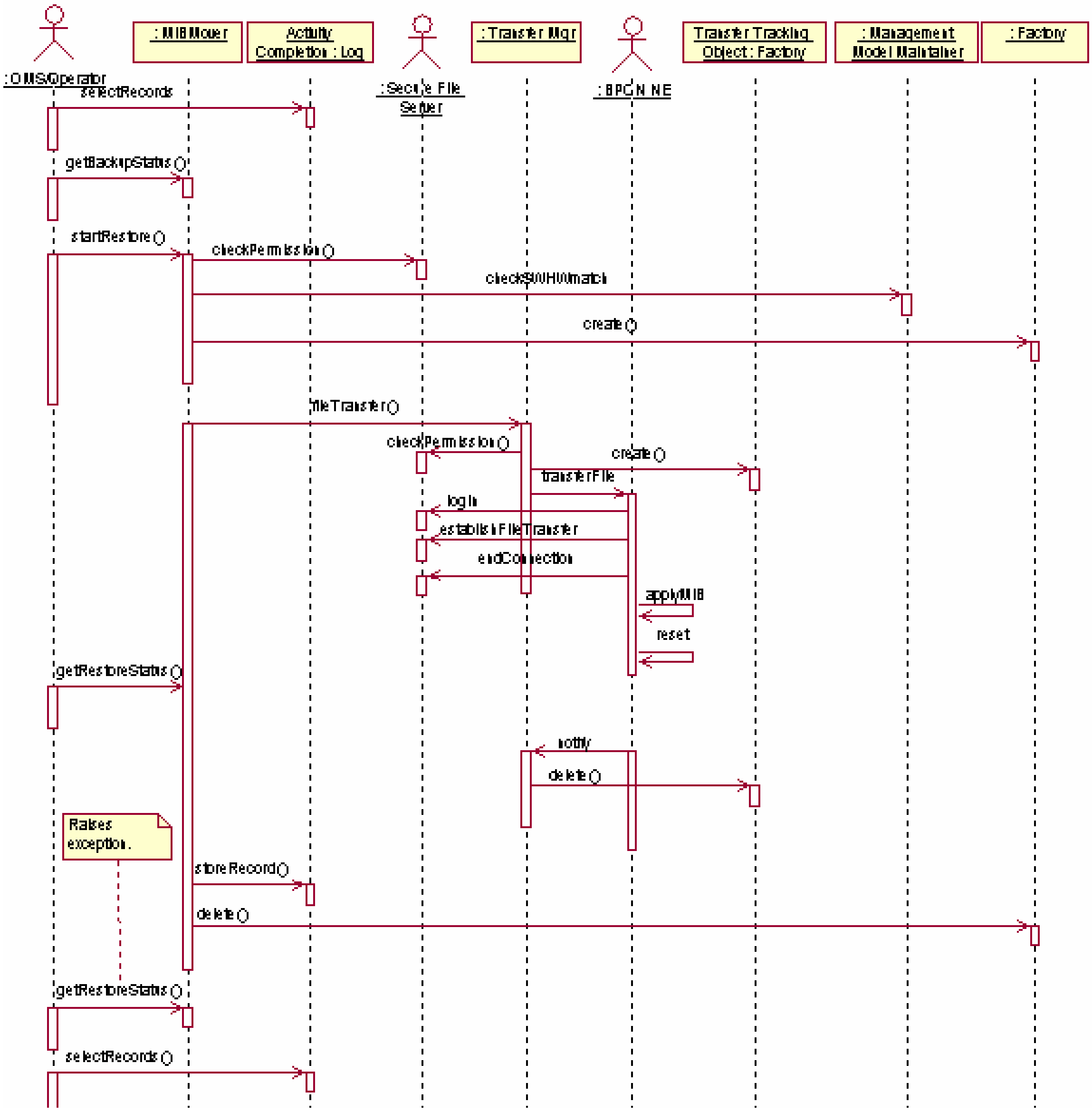


Figure 6-43 – Restore NE sequence diagram

Operations

Operation name	Operation purpose
1) startBackup	This operation initiates an immediate backup of system configuration data from a system and/or supplier management system to a backup server destination.
2) getBackupStatus	This operation provides the capability to retrieve the status of a backup process.
3) scheduleBackup	This operation cancels all subsequent backup processes for a system based on a scheduler. This operation will not interrupt a backup process in progress.
4) modifyBackupSchedule	This operation cancels all subsequent backup processes for a system based on a scheduler.
5) cancelScheduledBackup	This operation aborts a backup process in progress whether scheduled or not. Subsequent scheduled backup process are not affected by this operation.
6) abortBackup	This operation aborts a backup process in progress whether scheduled or not. Subsequent scheduled backup process are not affected by this operation.
7) startRestore	This operation provides functionality to restore a system based on a backed up copy of configuration data.
8) getRestoreStatus	This operation provides the status of a restoral process.
9) transferTrackingObjectIdListGet	This operation retrieves the list of outstanding system MIB transfers, both backup and restore.

Figure 6-44 – MIB mover operations

Operation signatures[11]

Operation name	Input parameters	Return value	Exceptions
1) startBackup	ManagedEntityIdType (NE), DCNAddressType, UserIdType, PasswordType, FilenameType, boolean (overwrite file?)	TransferTrackingObjectId Type	UnknownNE, UnknownDestinationServer, CommFailure, EquipmentFailure, DeniedAccess, AccessDenied
2) getBackupStatus	TransferTrackingObjectIdType	StatusAttributeSeqType	UnknownBackupProcess, AccessDenied
3) scheduleBackup	ManagedEntityIdType (NE), UserIdType, PasswordType, UserLabelType, DCNAddressType, FilenameType, boolean (overwrite file?)	TransferTrackingObjectId Type	UnknownNE, UnknownDestination Server, UnknownScheduler, InvalidScheduler, AccessDenied
4) modifyBackupSchedule	TransferTrackingObjectIdType, UserLabelType	void	UnknownBackupProcess, AccessDenied, UnknownScheduler, InvalidScheduler
5) cancelScheduledBackup	TransferTrackingObjectIdType,	void	UnknownBackupProcess, AccessDenied
6) abortBackup	TransferTrackingObjectIdType,	void	UnknownBackupProcess, CommFailure, EquipmentFailure, AccessDenied
7) startRestore	ManagedEntityIdType (NE), DCNAddressType, UserIdType, PasswordType, FilenameType	TransferTrackingObjectId Type	UnknownNE, CommFailure, EquipmentFailure, UnknownSourceServer, DeniedAccess, SoftwareLoadHardware Mismatch, AccessDenied
8) getRestoreStatus	TransferTrackingObjectIdType	StatusAttributeSeqType	UnknownRestoreProcess, AccessDenied
9) transferTrackingObjectId ListGet		TransferTrackingObjectId SeqType	AccessDenied

Figure 6-45 – MIB mover signatures

[11] The operation "overWriteBackup" has the same behaviour as "startBackup" except that the named destination file (the target) may be non-empty.

Exceptions

Exception raised	Description
AccessDenied	System is not granted access to this interface object.
CommFailure	There was a DCN link failure between the NE and the supplier management system.
DeniedAccess	System is not granted access to the NE.
EquipmentFailure	The NE currently has a failure condition preventing the requested transaction from being completed.
InvalidScheduler	The scheduler parameters values are outside defined scope.
SoftwareLoadHardwareMismatch	The former NE configuration data could not be downloaded to the NE because there were changes made to the NE hardware that caused an incapability.
UnknownBackupProcess	The named transfer-tracking object identifying the file transfer process is unknown to the supplier management system.
UnknownDestinationServer	The identified destination server cannot be accessed by the transfer agent.
UnknownNE	Identified NE is unknown to the supplier management system.
UnknownRestoreProcess	The name restore activity is unknown to the supplier management system.
UnknownScheduler	The named scheduler is unknown to the supplier management system.
UnknownSourceServer	The supplier management system and/or OLT cannot communicate with the source server. The DCN address is unknown or access is blocked.

Figure 6-46 – MIB mover exceptions

6.3.3.3 NE software version control

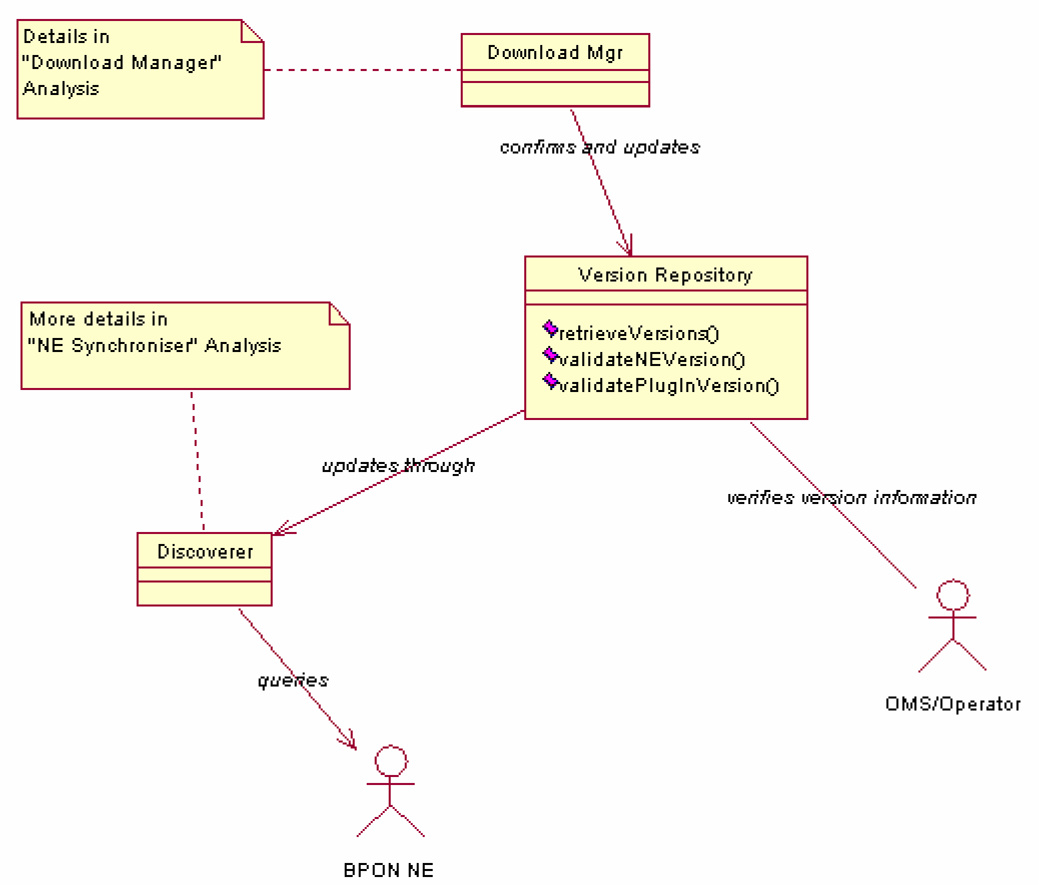


Figure 6-47 – NE software version control class diagram

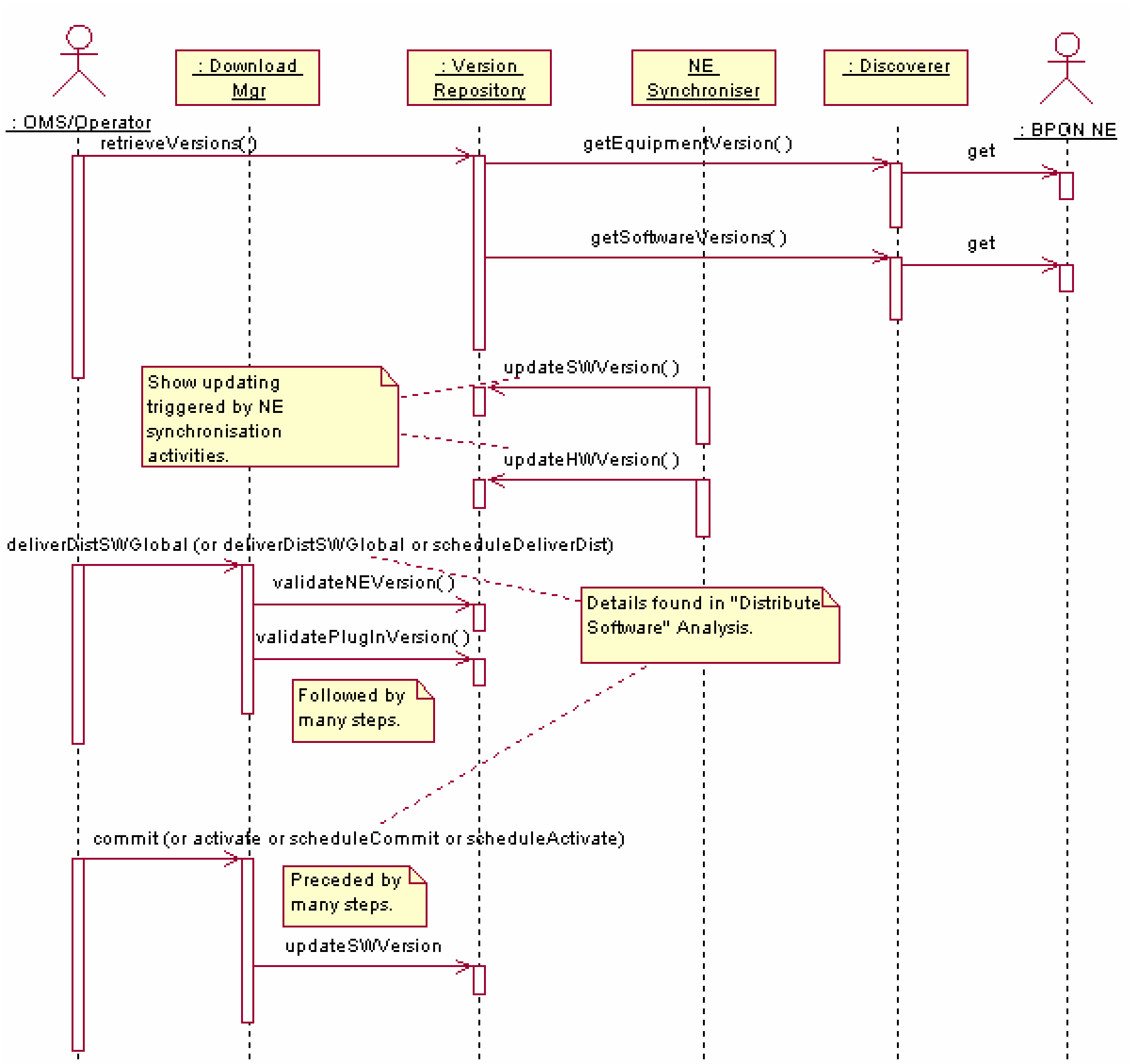


Figure 6-48 – NE software version control sequence diagram

Operations

Operation name	Operation purpose
1) retrieveVersions	This operation retrieves all version information (both software and hardware) for a network resource.
2) validateNEVersion	This operation requests the supplier management system to validate if the proposed software is compatible with the the NE.
3) validatePlugInVersion	This operation requests the supplier management system to validate if the proposed software is compatible with the plugInUnit.

Figure 6-49 – Version repository operations

Operation signatures

Operation name	Input parameters	Return value	Exceptions
1) retrieveVersions	ManagedEntityIdType	VersionsSeqType	CommFailure, UnknownManagedEntity, AccessDenied
2) validateNEVersion	ManagedEntityIdType, VersionType	boolean (valid?)	UnknownNE, AccessDenied
3) validatePlugInVersion	ManagedEntityIdType, VersionType	boolean (valid?)	UnknownManagedEntity, AccessDenied

Figure 6-50 – Version repository signatures

Exceptions

Exception raised	Description
AccessDenied	System is not granted access to this interface object.
CommFailure	There was a DCN link failure between the NE and the supplier management system.
UnknownManagedEntity	The specified managed entity is unknown to the supplier management system.

Figure 6-51 – Version repository exceptions

6.3.3.4 Scheduler

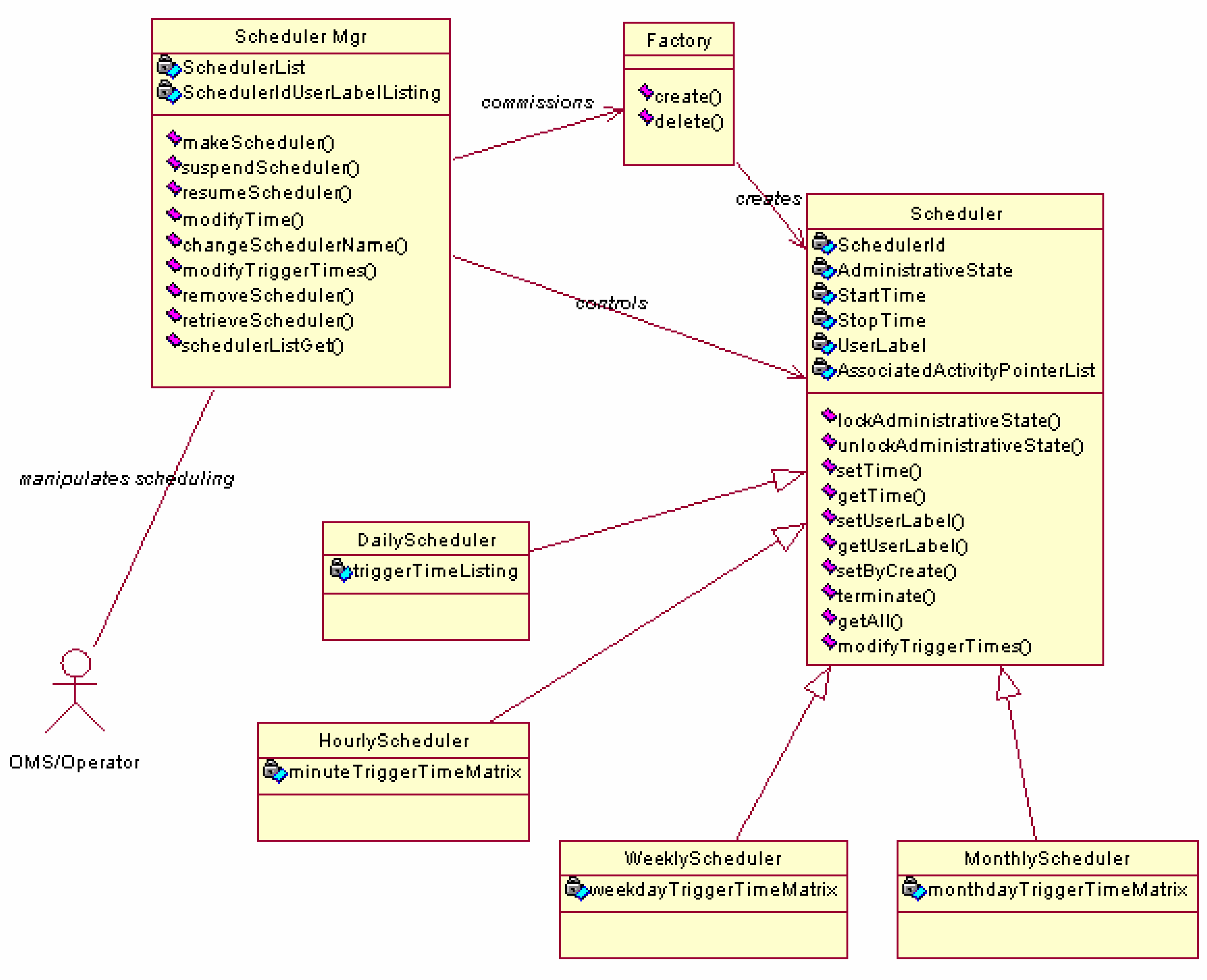


Figure 6-52 – Scheduler management class diagram

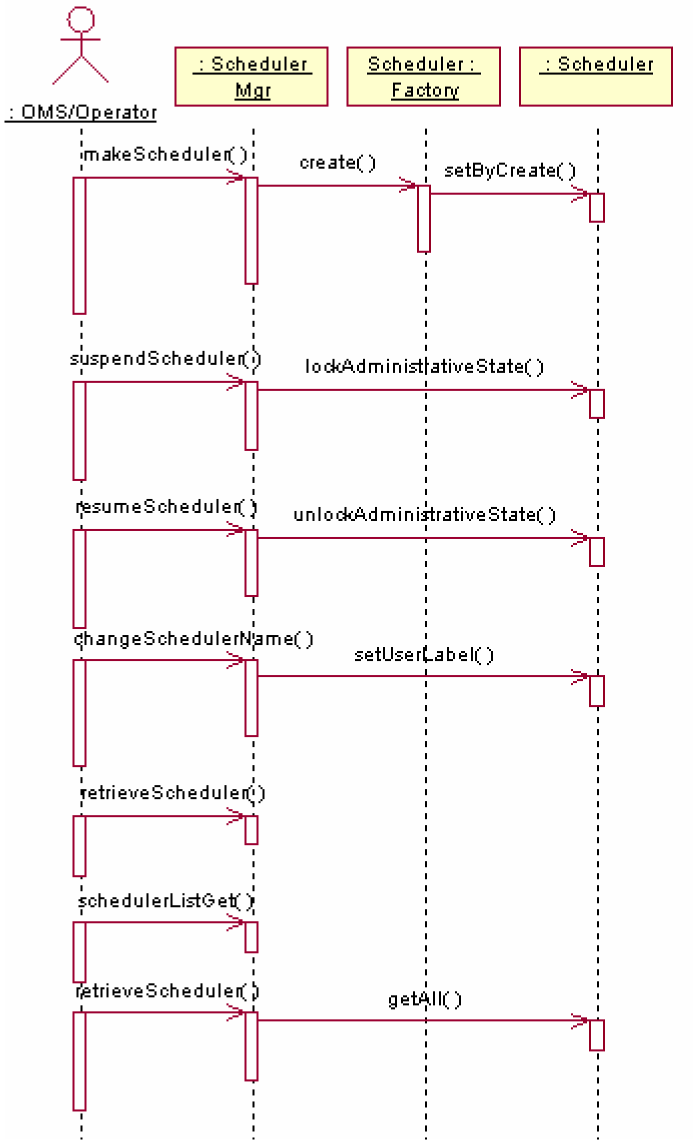
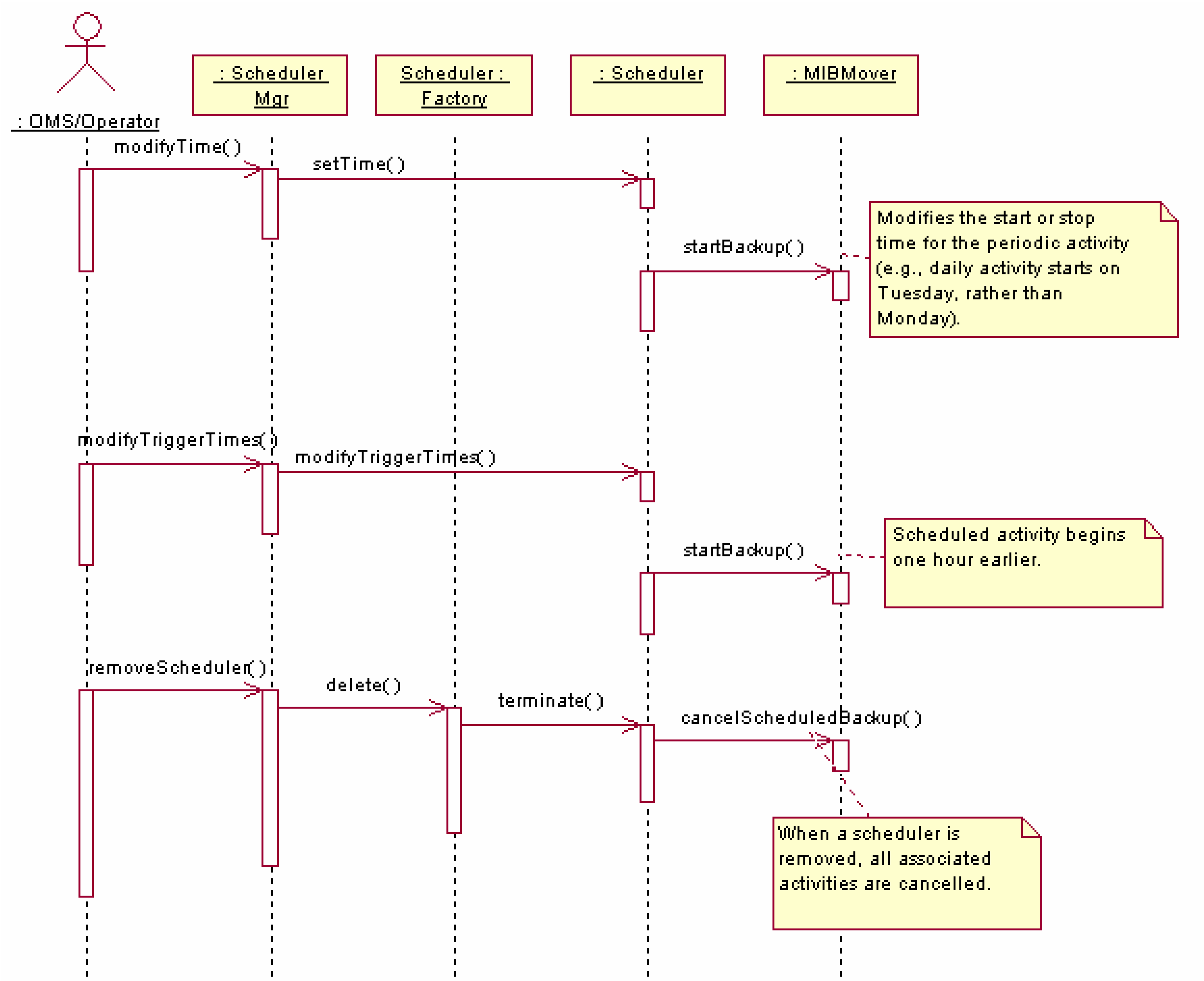


Figure 6-53 – Scheduler control sequence diagram



: OMS/Operator
: Scheduler Mgr
Scheduler : Factory
: Scheduler
: MIBMover
modifyTime( )
setTime( )
startBackup( )
Modifies the start or stop time for the periodic activity (e.g., daily activity starts on Tuesday, rather than Monday).
modifyTriggerTimes( )
modifyTriggerTimes( )
startBackup( )
Scheduled activity begins one hour earlier.
removeScheduler( )
delete( )
terminate( )
cancelScheduledBackup( )
When a scheduler is removed, all associated activities are cancelled.

Figure 6-54 – Scheduler modifications sequence diagram[12]

Operations

Operation name	Operation purpose
1) makeScheduler	This operation creates a new scheduler object.
2) suspendScheduler	This operation is used to suspend a schedule.
3) resumeScheduler	This operation is used to resume a suspended schedule.
4) modifyTime	This operation is used in order to change the startTime and stopTime of a schedule.
5) changeSchedulerName	This operation is used to change the name of the scheduler object.
6) modifyTriggerTimes	This operation is used by the OMS to specify new trigger times and iteration for a scheduler.
7) removeScheduler	This operation is used to delete a scheduler.
8) retrieveScheduler	This operation is used to retrieve information on the schedule.
9) schedulerListGet	This operation is used to retrieve the names of all existing schedulers defined for the supplier management system.

Figure 6-55 – Scheduler operations

[12] This sequence diagram uses an associated scheduled activity of MIB backup as an example. There can be others, and more than one associated with a given scheduler.

Operation signatures

Operation name	Input parameters	Return value	Exceptions
1) makeScheduler	UserLabelType, GeneralizedTimeType (start time), GeneralizedTimeType (stop time), HourlyDailyWeeklyMonthlyIndType, TriggerTimeMatrixSeqType	void	InvalidStartTime, InvalidStopTime, DuplicateUserLabel, MatrixSchedulerType Mismatch, AccessDenied, InvalidTrigger
2) suspendScheduler	UserLabelType	void	UnknownScheduler, AccessDenied
3) resumeScheduler	UserLabelType	void	UnknownScheduler, AccessDenied
4) modifyTime	UserLabelType, GeneralizedTimeType (start time), GeneralizedTimeType (stop time)	void	InvalidStartTime, InvalidStopTime, UnknownScheduler, AccessDenied
5) changeSchedulerName	UserLabelType (old name), UserLabelType (new name)	void	UnknownScheduler, DuplicateUserLabel, AccessDenied
6) modifyTriggerTimes	UserLabelType, HourlyDailyWeeklyMonthlyIndType, TriggerTimeMatrixSeqType	void	UnknownScheduler, MatrixSchedulerType Mismatch, InvalidTrigger, AccessDenied
7) removeScheduler	UserLabelType	void	UnknownScheduler, AccessDenied, ScheduleInUse
8) retrieveScheduler	UserLabelType	SchedulerType	UnknownScheduler, AccessDenied
9) schedulerListGet		SchedulerSeqType	AccessDenied

Figure 6-56 – Scheduler signatures

Exceptions

Exception raised	Description
AccessDenied	System is not granted access to this interface object.
DuplicateUserLabel	The user label provided in the request has been used to label another scheduler.
InvalidStartTime	The new start time is inconsistent with the current time, the current trigger time matrix or the new stop time.
InvalidStopTime	The new stop time is inconsistent with the current time, the current trigger time matrix or the new start time.
InvalidTrigger	The specified trigger has values that cannot be interpreted by the scheduler.
MatrixSchedulerTypeMismatch	The syntax for the trigger time matrix is mismatched with the type of scheduler named.
ScheduleInUse	There are still activities scheduled by the named scheduler.
UnknownScheduler	The named scheduler is unknown to the supplier management system.

Figure 6-57 – Scheduler exceptions

6.3.4 Testing

6.3.4.1 Conduct tests

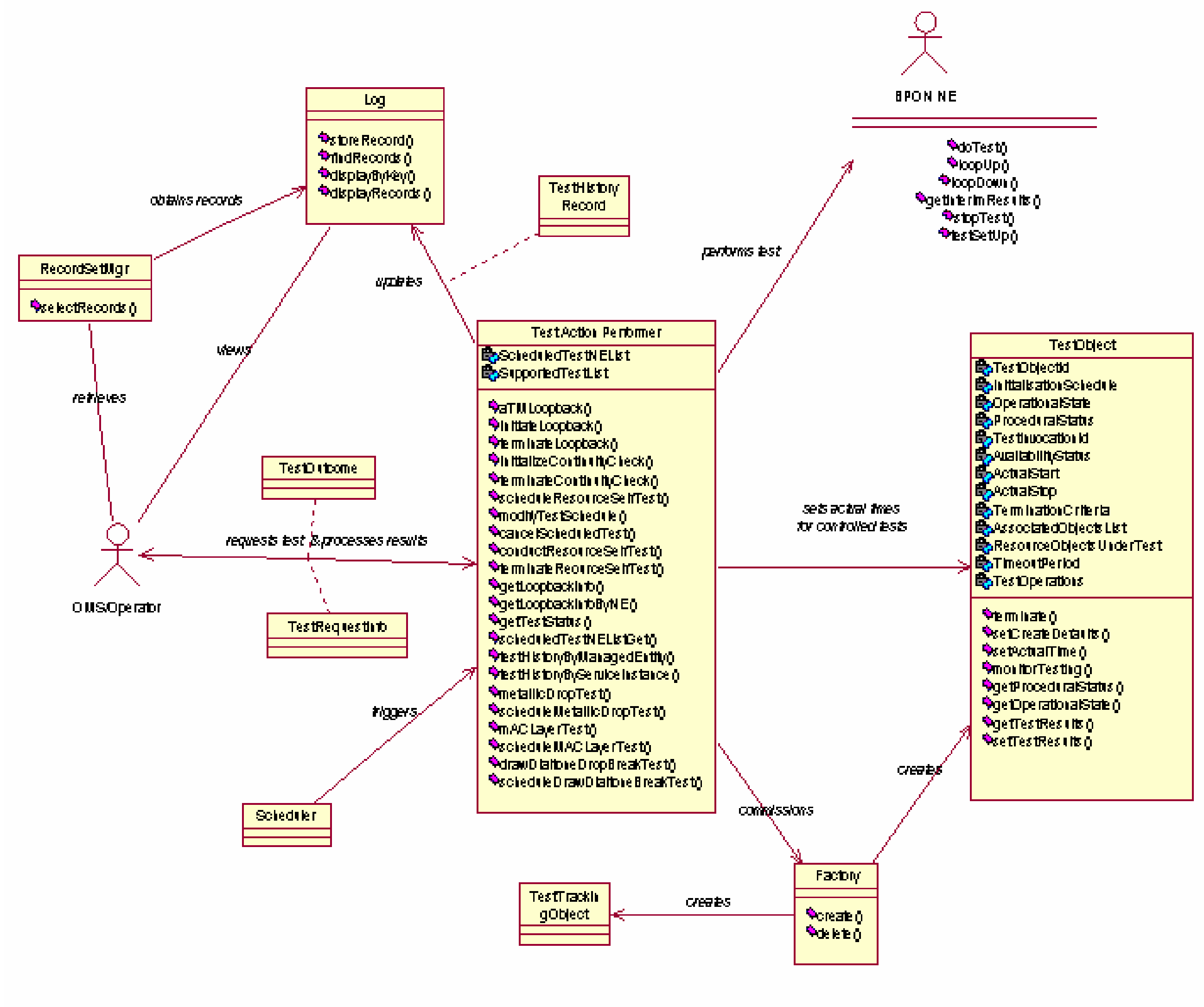


Figure 6-58 – Conduct tests and report results class diagram

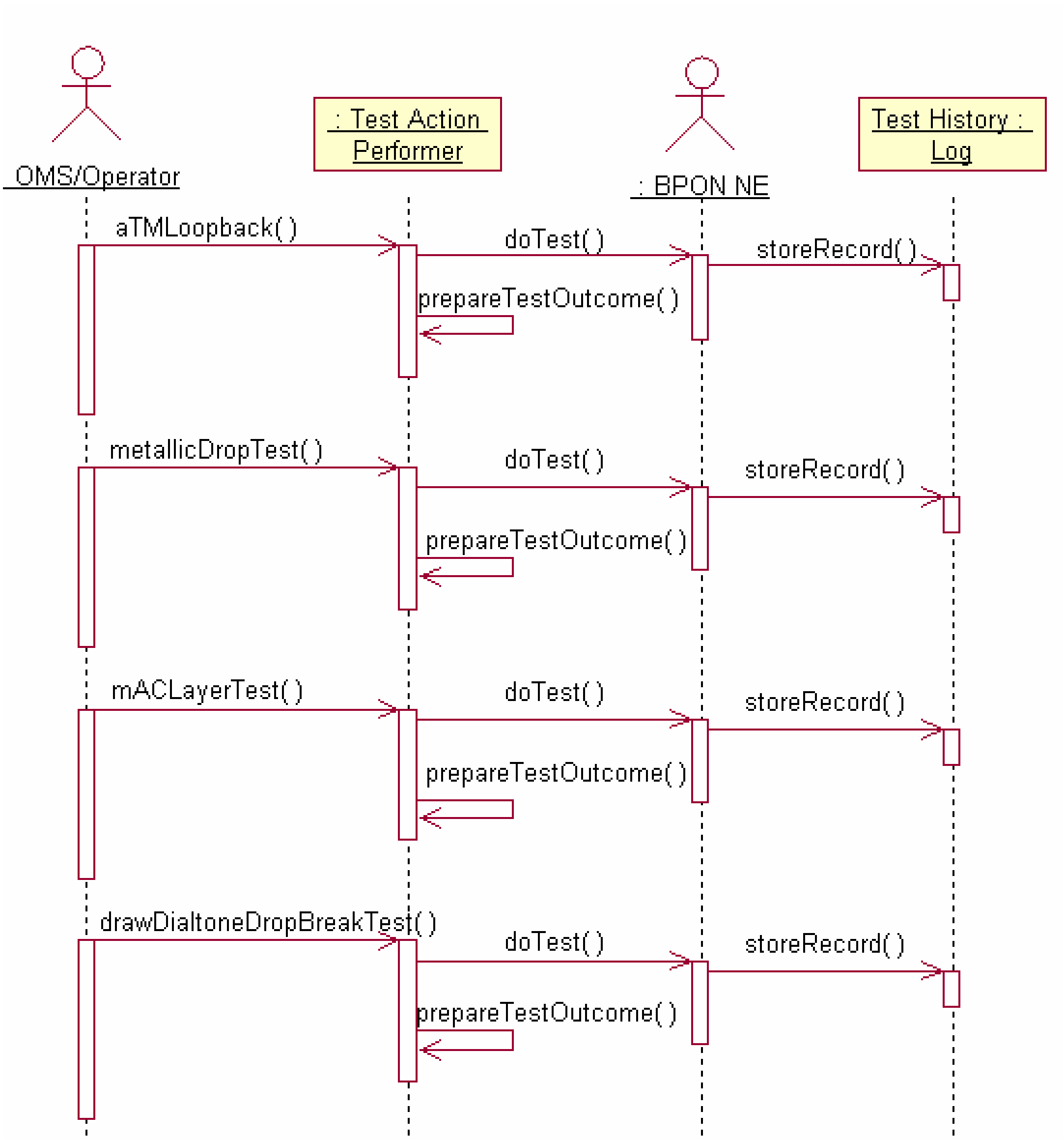


Figure 6-59 – Conduct uncontrolled tests sequence diagram

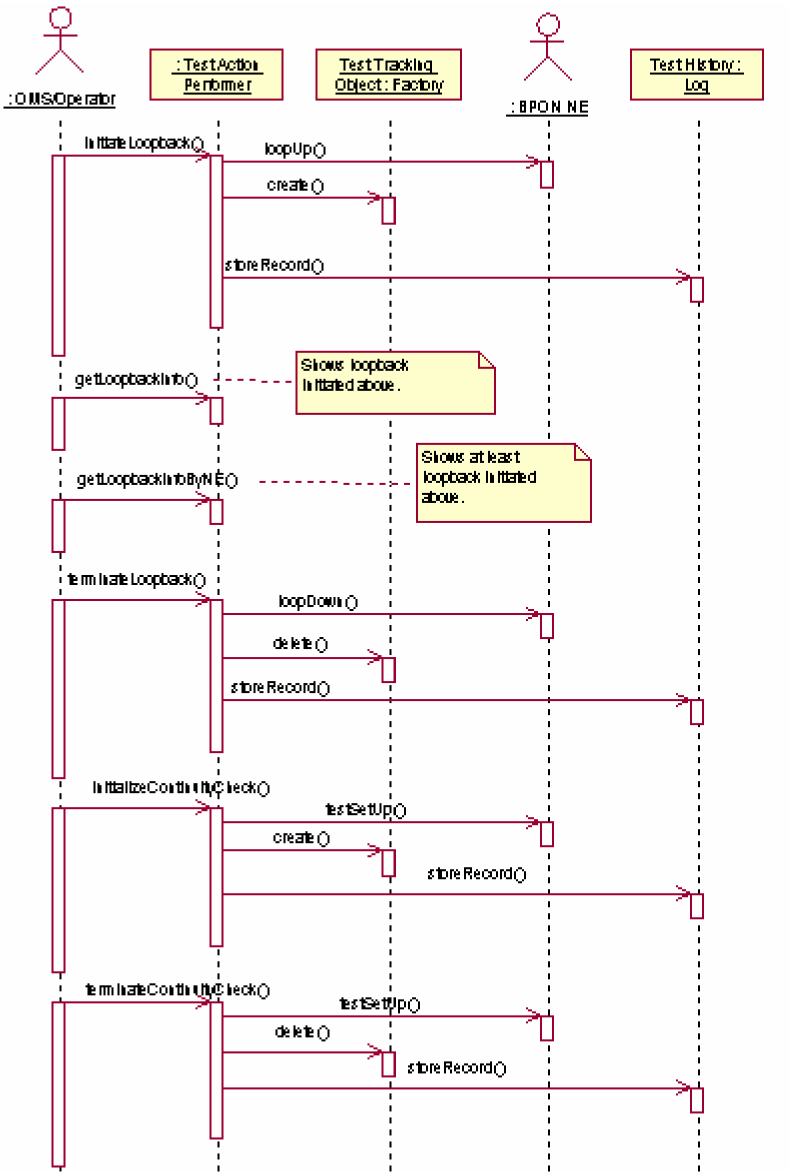


Figure 6-60 – Test set up sequence diagram

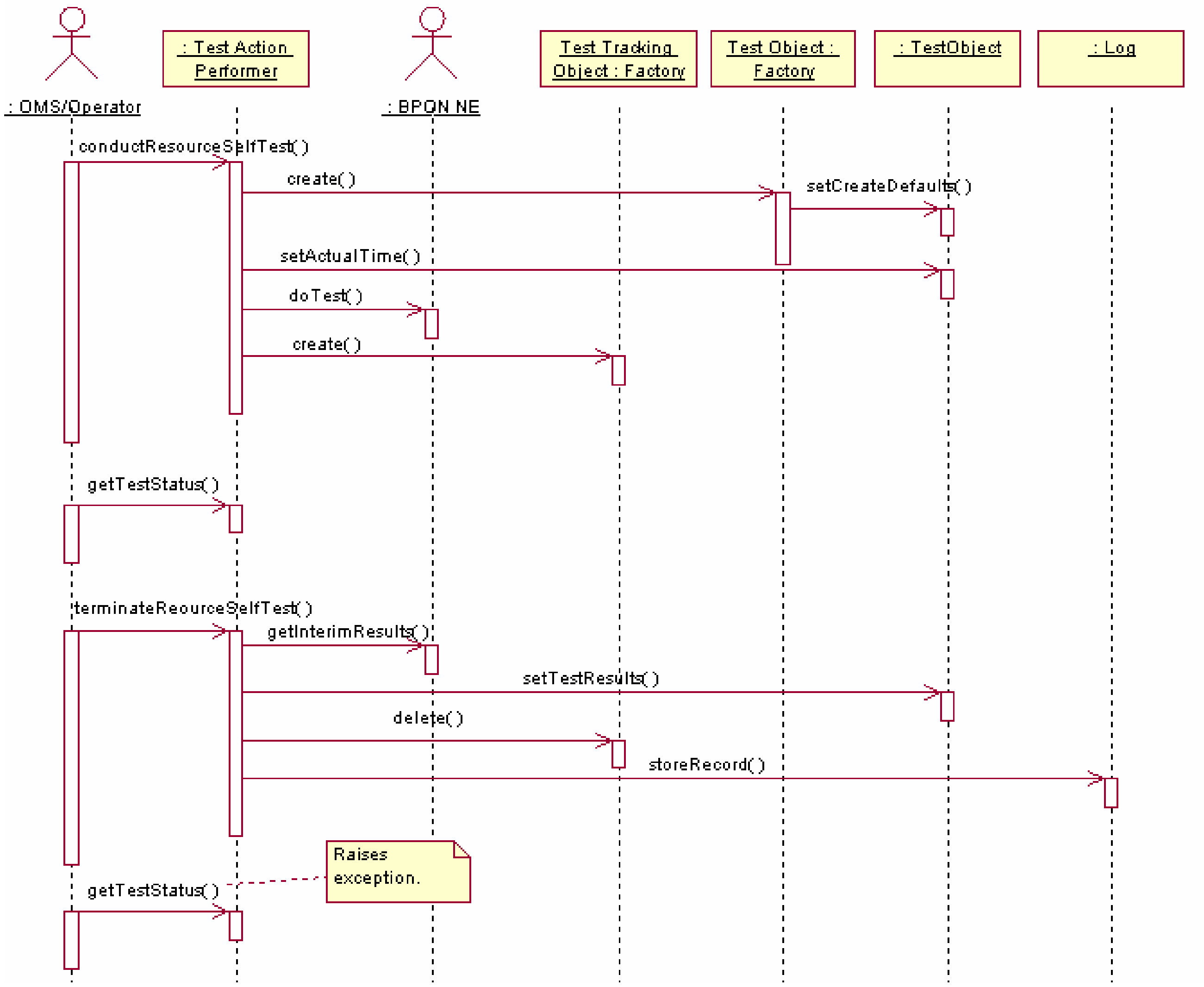


Figure 6-61 – Controlled test sequence diagram

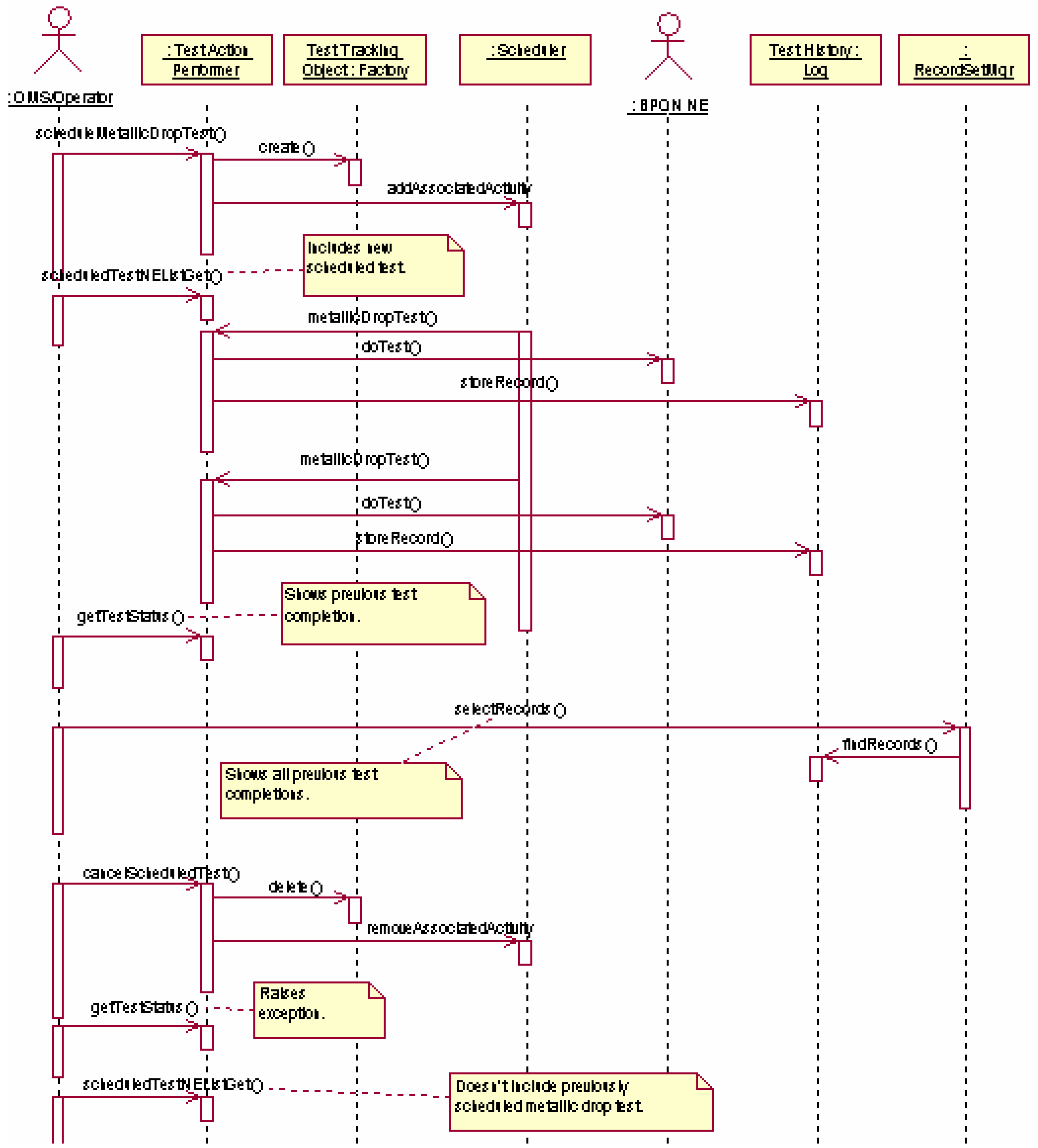


Figure 6-62 – Schedule test and view status sequence diagram[13]

[13] Using MetallicDropTest as one example. All other scheduled tests would have similar behavioural characteristics.

Operations

Operation name	Operation purpose
1) aTMLoopback	This operation is used to invoke an ATM OAM loopback test.
2) initializeContinuityCheck	This operation is used to prepare for an ATM continuity check.
3) terminateContinuityCheck	This operation is used to take down the ATM continuity test environment.
4) scheduleResourceSelfTest	This operation is used to schedule a resource self test.
5) modifyTestSchedule	This operation is used to modify the schedule for a regularly conducted test.
6) cancelScheduledTest	This operation is used to cancel a regularly scheduled test.
7) conductResourceSelfTest	This operation is used to initiate a resource self test following the identification of a system fault or a subscriber service complaint.
8) terminateResourceSelfTest	This operation terminates a resource self test in progress.
9) initiateLoopback	This operation is used to initiate a loopback for a service.
10) terminateLoopback	This operation is used to cancel a running loopback.
11) getLoopbackInfo	This operation is used to retrieve the loopback information of a particular connection termination point.
12) getLoopbackInfoByNE	This operation is used to retrieve the location and details of every connection point in an NE that are in loopback mode.
13) getTestStatus	This operation is used to retrieve the status of a loopback in progress.
14) scheduledTestNEListGet	This operation is used to retrieve the list of all scheduled NE testing.
15) testHistoryByManagedEntity	This operation is used to retrieve the test history associated with a managed entity.
16) testHistoryByServiceInstance	This operation is used to retrieve the test history associated with a service instance.
17) metallicDropTest	This operation is used to conduct a metallic drop test following the identification of a system fault or a subscriber service complaint.
18) scheduleMetallicDropTest	This operation is used to schedule a metallic trop test.
19) mACLayerTest	This operation is used to conduct a MAC layer test following the identification of a system fault or a subscriber service complaint.
20) scheduleMACTest	This operation is used to schedule a MAC layer test.
21) drawDialToneBreakTest	This operation is used to conduct a telephony service related test following the identification of a system fault or a subscriber service complaint.
22) scheduleDrawDialToneBreakTest	This operation is used by the OMS to set up draw dialtone/break dialtone testing for telephony service ports to be executed at a regular basis.

Figure 6-63 – Test action performer operations

Operation signatures[14]

Operation name	Input parameters	Return value	Exceptions
1) aTMLoopback	UserIdType, ManagedEntityIdType (TP), ATMLoopbackInfoType, TestIterationNumType, ServiceInstanceIdType	AggregateATM LoopbackResult SeqType	AccessDenied, CommFailure, UnknownManagedEntity, NotAvailableForTest, InvalidLocationId, InvalidDirection
2) initializeContinuityCheck	UserIdType, ManagedEntityIdType (TP), ATMContinuityCheckInfoType, GeneralizedTimeType, ServiceInstanceIdType	CCSetUpIdType	AccessDenied, CommFailure, UnknownManagedEntity, NotAvailableForTest, InvalidStartTime, InvalidStopTime, InvalidDirection
3) terminateContinuityCheck	CCSetUpIdType	void	AccessDenied, CommFailure, UnknownTest
4) scheduleResourceSelfTest	UserIdType, ManagedEntityIdType (NE), unsigned long (timeout), ResourceSelfTestInfoSeqType, UserLabelType (scheduler)	TestTrackingObject IdType	AccessDenied, UnknownNE, UnknownScheduler, InvalidScheduler, InvalidTimeoutPeriod, InvalidTestOperations
5) modifyTestSchedule	TestTrackingObjectIdType, UserLabelType (new scheduler)	TestTrackingObject IdType	UnknownTest, UnknownScheduler, InvalidScheduler, AccessDenied
6) cancelScheduledTest	TestTrackingObjectIdType	void	UnknownTest, UncontrolledTestInProgress, AccessDenied
7) conductResourceSelfTest	UserIdType, ManagedEntityIdType (NE), unsigned long (timeout), ResourceSelfTestInfoType	TestTracking ObjectId	AccessDenied, CommFailure, UnknownNE, InvalidTimeoutPeriod, InvalidTestOperations
8) terminateResourceSelfTest	TestTrackingObjectIdType	ResourceSelfTest ResultSeqType	UnknownTest, UncontrolledTestInProgress, AccessDenied
9) initiateLoopback	UserIdType, ManagedEntityIdType (TP), long (duration), DirectionalityType, LoopbackTestType, ServiceInstanceIdType	LoopbackTracking ObjectIdType	AccessDenied, CommFailure, UnknownManagedEntity, NotAvailableForTest
10) terminateLoopback	LoopbackTrackingObjectId	void	UnknownTest, AccessDenied
11) getLoopbackInfo	ManagedEntityIdType (TP)	LoopbackInfoType	UnknownManagedEntity, AccessDenied
12) getLoopbackInfoByNE	ManagedEntityIdType (NE)	LoopbackInfo SeqType	UnknownManagedEntity, AccessDenied
13) getTestStatus	LoopbackTrackingObjectIdType	StatusValueType	UnknownTest, AccessDenied
14) scheduledTestNEListGet		ScheduledTestNE SeqType	AccessDenied
15) testHistoryByManagedEntity	ManagedEntityIdType	TestHistorySeqType	AccessDenied, UnknownManagedEntity

[14] At the moment, controlled testing is not required for BPON network resources. However, for the sake of completeness, two operations called "requestControlledTest" and "requestScheduledControlledTest" have been included and shown in the sequence diagrams. Scheduled tests can be periodic.

Operation name	Input parameters	Return value	Exceptions
16) testHistoryByServiceInstance	ServiceInstanceIdType	TestHistorySeqType	AccessDenied, UnknownServiceInstance
17) metallicDropTest	UserIdType, ManagedEntityIdType (port), ServiceInstanceIdType	DropTestResultsType	AccessDenied, CommFailure, UnknownManagedEntity
18) scheduleMetallicDropTest	UserIdType, ManagedEntityIdType (port), ServiceInstanceIdType, UserLabelType (scheduler)	TestTrackingObject IdType	AccessDenied, UnknownManagedEntity, UnknownScheduler, InvalidScheduler
19) mACLayerTest	UserIdType, ManagedEntityIdType (port), ServiceInstanceIdType	short	AccessDenied, CommFailure, UnknownManagedEntity
20) scheduleMACTest	UserIdType, ManagedEntityIdType (port), ServiceInstanceIdType, UserLabelType (scheduler)	TestTrackingObject IdType	AccessDenied, UnknownManagedEntity, UnknownScheduler, InvalidScheduler
21) drawDialToneBreakTest	UserIdType, ManagedEntityId Type (port), ServiceInstanceIdType	boolean	AccessDenied, CommFailure, UnknownManagedEntity
22) scheduleDrawDialToneBreak Test	UserIdType, ManagedEntityIdType (port), ServiceInstanceIdType, UserLabelType (scheduler)	TestTrackingObject IdType	AccessDenied, UnknownManagedEntity, UnknownScheduler, InvalidScheduler

Figure 6-64 – Test action performer signatures

Exceptions

Exception raised	Description
AccessDenied	System is not granted access to this interface object.
CommFailure	There was a DCN link failure between the NE and the supplier management system.
InvalidDirection	Identified test operations unknown to the supplier management system.
InvalidLocationId	The LLID specified is not valid.
InvalidScheduler	The scheduler parameters values are outside defined scope.
InvalidStartTime	The new start time is inconsistent with the current trigger time matrix or the new stop time.
InvalidStopTime	The new stop time is inconsistent with the current trigger time matrix or the new start time.
InvalidTestOperations	The requested self test operation is not valid.
InvalidTimeoutPeriod	Designated timeout period violates definition of valid values.
NotAvailableForTest	The specified CTP is not available for this test.
UncontrolledTestInProgress	The scheduled test cannot be cancelled because of an uncontrolled test in progress.
UnknownManagedEntity	The specified managed entity is unknown to the supplier management system.
UnknownNE	Identified NE is unknown to the supplier management system.
UnknownScheduler	The named scheduler is unknown to the supplier management system.
UnknownServiceInstance	The service instance is unknown to the supplier management system.
UnknownTest	The test specified by the TestTrackingObjectId is not known in the supplier management system.

Figure 6-65 – Test action performer exceptions

6.3.5 Installation

6.3.5.1 Synchronize NE and current event listing

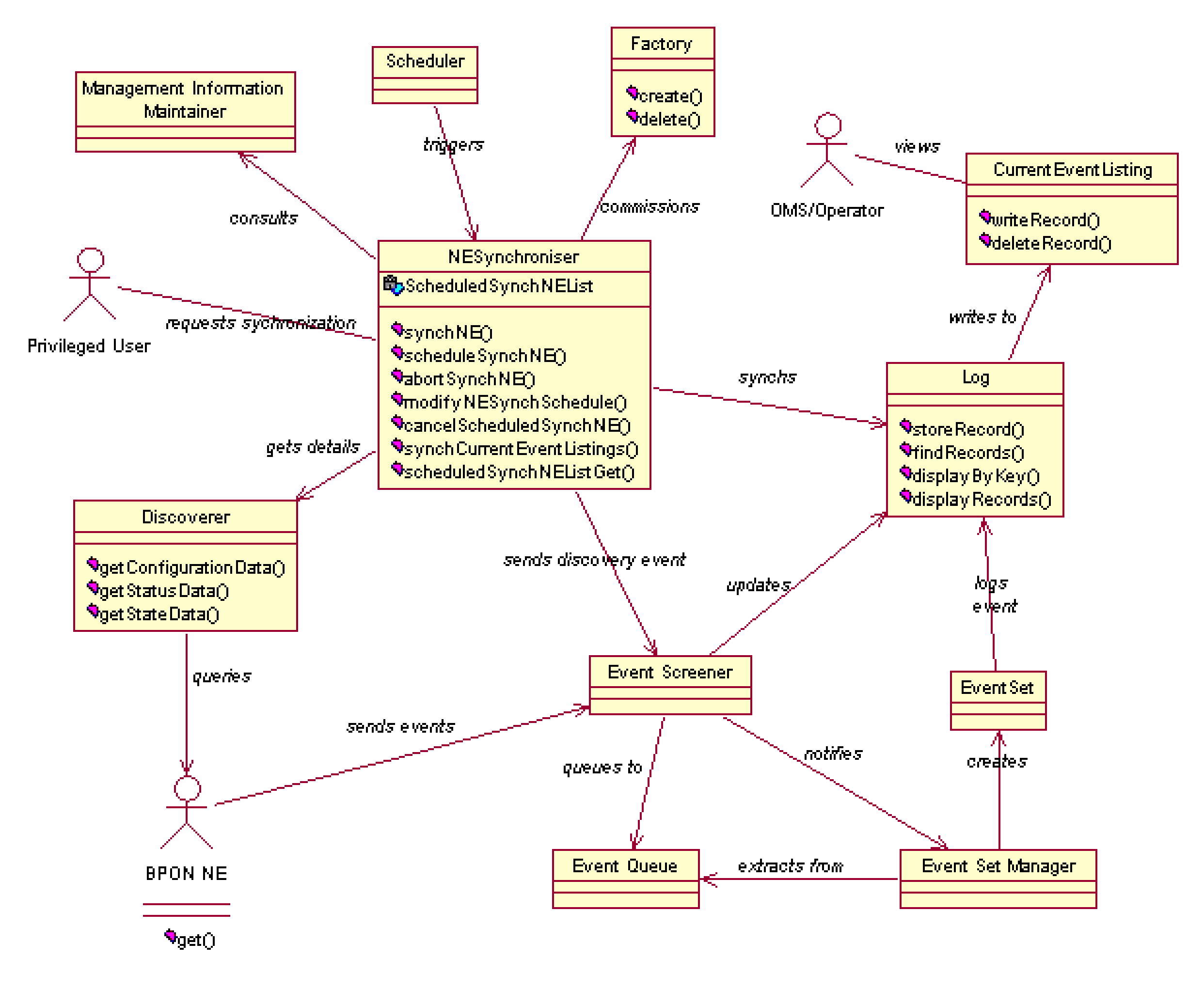


Figure 6-66 – NE synchronization class diagram

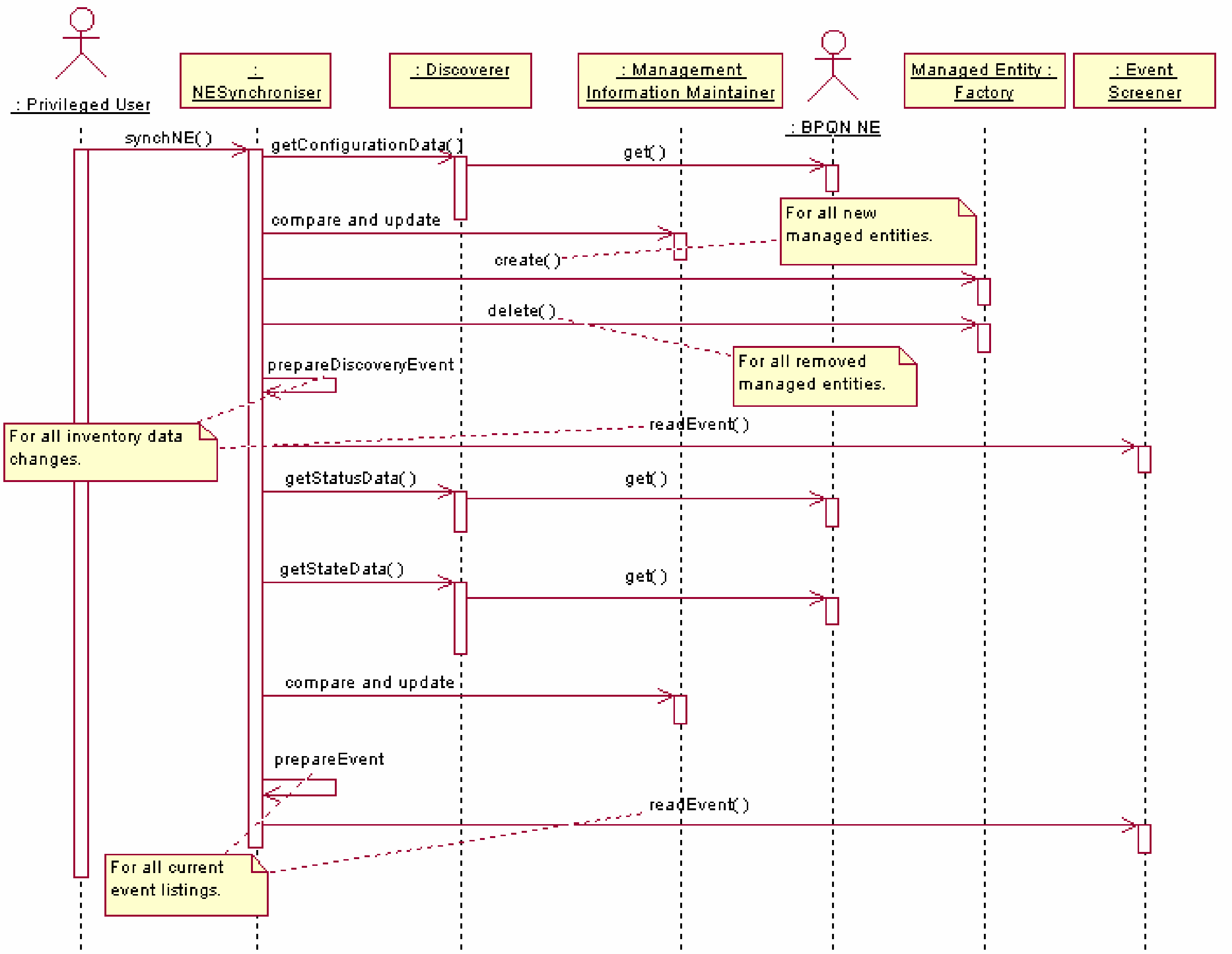


Figure 6-67 – NE synchronization requested by privileged user sequence diagram

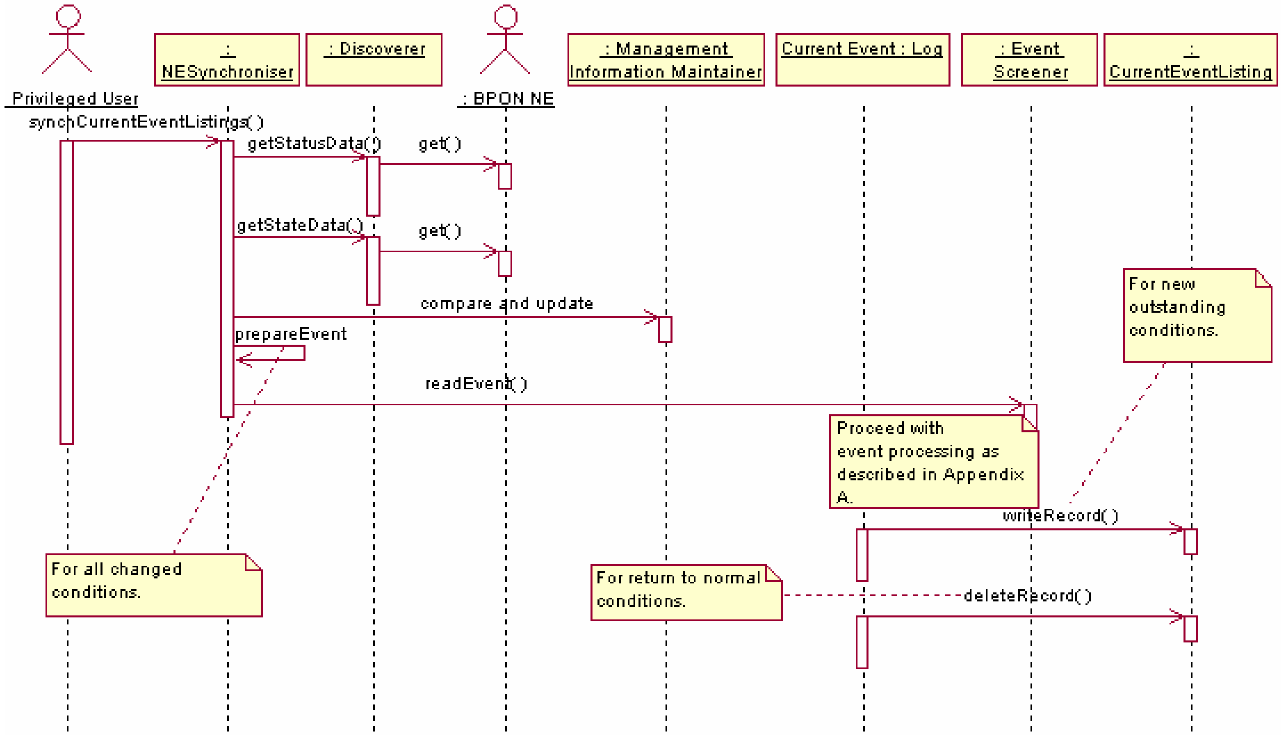


Figure 6-68 – Synchronize current event listing sequence diagram

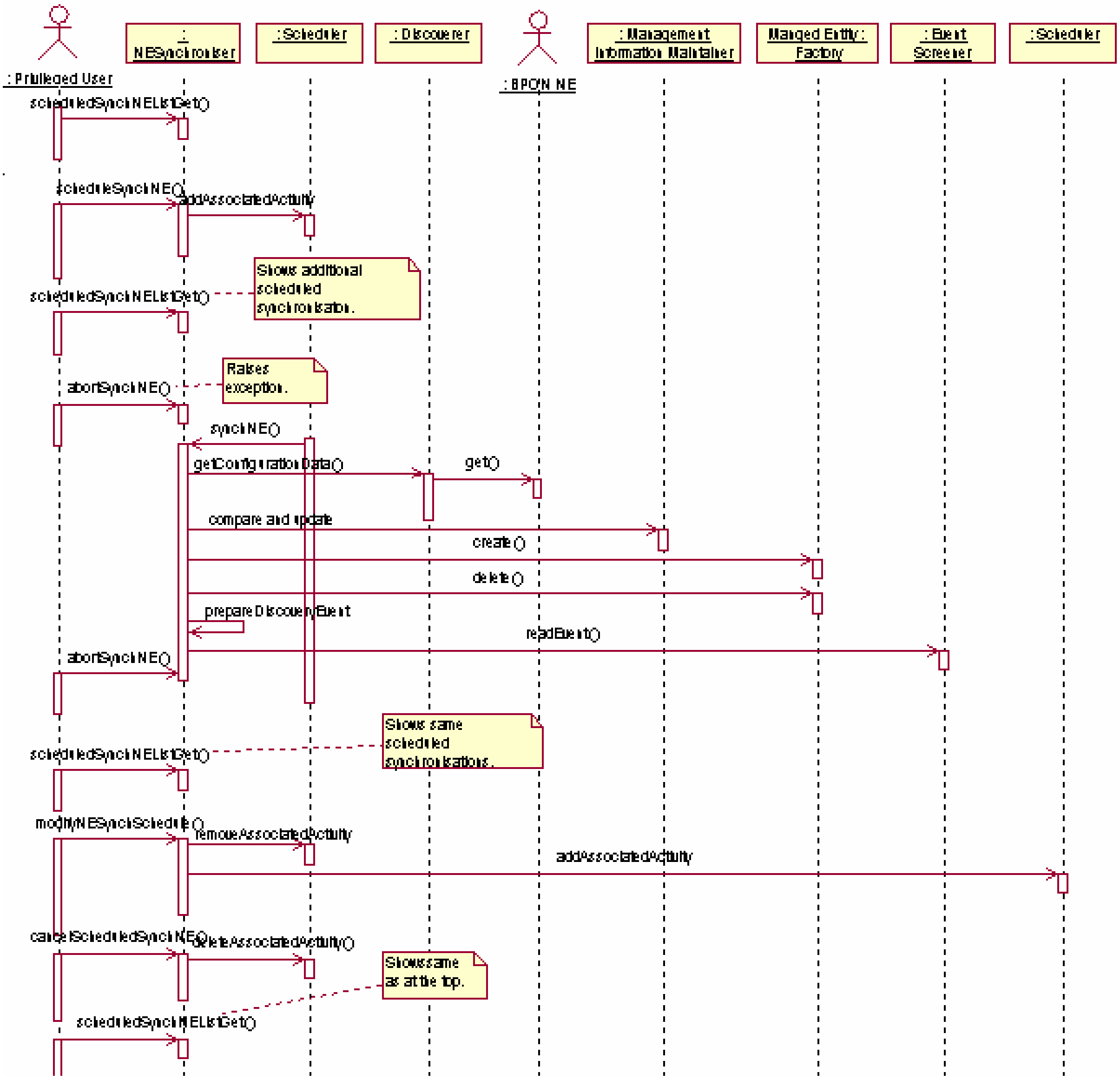


Figure 6-69 – Scheduled synchronization sequence diagram

Operations

Operation name	Operation purpose
1) synchNE[15]	This operation initiates a synchronization process between the supplier management system and a specific NE.
2) abortSynchNE	This operation aborts a synchronization process in progress between the supplier management system and a specific NE.
3) scheduleSynchNE	This operation schedules a synchronization process between the supplier management system and a specific NE.
4) modifyNESynchSchedule	This operation modifies the schedule for NE synchronization.
5) cancelScheduledSynchNE	This operation cancels all subsequent scheduled synchronization processes for this NE.
6) synchCurrentEventListings	The operation initiates synchronization between the supplier management system and specified NE for items in particular current event listings.
7) scheduledSynchNEListGet	This operation is used to retrieve the names of all NEs with synchronization schedules.

Figure 6-70 – NE synchronizer operations

[15] The "synch" operation is a best effort attempt. If the results are suspect as detected by the supplier management system, then the suspect flag is set to TRUE.

Operation signatures

Operation name	Input parameters	Return value	Exceptions
1) synchNE	ManagedEntityIdType (NE)	void	AccessDenied, CommFailure, UnknownNE, EquipmentFailure, BackupInProgress, SynchInProgress
2) abortSynchNE	ManagedEntityIdType (NE)	void	AccessDenied, CommFailure, UnknownNE, EquipmentFailure, NoSynchInProgress
3) scheduleSynchNE	ManagedEntityIdType (NE), UserLabelType (scheduler)	void	AccessDenied, UnknownNE, UnknownScheduler, InvalidScheduler
4) modifyNESynchSchedule	ManagedEntityIdType (NE), UserLabelType (new scheduler)	void	AccessDenied, UnknownNE, UnknownScheduler, InvalidScheduler, SynchNotScheduled
5) cancelScheduledSynchNE	ManagedEntityIdType (NE)	void	AccessDenied, UnknownNE
6) synchCurrentEventListings	ManagedEntityIdType, CurrentListingSeqType	void	AccessDenied, CommFailure, DCNTimeout, UnknownNE, EquipmentFailure, Timeout
7) scheduledSynchNEListGet		ScheduledSynchNE SeqType	AccessDenied

Figure 6-71 – NE synchronizer signatures

Exceptions

Exception raised	Description
AccessDenied	System is not granted access to this interface object.
BackupInProgress	This exception is raised when the request is issued while the backup is in progress.
CommFailure	There was a DCN link failure between the NE and the supplier management system.
DCNTimeout	The DCN communications link between at least one of the NEs and the supplier management system is so congested that current state or status information cannot be transferred within a system-defined synch time.
EquipmentFailure	The NE currently has a failure condition preventing the requested transaction from being completed.
InvalidScheduler	The scheduler parameter's values are outside defined scope.
NoSynchInProgress	The exception is raised if there is no synchronization process is in progress.
SynchInProgress	An operation is requested while the supplier management system is in the process of synchronizing with the NE, which prohibits the execution of the operation requested.
Timeout	The process duration reached a system-defined timeout before the process could complete.
UnknownNE	Identified NE is unknown to the supplier management system.
UnknownScheduler	The named scheduler is unknown to the supplier management system.
SynchNotScheduled	This exception is raised when the schedule modification references an NE for which no synchronization schedule has previously been established.

Figure 6-72 – NE synchronizer exceptions

6.3.5.2 Range ONT or ONU and register OLT

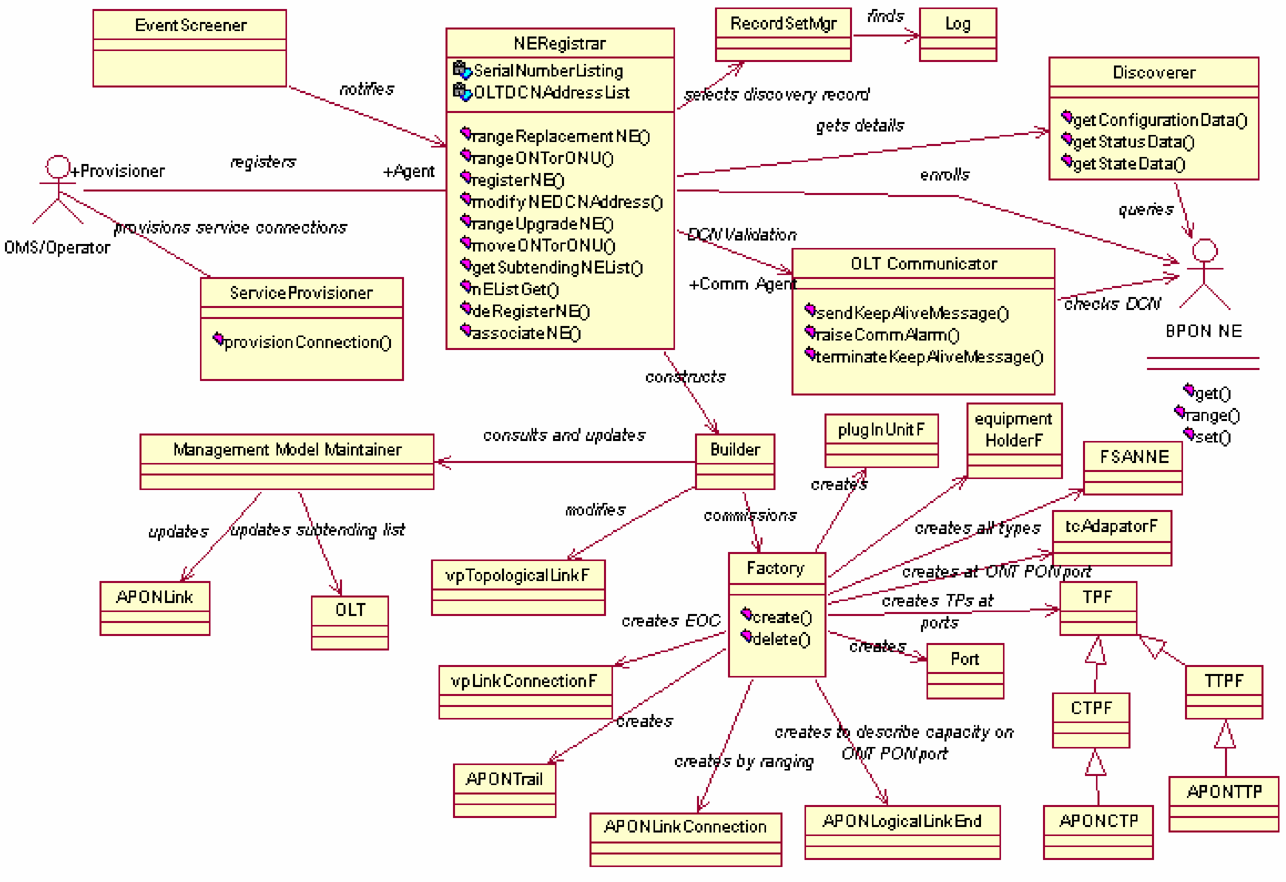


Figure 6-73 – Registration class diagram

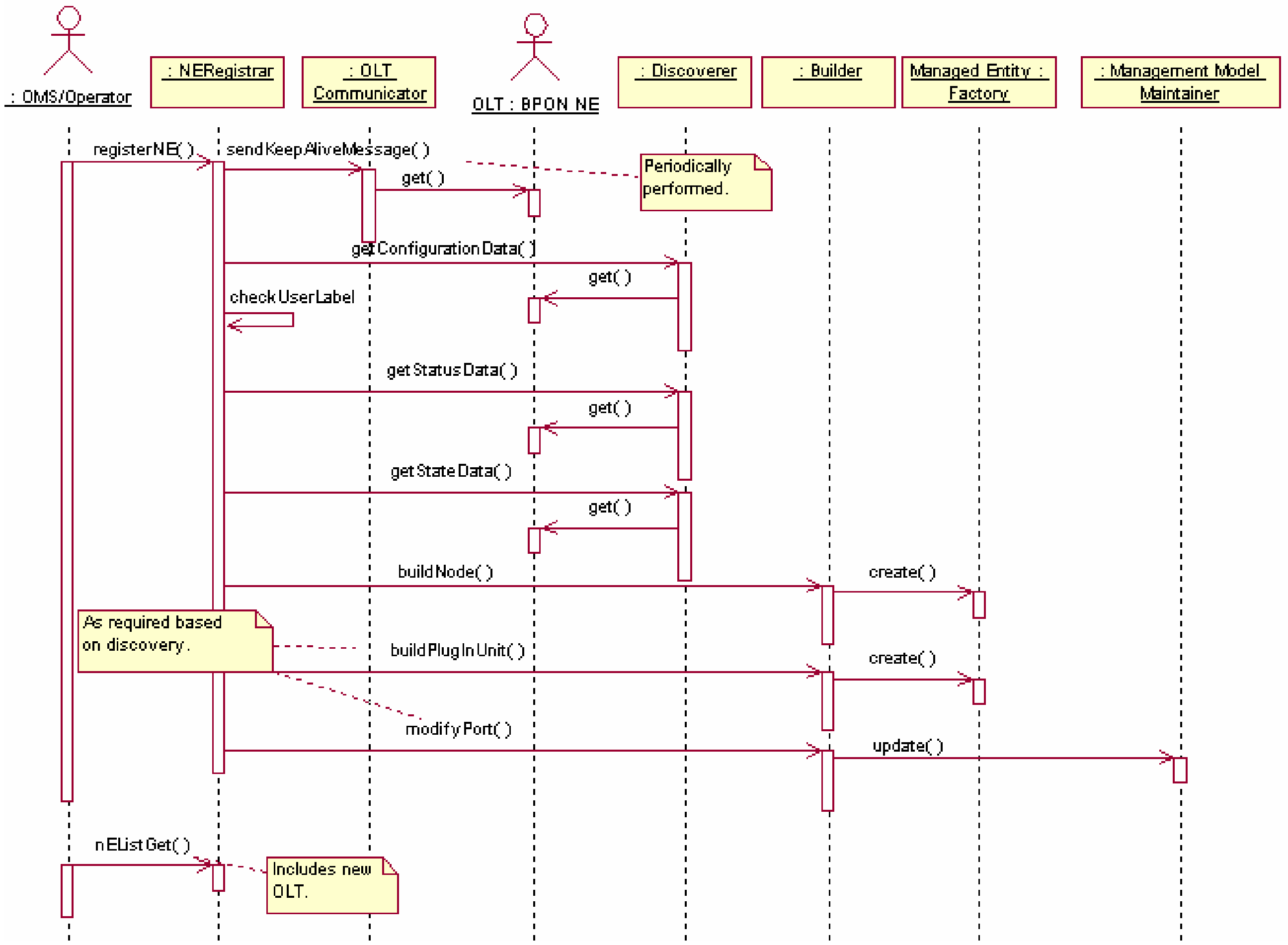


Figure 6-74 – Register NE sequence diagram[16]

[16] Applies only to OLT.

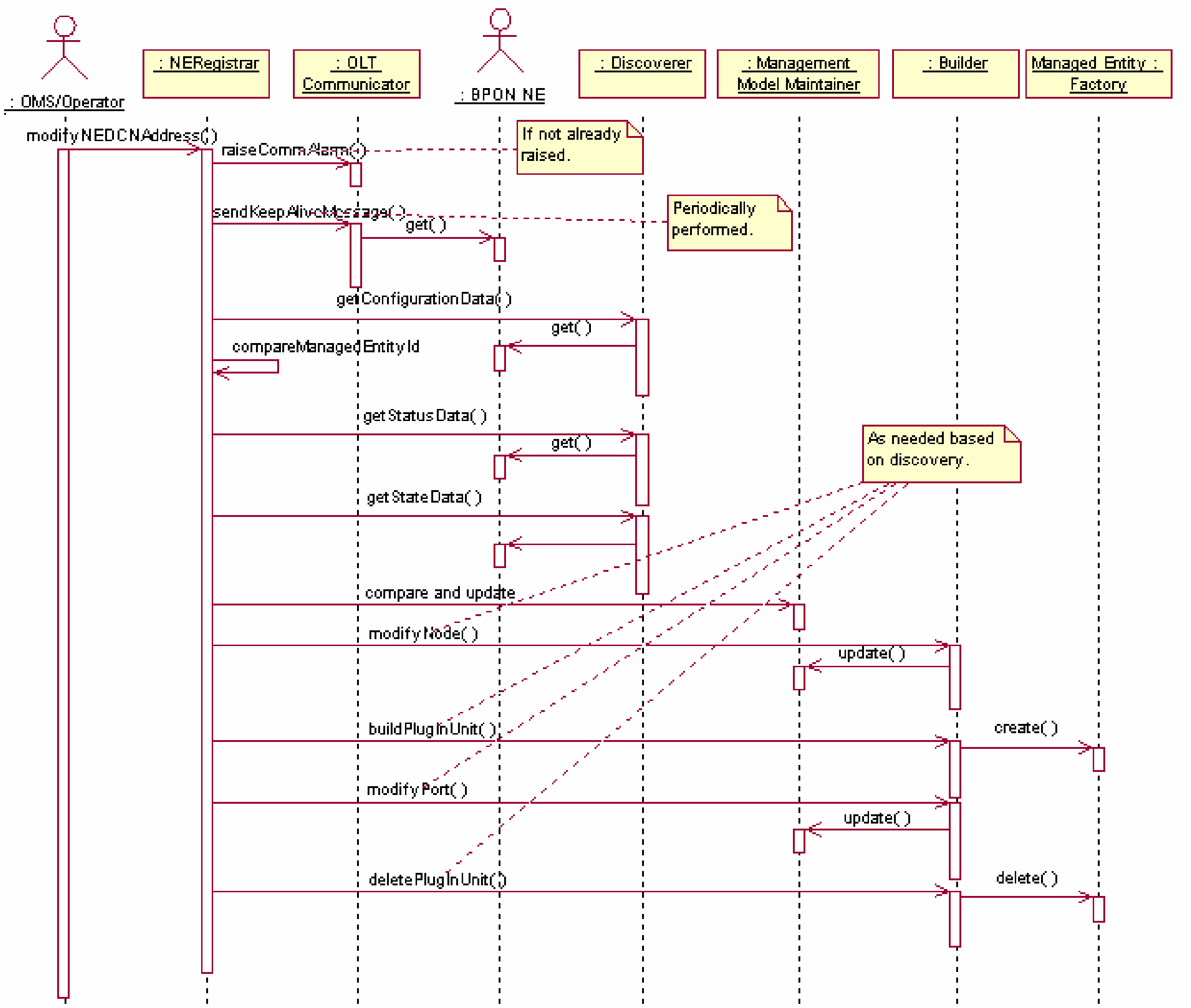


Figure 6-75 – Change DCN address sequence diagram

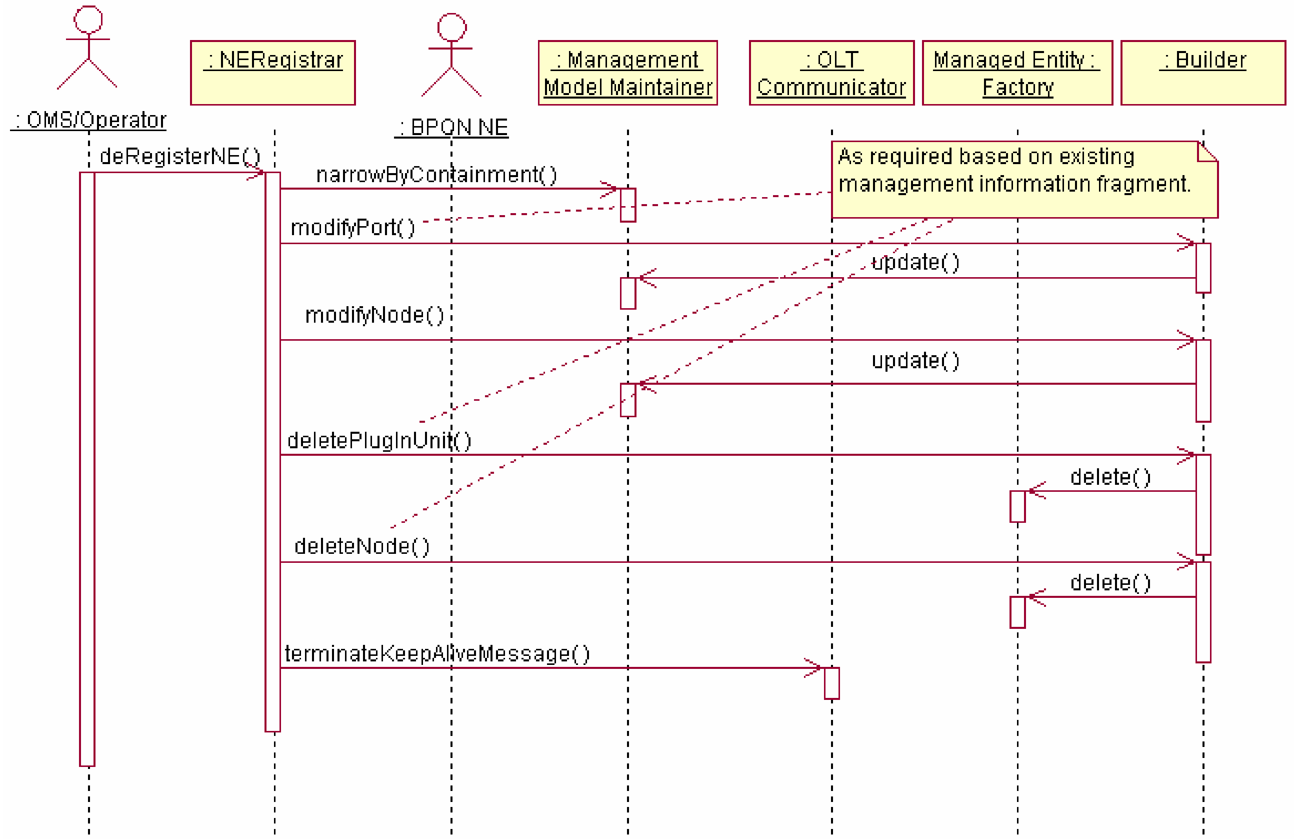


Figure 6-76 – Deregister NE sequence diagram

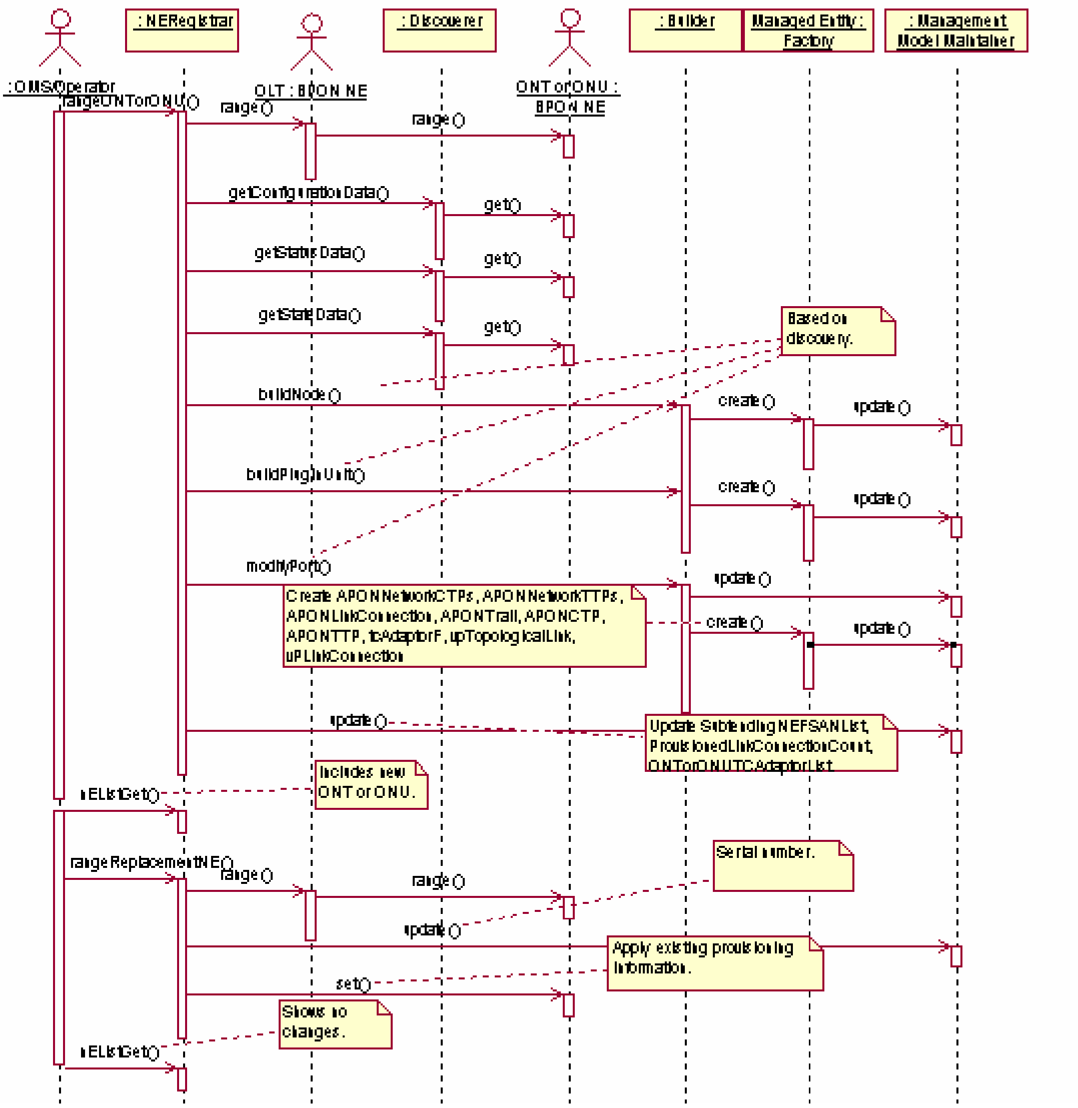


Figure 6-77 – Range ONT or ONU sequence diagram

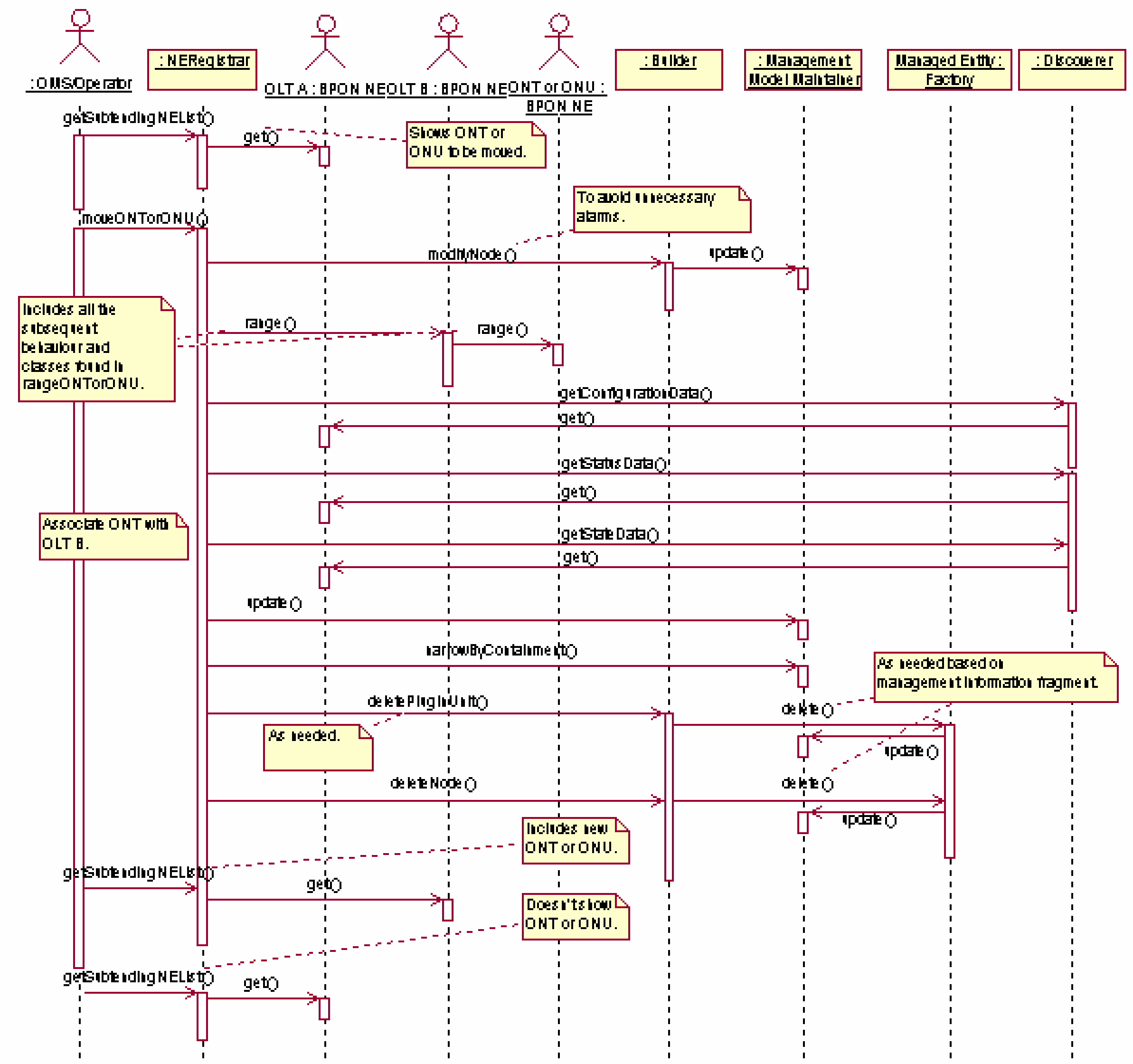


Figure 6-78 – Move ONT or ONU sequence diagram

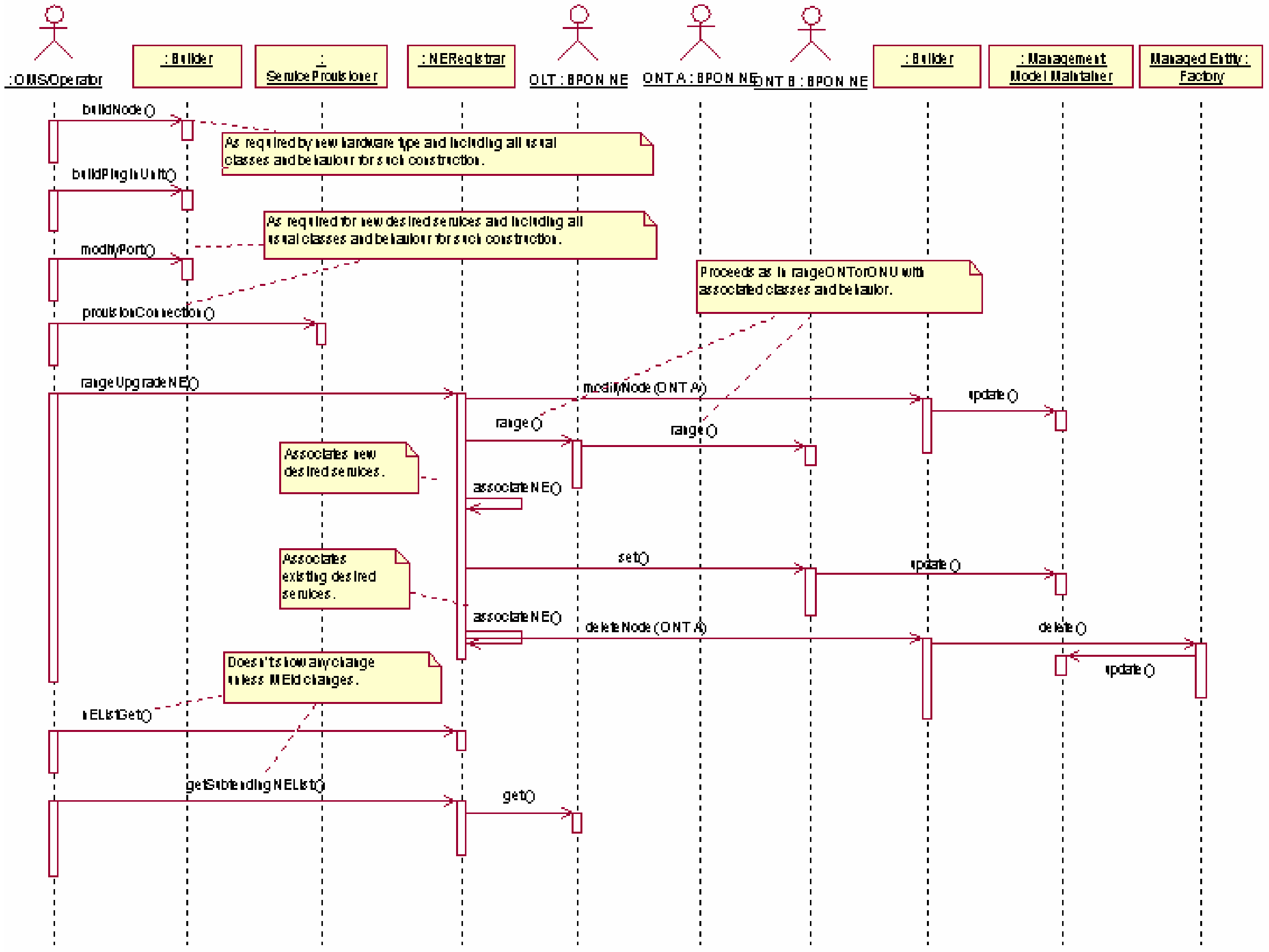

:OMS/Operator
: Builder
: Service Provisioner
: NERegistrar
OLT : BPON NE
ONT A : BPON NE
ONT B : BPON NE
: Builder
: Management Model Maintainer
Managed Entity : Factory
buildNode()
As required by new hardware type and including all usual classes and behaviour for such construction.
buildPlugInUnit()
As required for new desired services and including all usual classes and behaviour for such construction.
modifyPort()
Proceeds as in rangeONTorONU with associated classes and behavior.
provisionConnection()
rangeUpgradeNE()
modifyNode(ONT A)
update()
range()
range()
Associates new desired services.
associateNE()
Associates existing desired services.
set()
update()
associateNE()
deleteNode(ONT A)
delete()
update()
Doesn't show any change unless NEId changes.
nEListGet()
getSubtendingNEList()
get()

Figure 6-79 – Upgrade ONT or ONU sequence diagram

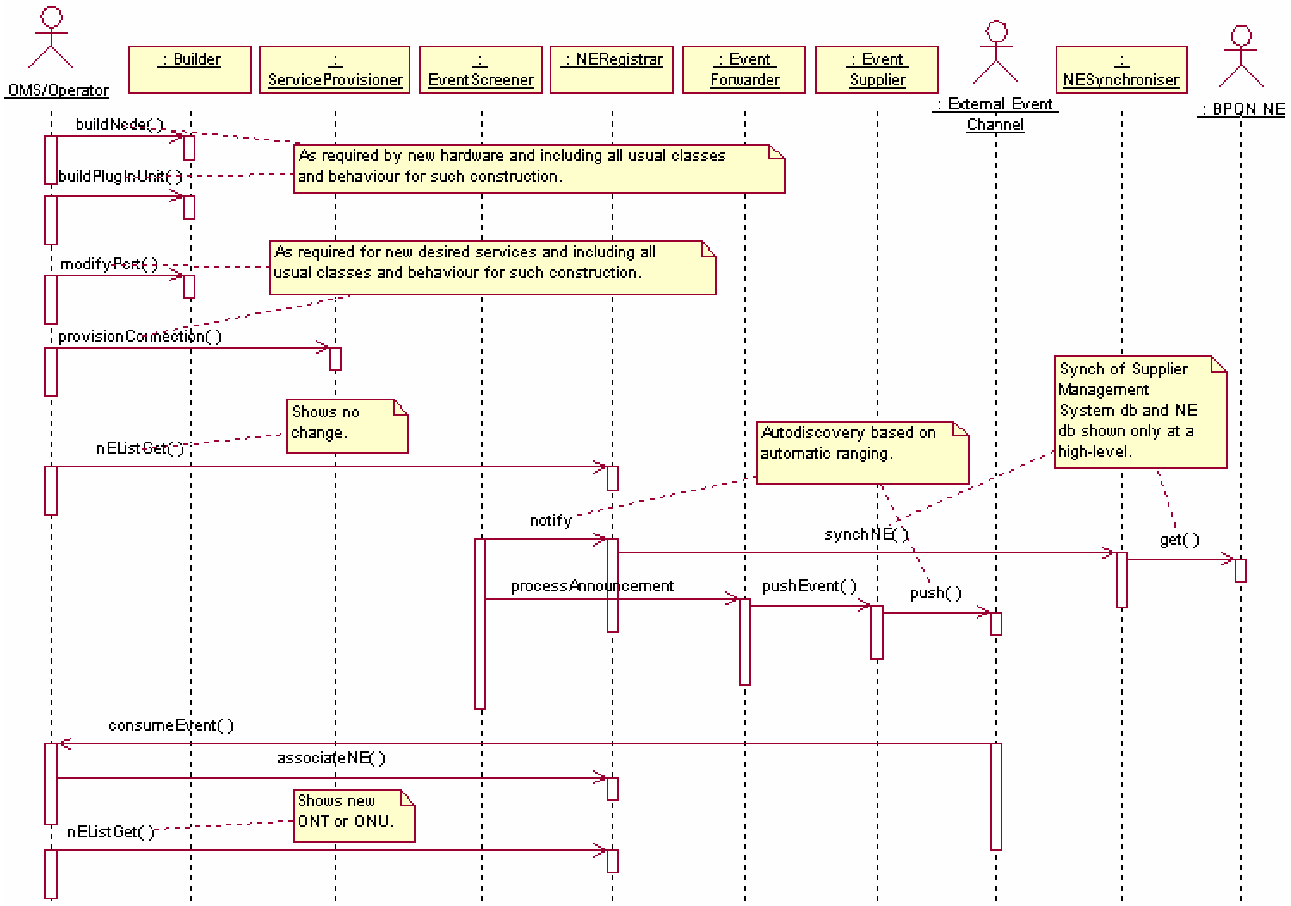


Figure 6-80 – Automatic ranging sequence diagram

Operations

Operations name	Operation purpose
1) registerNE	This operation registers an NE with a particular instance of supplier management system.
2) modifyNEDCNAddress	This operation changes the DCN address of a registered NE.
3) rangeONTorONU	This operation ranges an ONT or ONU using the serial number of the PON interface of the NE.
4) rangeReplacementNE	This operation ranges a replacement ONT or ONU using the serial number of the replacement equipment.
5) rangeUpgradeNE	This operation ranges a replacement NE for the purposes of upgrading the hardware.
6) moveONTorONU	This operation is used to move an ONT or ONU from one PON to another and also move all of the associated services.
7) getSubtendingNEList	This operation returns all subtending NEs of a particular NE.
8) nEListGet	This operation retrieves the network elements under the management jurisdiction of the supplier management system.
9) deRegisterNE	This operation removes the network element from the management jurisdiction of the supplier management system.
10) associateNE	This operation associates pre-provisioning information with a network element that has been installed and autodiscovered.

Figure 6-81 – NE registrar operations

Operation signatures[17]

Operations name	Input parameters	Return value	Exceptions
1) registerNE	DCNAddressType, UserLabelType, AdministrationDomainType	ManagedEntityIdType	AccessDenied, DCNTimeout, AddressLabelMismatch, DuplicateUserLabel, TooManyNEs, InvalidDCNAddress, DeniedAccess, InvalidUserLabelSyntax
2) modifyNEDCNAddress	ManagedEntityIdType, DCNAddressType	void	AccessDenied, DeniedAccess, AddressLabelMismatch, DCNTimeout, CommFailure, UnknownNE, InvalidDCNAddress, BackupInProgress
3) rangeONTorONU	ManagedEntityIdType (OLT), UserLabelType, SerialNumType, ManagedEntityIdType (port)	void	AccessDenied, CommFailure, EquipmentFailure, UnknownNE, UnknownPort, MaxSubtendingNodesExceeded, InsufficientPONBW, InvalidSerialNumSyntax, APONLayerFailure, DuplicateUserLabel, InvalidUserLabelSyntax, BackupInProgress, SynchInProgress
4) rangeReplacementNE	ManagedEntityIdType (old NE), UserLabelType, SerialNumType	ManagedEntityIdType	AccessDenied, CommFailure, UnknownNE, InvalidSerialNumSyntax, APONLayerFailure, EquipmentFailure, InvalidUserLabelSyntax, HWServicesMismatch, DuplicateUserLabel, BackupInProgress, SynchInProgress
5) rangeUpgradeNE	ManagedEntityIdType (old NE), ManagedEntityIdType (pre-provisioned NE), UserLabelType, SerialNumType	ManagedEntityIdType	AccessDenied, CommFailure, APONLayerFailure, EquipmentFailure, InvalidUserLabelSyntax, DuplicateUserLabel, UnknownNE, HWServicesMismatch, InsufficientPONBW, BackupInProgress, SynchInProgress

[17] The operation "rangeNewONU" has the same behaviour as "rangeNewONT" so there was no apparent need to show another sequence diagram.

Operations name	Input parameters	Return value	Exceptions
6) moveONTorONU	ManagedEntityIdType (old NE), ManagedEntityIdType (new port)	ManagedEntityIdType	AccessDenied, CommFailure, UnknownNE, UnknownPort, APONLayerFailure, EquipmentFailure, InsufficientPONBW, BackupInProgress, SynchInProgress
7) getSubtendingNEList	ManagedEntityIdType (subtended NE)	ManagedEntityIdSeqType	UnknownNE, AccessDenied
8) nEListGet		ManagedEntityIdSeqType	AccessDenied
9) deRegisterNE	ManagedEntityIdType	void	AccessDenied
10) associateNE	ManagedEntityIdType (pre-provisioned NE), ManagedEntityIdType (discovered NE)	ManagedEntityIdType	AccessDenied, UnknownManagedEntity

Figure 6-82 – NE registrar signatures

Exceptions

Exception raised	Description
AccessDenied	System is not granted access to this interface object.
AddressLabelMismatch	The identified NE does not have the current DCN address provided in the request.
APONLayerFailure	There was an APON protocol ranging failure between the OLT and the designed subtending node.
BackupInProgress	This exception is raised when the request is issued while the backup is in progress.
CommFailure	There was a DCN link failure between the NE and the supplier management system.
DCNTimeout	The DCN communications link between at least one of the NEs and the supplier management system is so congested that current state or status information cannot be transferred within a system-defined synch time.
DeniedAccess	System is not granted access to the NE.
DuplicateUserLabel	The user label provided in the request has been used to label another archive, i.e., one that is defined by a different set of creation request parameters.
EquipmentFailure	The NE currently has a failure condition preventing the requested transaction from being completed.
HWServicesMismatch	The replacement NE cannot perform the provisioned services.
InsufficientPONBW	The ONT or ONU cannot be ranged due to insufficient bandwidth on the APONLink.
InvalidDCNAddress	The specified DCN address is not valid.
InvalidSerialNumSyntax	Syntax of the serial number provided does not match definition rules.
InvalidUserLabelSyntax	The specified user label does not follow established rules for user label.
MaxSubtendingNodesExceeded	The maximum engineered number of subtending nodes for the identified PON interface has been exceeded with this request for service provisioning.
SynchInProgress	An operation is requested while the supplier management system is in the process of synchronizing with the NE that prohibits the execution of the operation requested.
TooManyNEs	The supplier management system cannot manage one more OLT.
UnknownManagedEntity	The specified managed entity is unknown to the supplier management system.
UnknownNE	Identified NE is unknown to the supplier management system.
UnknownPort	The identified port is unknown to the supplier management system.

Figure 6-83 – NE registrar exceptions

6.3.6 Provisioning

6.3.6.1 Build BPON resources

This clause shows the construction of management infrastructure to support the management of an OLT, an ONT or ONU, and of a port. In each case, a class diagram is followed by the associated sequence diagram.

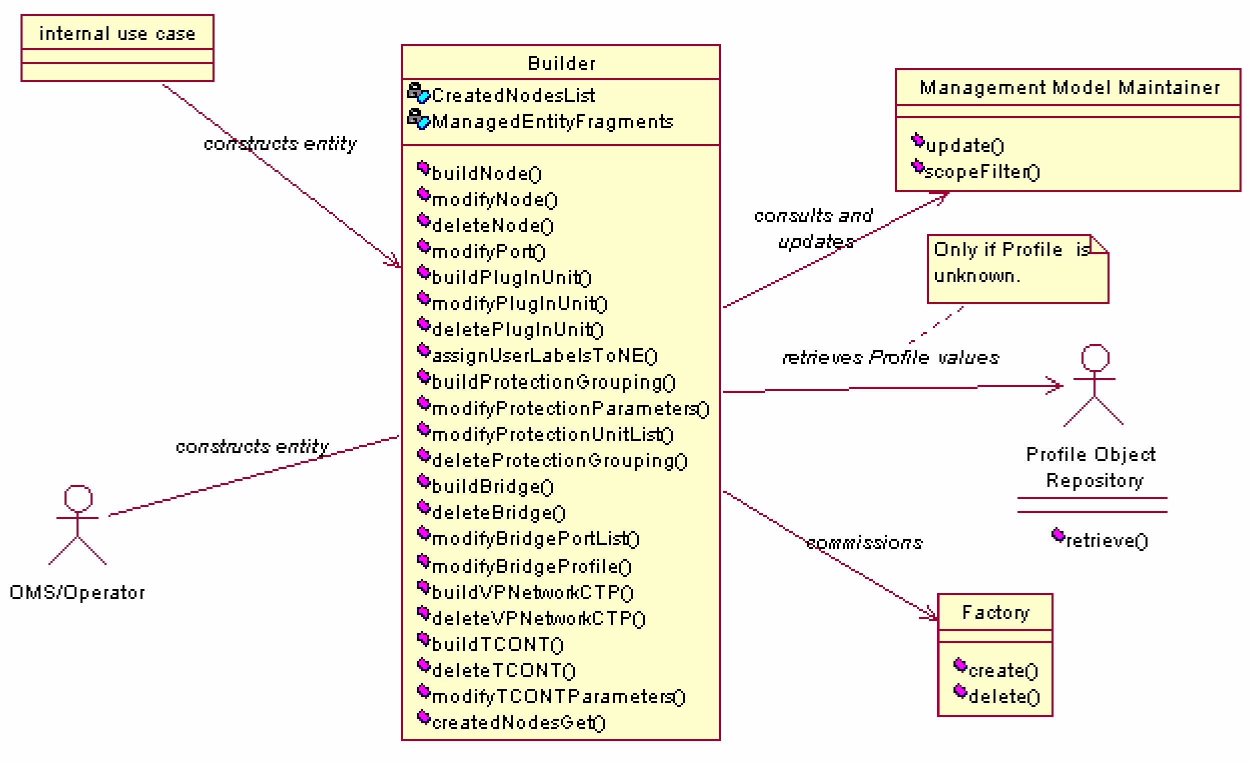


Figure 6-84 – Build class diagram

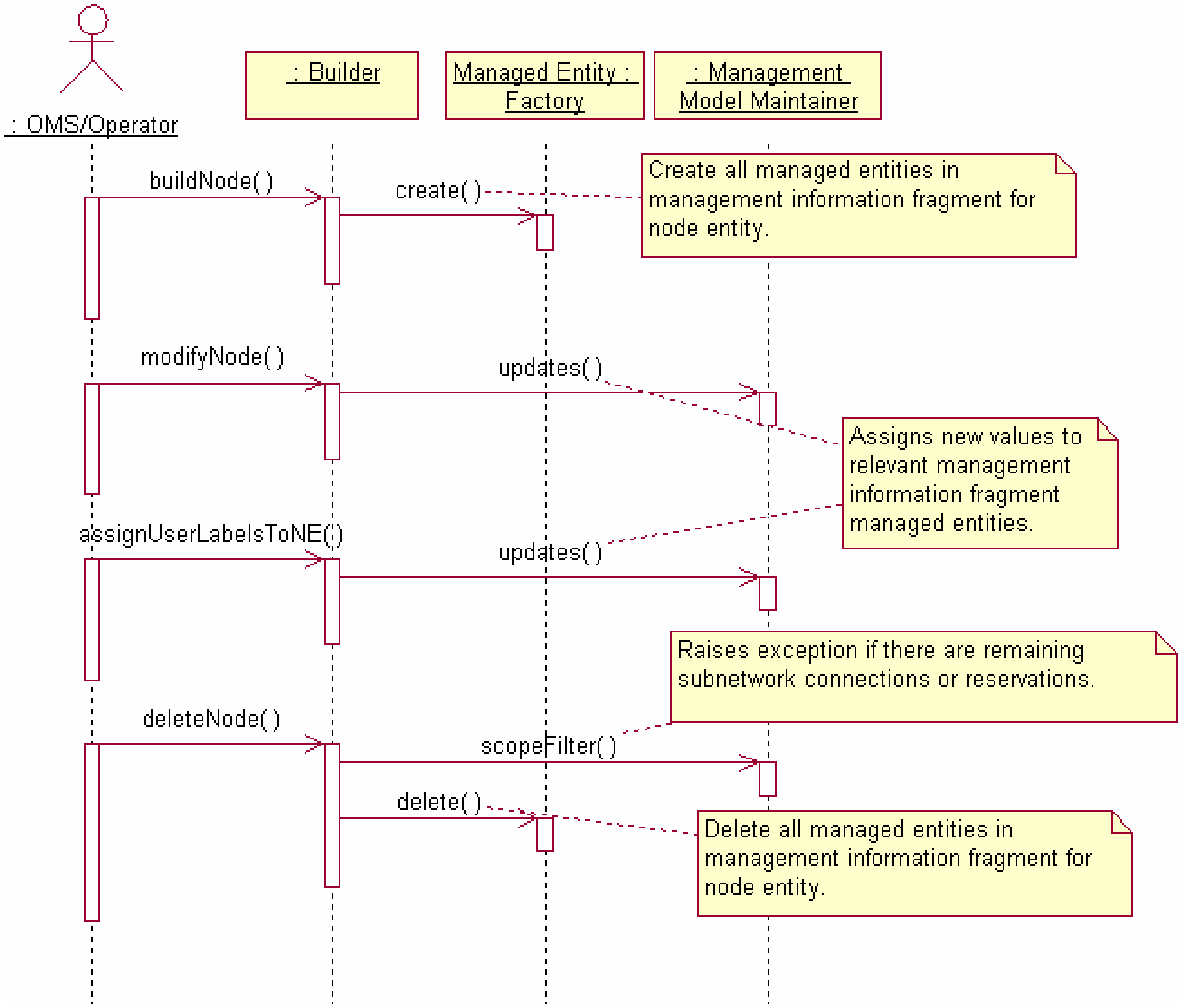

: OMS/Operator
: Builder
Managed Entity : Factory
: Management Model Maintainer
buildNode( )
create( )
Create all managed entities in management information fragment for node entity.
modifyNode( )
updates( )
Assigns new values to relevant management information fragment managed entities.
assignUserLabelsToNE( )
updates( )
Raises exception if there are remaining subnetwork connections or reservations.
deleteNode( )
scopeFilter( )
delete( )
Delete all managed entities in management information fragment for node entity.

Figure 6-85 – Build, modify and delete sequence diagram[18]

[18] This example concerns the "node" entity (for BPON technology this would be an OLT, ONT, ONU or NT), but the behaviour described applies to all the other entities in this interface including the following: Port, ProtectionGrouping, TCONT, PlugInUnit, MACBridge or VPNetworkCTP.

Operations

Operation name	Operation purpose
1) buildNode	This operation builds an NE in the supplier management system.
2) assignUserLabelsToNE	This operation assigns operator administrative designations to NEs.
3) modifyNode	The operation initiates reconfiguration and update of specific parameters associated with an NE.
4) deleteNode	This operation deletes the NE from the supplier management system and cancels a previous pre-provisioning request.
5) modifyPort	The operation modifies parameters of the designated port identified by physicalPathTPId.
6) buildPlugInUnit	This operation builds a plug-in unit in the supplier management system as part of the pre-provisioning activities.
7) modifyPlugInUnit	This operation modifies attributes of the plug-in unit in the supplier management system.
8) deletePlugInUnit	This operation deletes a plug-in unit from the supplier management system.
9) buildProtectionGrouping	This operation builds a protectionGrouping in the supplier management system.
10) modifyProtectionParameters	This operation modifies the protection schema for the identified protection grouping.
11) modifyProtectionUnitList	This operation either adds to or removes from the list of protected and protecting ports for the identified protection grouping.
12) deleteProtectionGrouping	This operation deletes a protection grouping of ports from the supplier management system.
13) buildBridge	This operation builds a MAC bridge in the supplier management system.
14) modifyBridgeProfile	This operation modifies the characteristics of the bridging function by changing the MAC bridge service profile associated with the bridge.
15) modifyBridgePortList	This operation either adds to or removes from the list of UNI ports belonging to the bridge grouping.
16) deleteBridge	This operation deletes a bridge provisioning from the supplier management system.
17) buildVPNetworkCTP	This operation builds a VP network CTP in the supplier management system.
18) deleteVPNetworkCTP	This operation deletes a VP network CTP provisioning from the supplier management system.
19) createdNodesGet	This operation retrieves the list of network elements that have been constructed through invocation of this interface.
20) buildTCONT	This operation builds a TCONT in the supplier management system.
21) modifyTCONTParameters	This operation modifies the parameters associated with an existing TCONT in the supplier management system.
22) deleteTCONT	This operation deletes a TCONT provisioning from the supplier management system.

Figure 6-86 – Builder operations

Operation signatures

Operation name	Input parameters	Return value	Exceptions
1) buildNode	NEKindType, string (supplier name), string (location), VersionType (hardware version), SerialNumType, string (registration Id) NameSeqType (alarm severity profile), NameSeqType (threshold data profile), SlotAssignmentSeqType, ManagedEntityIdType (port), string (equipment code) UserLabelType, ExternalTimeType, SystemTimingType, RegistrationIdType, boolean (status reporting indicator) AdministrationDomainType	ManagedEntity IdType	UnrecognisedVersion, InvalidSerialNumSyntax, DuplicateSerialNumber, UnknownProfiles, UnknownManagedEntity, DuplicateUserLabel, AccessDenied, InvalidExternalTime, UnknownSystemTimingSource, ProfileSuspended
2) assignUserLabelsToNE	SerialNumType, string (registration Id), UserLabelType, RegistrationIdType AdministrationDomainType	void	InvalidSerialNumSyntax, DuplicateSerialNumber, DuplicateUserLabel, AccessDenied
3) modifyNode	ManagedEntityIdType, SlotAssignmentSeqType, NameSeqType (alarm severity profile), NameSeqType (threshold data profile), string (registration Id), UserLabelType, ExternalTimeType, RegistrationIdType, boolean (status reporting indicator) AdministrationDomainType	void	UnknownManagedEntity, UnknownNE, InvalidSlotAssignmentList, UnknownProfiles, DuplicateUserLabel, AccessDenied, InvalidExternalTime, ProfileSuspended
4) deleteNode	ManagedEntityIdType	void	UnknownNE, RemainingContainedManaged Entities, AccessDenied, RemainingReservations, RemainingSubnetworkConnections
5) modifyPort	ManagedEntityIdType, NameSeqType (alarm severity profile), NameSeqType (threshold data profile), NameSeqType (port profiles), string, AdministrativeStateType, OpticalWaveLengthArraySeqType, LoopbackLocationIdSeqType, unsigned long (interface speed), unsigned long (ARC timer)	void	UnknownManagedEntity, UnknownProfiles, AccessDenied, InterfaceSpeedNotChangeable, ProfileSuspended
6) buildPlugInUnit	ManagedEntityIdType, NameSeqType (alarm severity profile), UserLabelType, string (equipment code), AdministrativeStateType, ManagedEntityIdType (slot)	ManagedEntity IdType	UnknownNE, DuplicateUserLabel, AccessDenied, UnknownManagedEntity, InvalidEquipmentCode, SlotAlreadyAssigned, UnknownSlot, InvalidSlotAssignmentList, UnknownProfiles, ProfileSuspended

Operation name	Input parameters	Return value	Exceptions
7) modifyPlugInUnit	ManagedEntityIdType, NameType (alarm severity profile), string (equipment code), ManagedEntityIdType, UserLabelType, AdministrativeStateType	ManagedEntity IdType	UnknownManagedEntity, UnknownProfiles, AccessDenied, InvalidEquipmentCode, SlotAlreadyAssigned, UnknownSlot, InvalidSlotAssignmentList, InvalidUserLabelSyntax, ProfileSuspended
8) deletePlugInUnit	ManagedEntityIdType	void	UnknownManagedEntity, RemainingSubnetworkConnections, AccessDenied, RemainingReservations
9) buildProtection Grouping	ProtectionParameterType, ProtectionUnitSeqType	ManagedEntity IdType	InvalidProtectionScheme, AccessDenied
10) modifyProtection Parameters	ManagedEntityIdType, ProtectionParameterType	void	UnknownManagedEntity, InvalidProtectionScheme, AccessDenied
11) modifyProtection UnitList	ManagedEntityIdType, ProtectionUnitSeqType, boolean (add delete indication)	void	UnknownManagedEntity, InvalidProtectionScheme, AccessDenied
12) deleteProtection Grouping	ManagedEntityIdType	void	UnknownManagedEntity, AccessDenied
13) buildBridge	NameType (MAC bridge profile), ManagedEntityIdType (port), ManagedEntityIdSeqType (UNI ports)	ManagedEntity IdType	UnknownProfiles, AccessDenied, UnknownManagedEntity, ProfileSuspended
14) modifyBridgeProfile	ManagedEntityIdType, NameType (MAC bridge profile)	void	UnknownManagedEntity, UnknownProfiles, AccessDenied, ProfileSuspended
15) modifyBridgePortList	ManagedEntityIdType, ManagedEntityIdSeqType (delta UNI ports), boolean (add delete indication)	void	UnknownManagedEntity, RemainingSubnetworkConnections, AccessDenied
16) deleteBridge	ManagedEntityIdType	void	UnknownManagedEntity, AccessDenied, RemainingSubnetworkConnections
17) buildVPNetworkCTP	ManagedEntityIdType (port), short (VPI), NameType(traffic descriptor profile) ATMOverbookingFactorType, UserLabelType, SegmentEndpointIndType	ManagedEntity IdType	UnknownProfiles, AccessDenied, UnknownManagedEntity, ParameterViolation, ProfileSuspended
18) deleteVPNetwork CTP	ManagedEntityIdType	void	UnknownManagedEntity, AccessDenied
19) createdNodesGet		ManagedEntity IdSeqType	AccessDenied
20) buildTCONT	ManagedEntityIdType (ONT or ONU), TCONTType, BWType (maxBW), BWType (fixedBW), BWType (guaranteedBW), UserLabelType	ManagedEntity IdType	UnknownNE, AccessDenied, InsufficientPONBW, UnsupportedTCONTType, DuplicateUserLabel
21) modifyTCONT Parameters	ManagedEntityIdType (TCONT), BWType (maxBW), BWType (fixedBW), BWType (guaranteedBW), UserLabelType	void	UnknownManagedEntity, AccessDenied, InsufficientPONBW, DuplicateUserLabel
22) deleteTCONT	ManagedEntityIdType (TCONT)	void	UnknownManagedEntity, AccessDenied, RemainingSubnetworkConnections

Figure 6-87 – Builder signatures

Exceptions

Exception raised	Description
AccessDenied	System is not granted access to this interface object.
DuplicateSerialNumber	There exists other equipment of the same type with this serial number.
DuplicateUserLabel	The user label provided in the request has been used to label another archive, i.e., one that is defined by a different set of creation request parameters.
InterfaceSpeedNotChangeable	The physical port cannot support the new interface speed or the speed is not configurable.
InvalidEquipmentCode	The equipment code does not conform to syntax.
InvalidExternalTime	External time specified is not valid.
InvalidProtectionScheme	The network resource does not support the protection parameters specified in context with the port listing or if the protection units are ports of dissimilar physical path characteristic.
InvalidSerialNumSyntax	Syntax of the serial number provided does not match definition rules.
InvalidSlotAssignmentList	Expected slot provisioning rules are violated by slot assignment provided.
InvalidUserLabelSyntax	The specified UserLabel does not follow established rules for UserLabel.
ParameterViolation	This exception is raised when the endpoint parameters do not match the protocol characteristics of the port, or when the values are out of range or invalid duplicates.
ProfileSuspended	The named profile(s) in the invocation have been suspended for use within the supplier management system by the OMS or operator.
RemainingContainedManagedEntities	Contained circuit packs or equipment holders have not been deleted yet.
RemainingReservations	The node cannot be deleted as resource reservations still exist.
RemainingSubnetworkConnections	The node or plug-in unit cannot be deleted as there are remaining subnetwork connections.
SlotAlreadyAssigned	The requested slot is already provisioned.
UnknownManagedEntity	The specified managed entity is unknown to the supplier management system.
UnknownNE	Identified NE is unknown to the supplier management system.
UnknownProfiles	This exception is raised if the profile name provided is unknown to the supplier management system and cannot be retrieved from the profile object repository.
UnknownSlot	The requested slot is unknown in the NE.
UnknownSystemTimingSource	External time source unknown to the supplier management system.
UnrecognisedVersion	Equipment version provided does not match known values.

Figure 6-88 – Builder exceptions

6.3.6.2 Profile object management

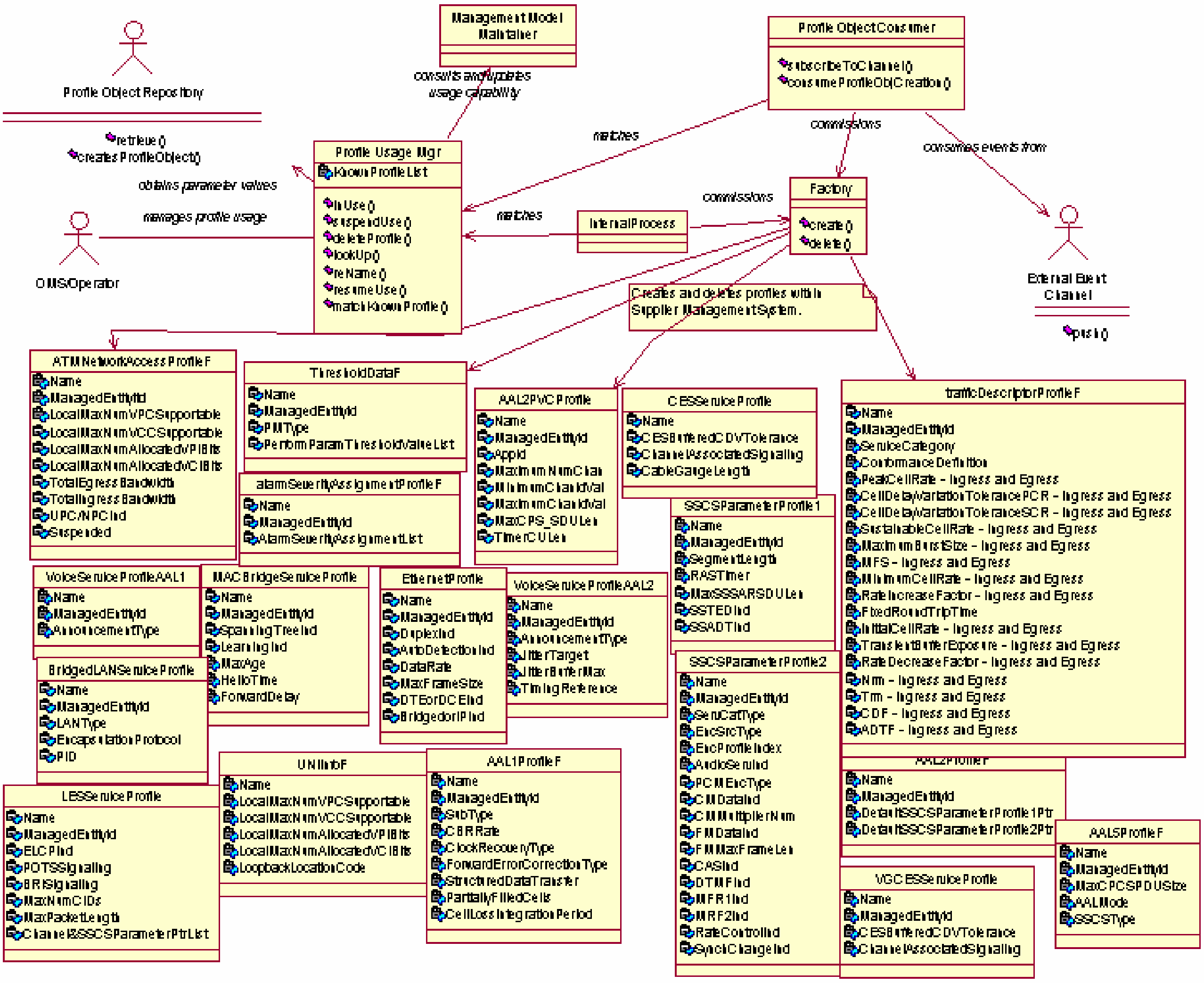


Figure 6-89 – Profile object management class diagram

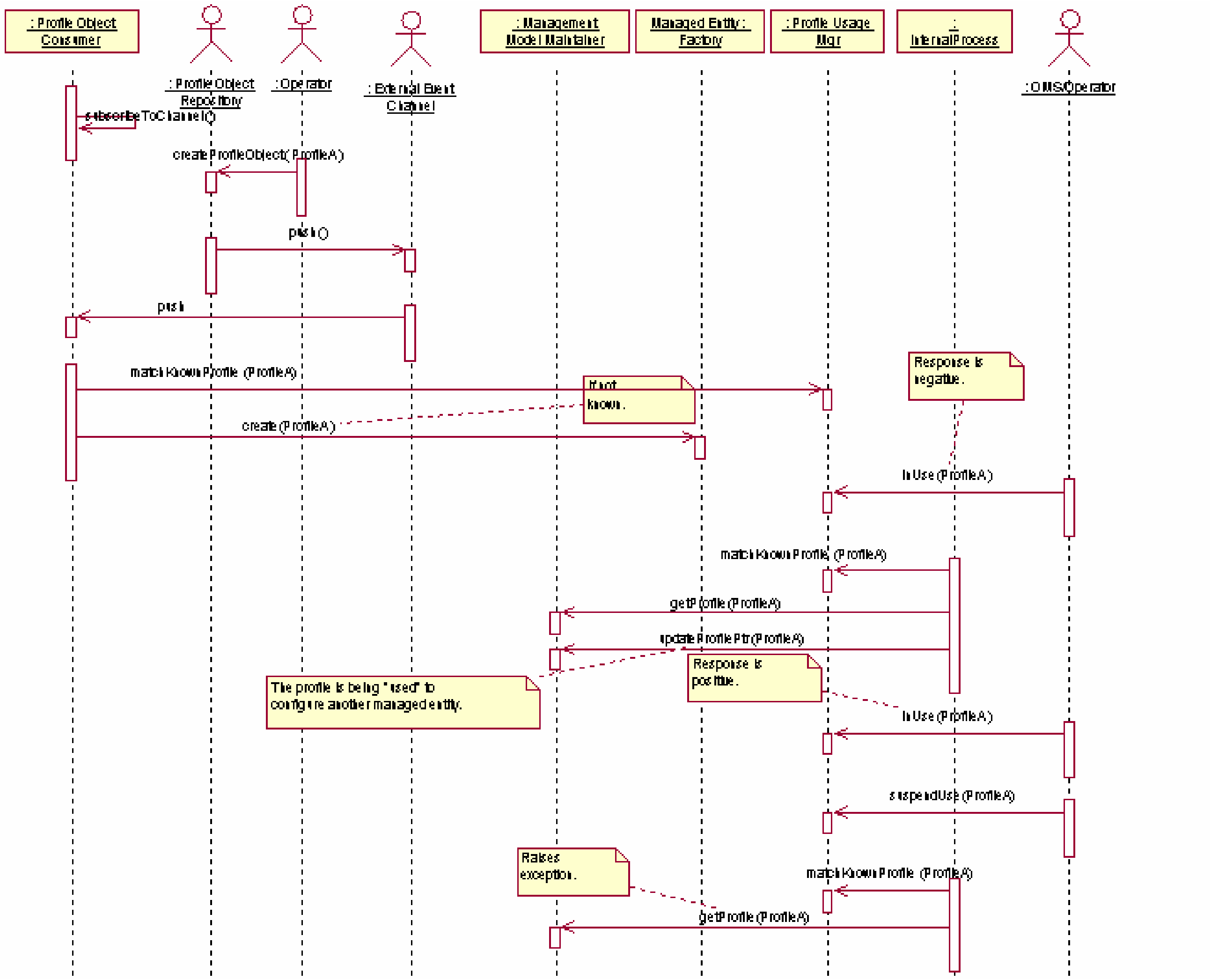


Figure 6-90 – Profile object management sequence diagram

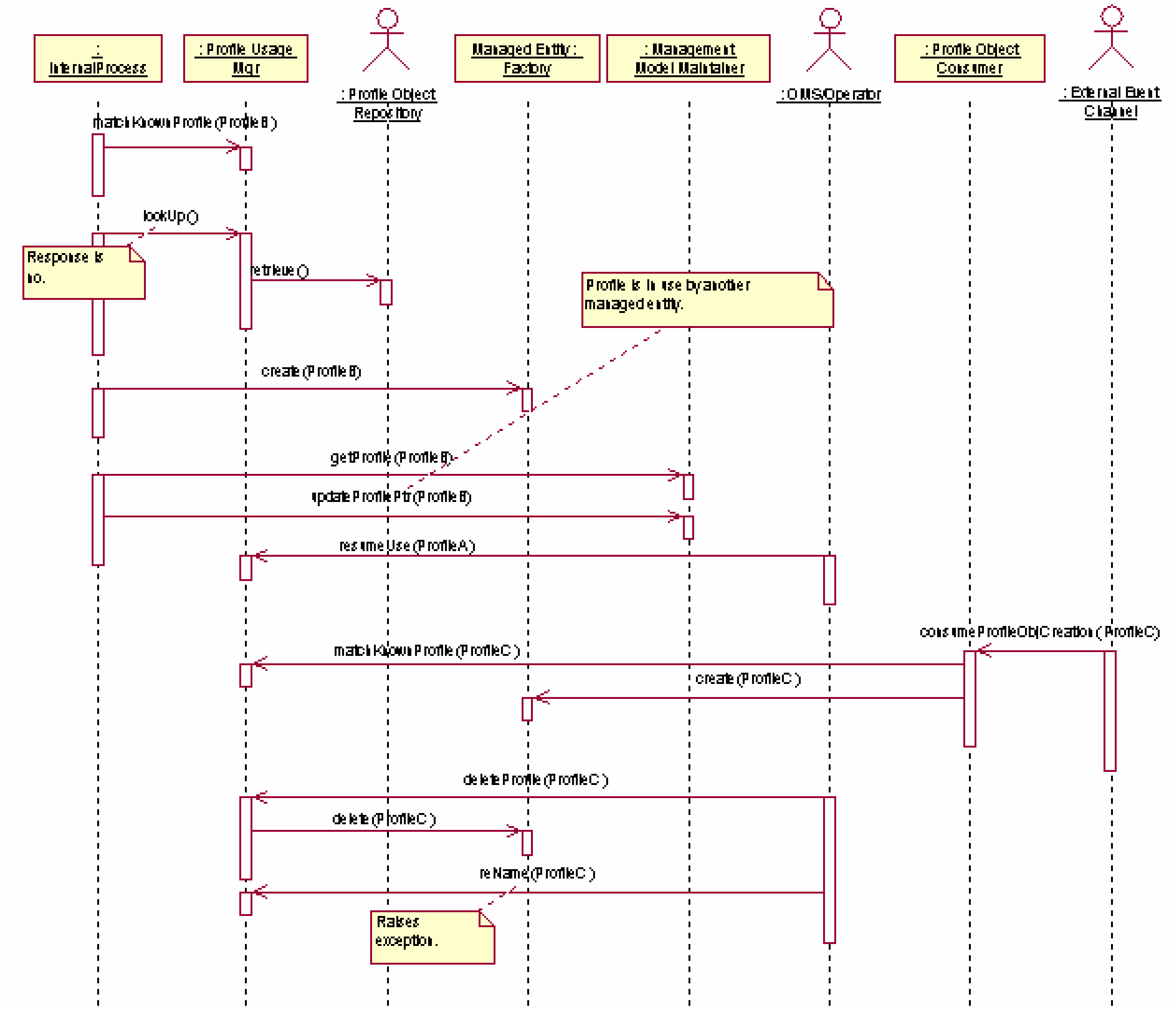


Figure 6-91 – Profile object management – New supplier management system sequence diagram

Operations

Operation name	Operation purpose
1) reName	This operation provides the capability to rename a profile.
2) inUse	This operation returns a boolean value to tell if the profile is in use.
3) suspendUse	This operation suspends the use of a profile.
4) resumeUse	This operation resumes the use of a named profile.
5) deleteProfile	This operation deleteProfile provides the capability to remove a profile which is not in use.
6) retrieve[19]	This operation provides the capability to retrieve a profile attribute values.

Figure 6-92 – Profile usage manager and profile retriever operations

[19] The operation "retrieve()" is the only one associated with the interface object profile retriever.

Operation signatures

Operation name	Input parameters	Return value	Exceptions
1) reName	NameType (old profile name), NameType (new profile name)	void	UnknownProfiles, AccessDenied, DuplicateProfileName
2) inUse	NameType (profile name)	boolean (indication of in use)	UnknownProfiles, AccessDenied
3) suspendUse	NameType (profile name)	void	UnknownProfiles, AccessDenied
4) resumeUse	NameType (profile name)	void	UnknownProfiles, AccessDenied
5) deleteProfile	NameType (profile name)	void	UnknownProfiles, AccessDenied, ProfileInUse
6) retrieve[20]	NameType (profile name)	ProfileInfoType	UnknownProfiles

Figure 6-93 – Profile usage manager and profile retriever signatures

Exceptions

Exception raised	Description
AccessDenied	System is not granted access to this interface object.
DuplicateProfileName	This exception is raised when the new profile name duplicates an existing profile name.
ProfileInUse	This exception is raised when the profile may not be deleted because it is still being used to characterize managed entities within the management jurisdiction of the supplier management system.
UnknownProfiles	This exception is raised if the profile name provided is unknown to the supplier management system and cannot be retrieved from the profile object repository.

Figure 6-94 – Profile usage manager and profile retriever exceptions

[20] The operation "retrieve()" is the only one associated with the interface object profile retriever. It is instantiated by the profile object repository.

6.3.6.3 Provision installed BPON resources

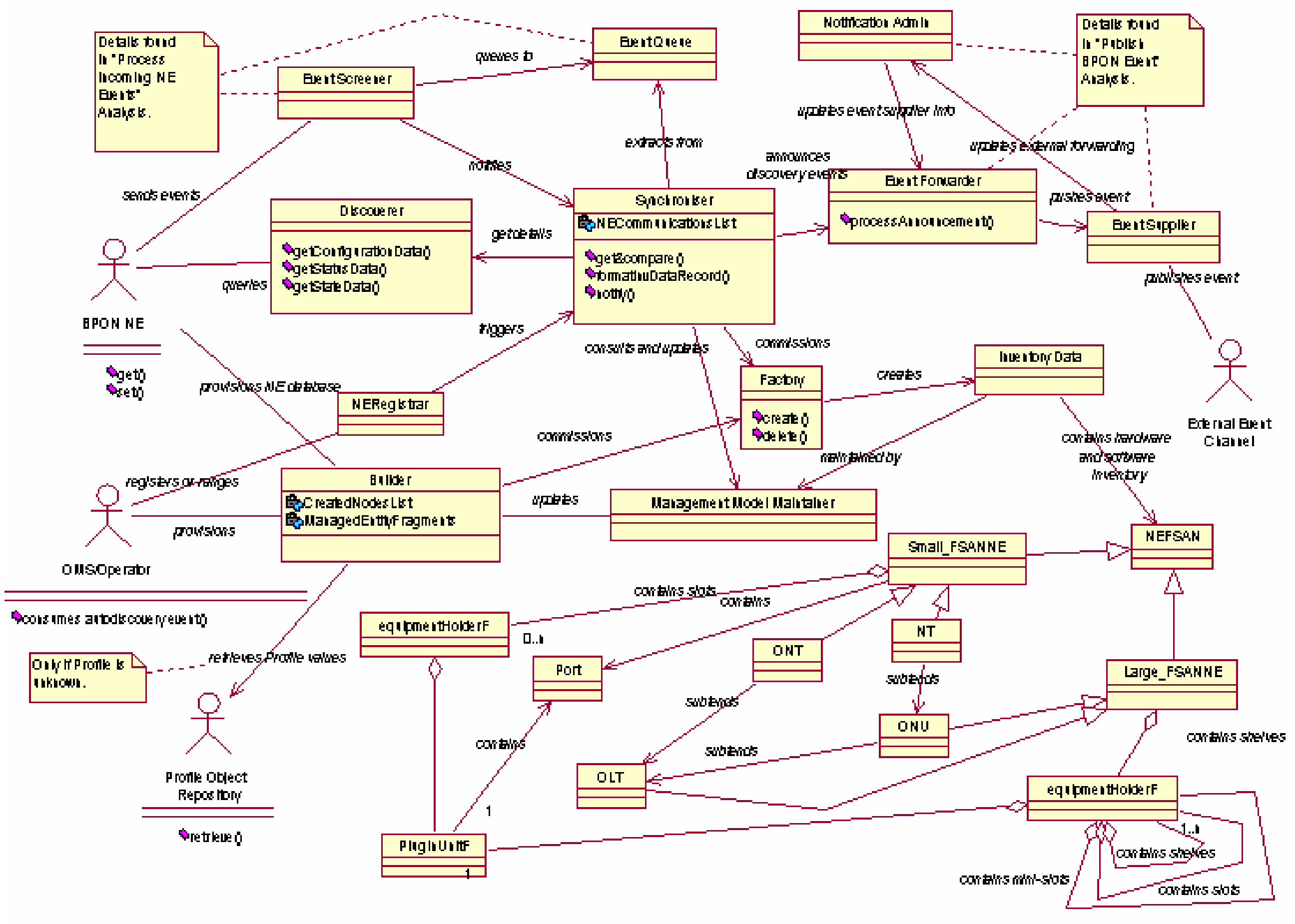


Figure 6-95 – Provision installed BPON resources class diagram

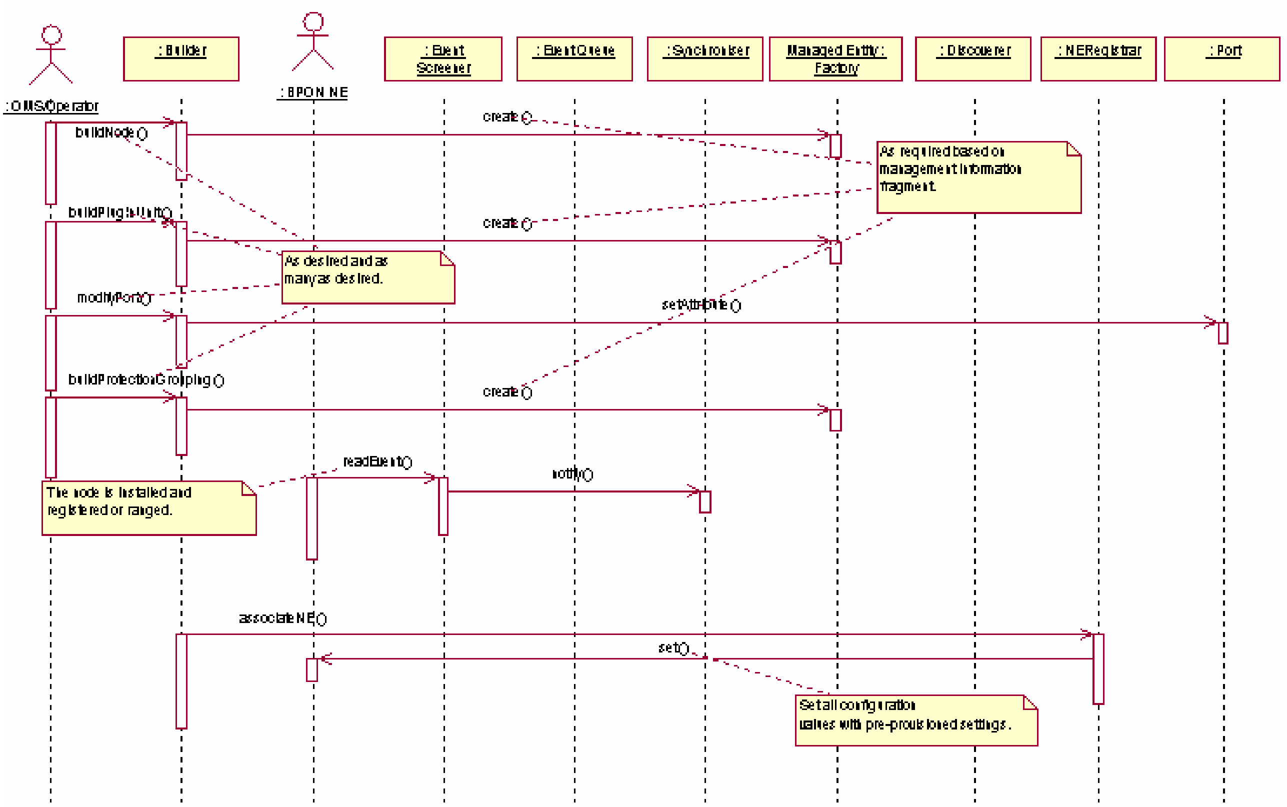
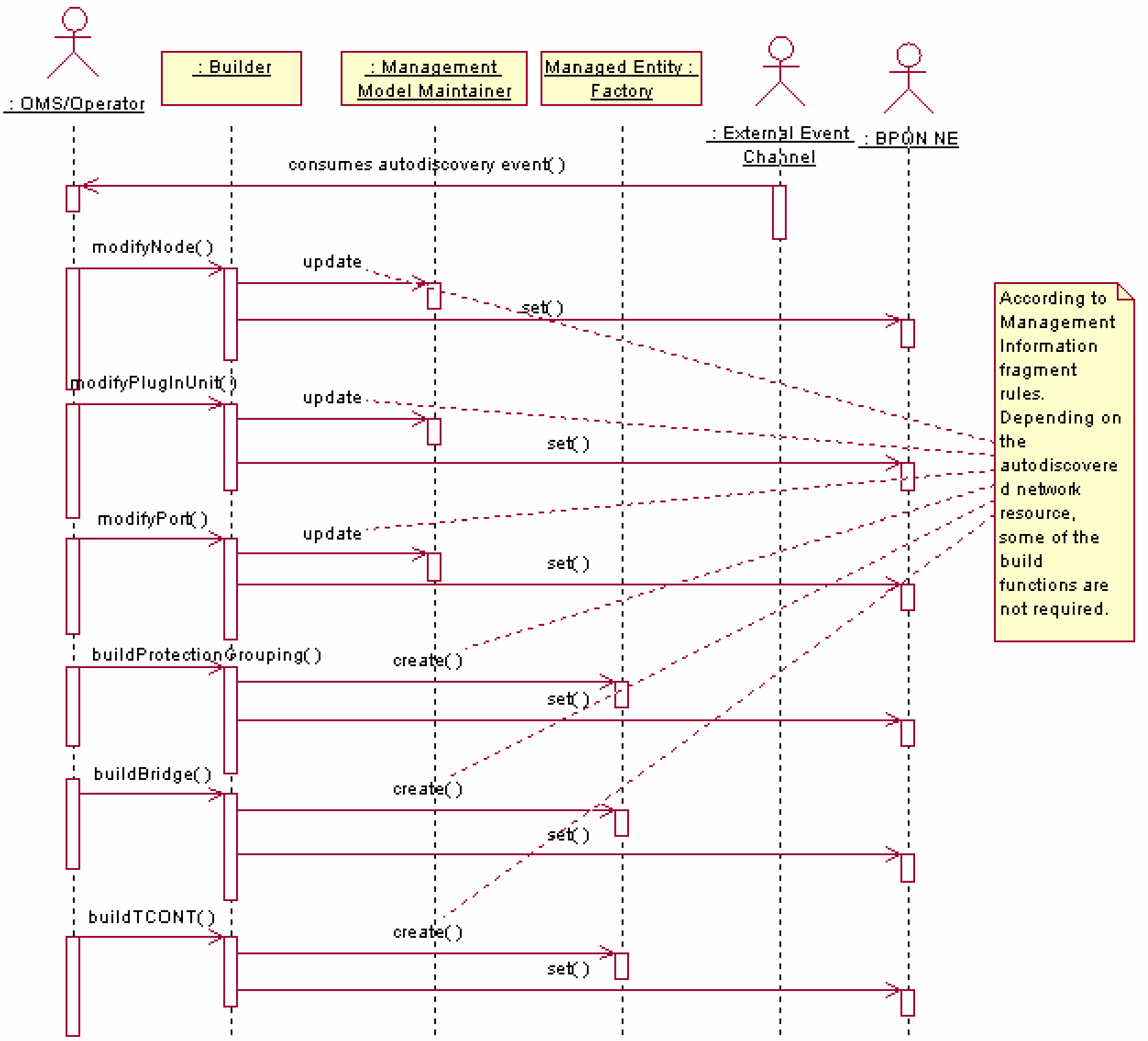


Figure 6-96 – Provision installed BPON resources sequence diagram with pre-provisioning



: OMS/Operator
: Builder
: Management Model Maintainer
Managed Entity : Factory
: External Event Channel
: BPON NE
consumes autodiscovery event( )
modifyNode( )
update
set( )
modifyPlugInUnit( )
update
set( )
modifyPort( )
update
set( )
buildProtectionGrouping( )
create( )
set( )
buildBridge( )
create( )
set( )
buildTCONT( )
create( )
set( )
According to Management Information fragment rules. Depending on the autodiscovered network resource, some of the build functions are not required.

Figure 6-97 – Provision installed BPON resources sequence diagram – No pre-provisioning

6.3.6.4 Provision service

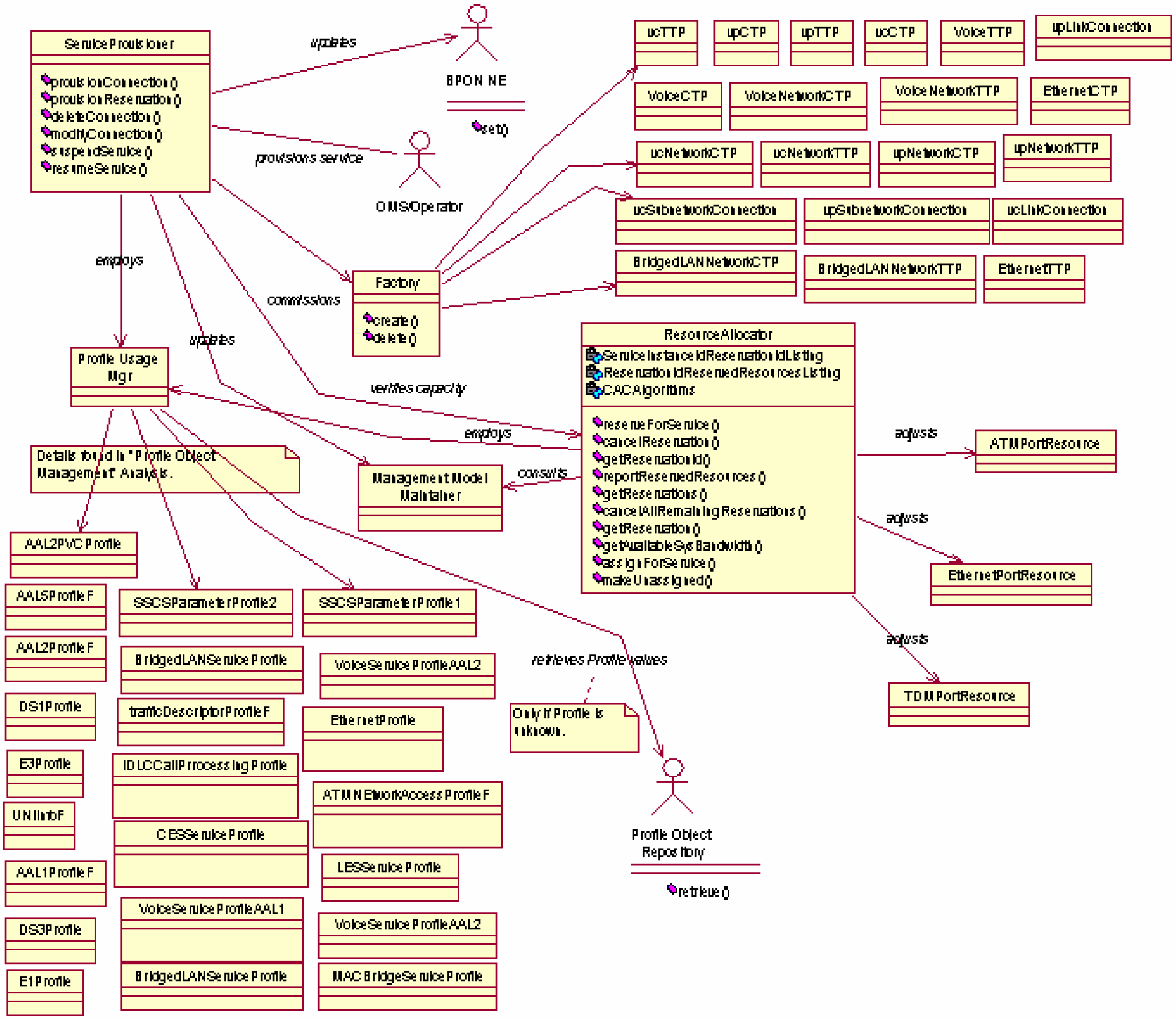


Figure 6-98 – Provision service class diagram

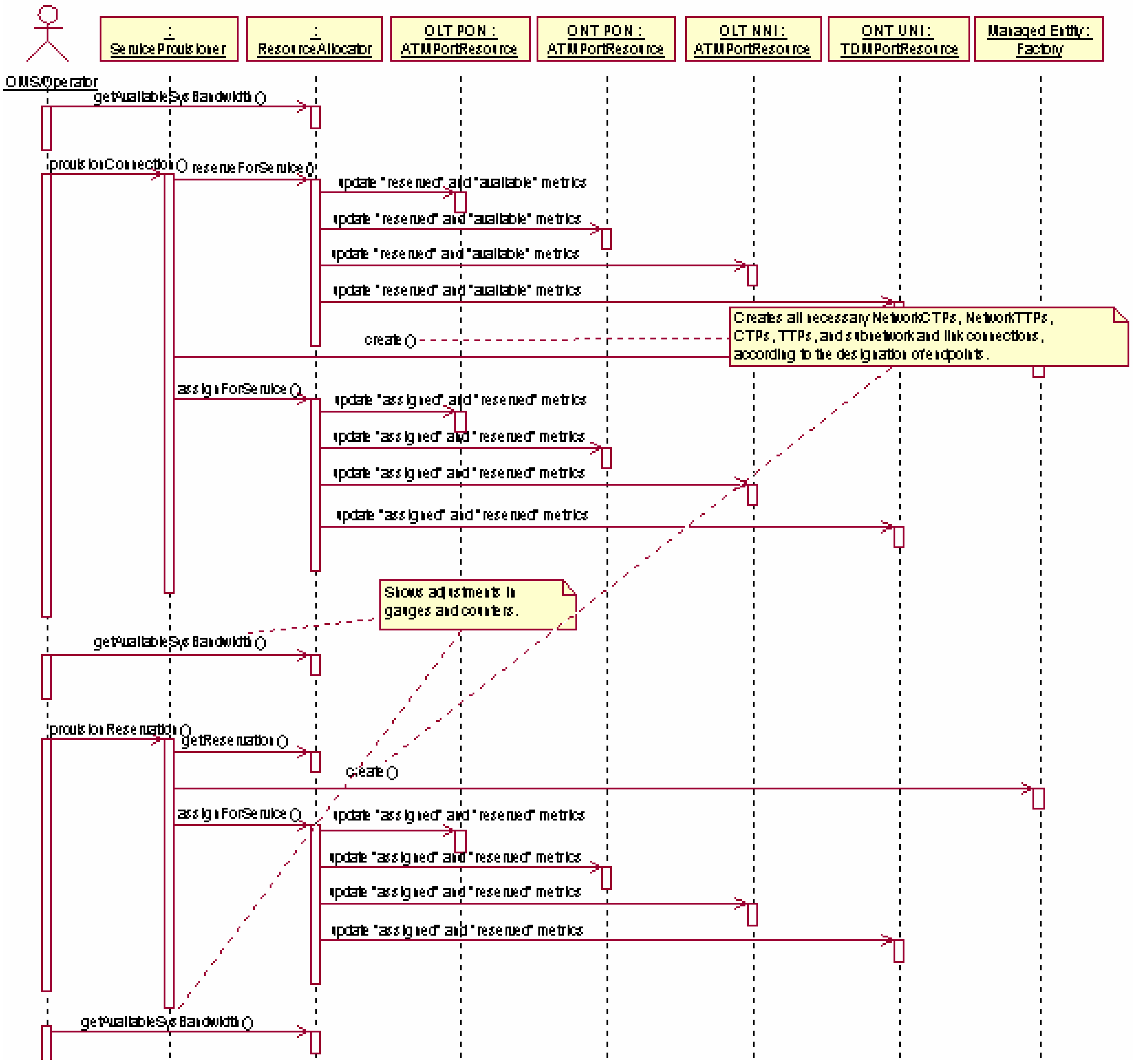

OMS/Operator
: ServiceProvisioner
: ResourceAllocator
OLT PON : ATMPortResource
ONT PON : ATMPortResource
OLT NNI : ATMPortResource
ONT UNI : TDMPortResource
Managed Entity : Factory
getAvailableSysBandwidth ()
provisionConnection ()
reserveForService ()
update "reserved" and "available" metrics
update "reserved" and "available" metrics
update "reserved" and "available" metrics
update "reserved" and "available" metrics
create ()
Creates all necessary NetworkCTPs, NetworkTTPs, CTPs, TTPs, and subnetwork and link connections, according to the designation of endpoints.
assignForService ()
update "assigned" and "reserved" metrics
update "assigned" and "reserved" metrics
update "assigned" and "reserved" metrics
update "assigned" and "reserved" metrics
Shows adjustments in gauges and counters.
getAvailableSysBandwidth ()
provisionReservation ()
getReservation ()
create ()
assignForService ()
update "assigned" and "reserved" metrics
update "assigned" and "reserved" metrics
update "assigned" and "reserved" metrics
update "assigned" and "reserved" metrics
getAvailableSysBandwidth ()

Figure 6-99 – Provision service and reservation connection sequence diagram

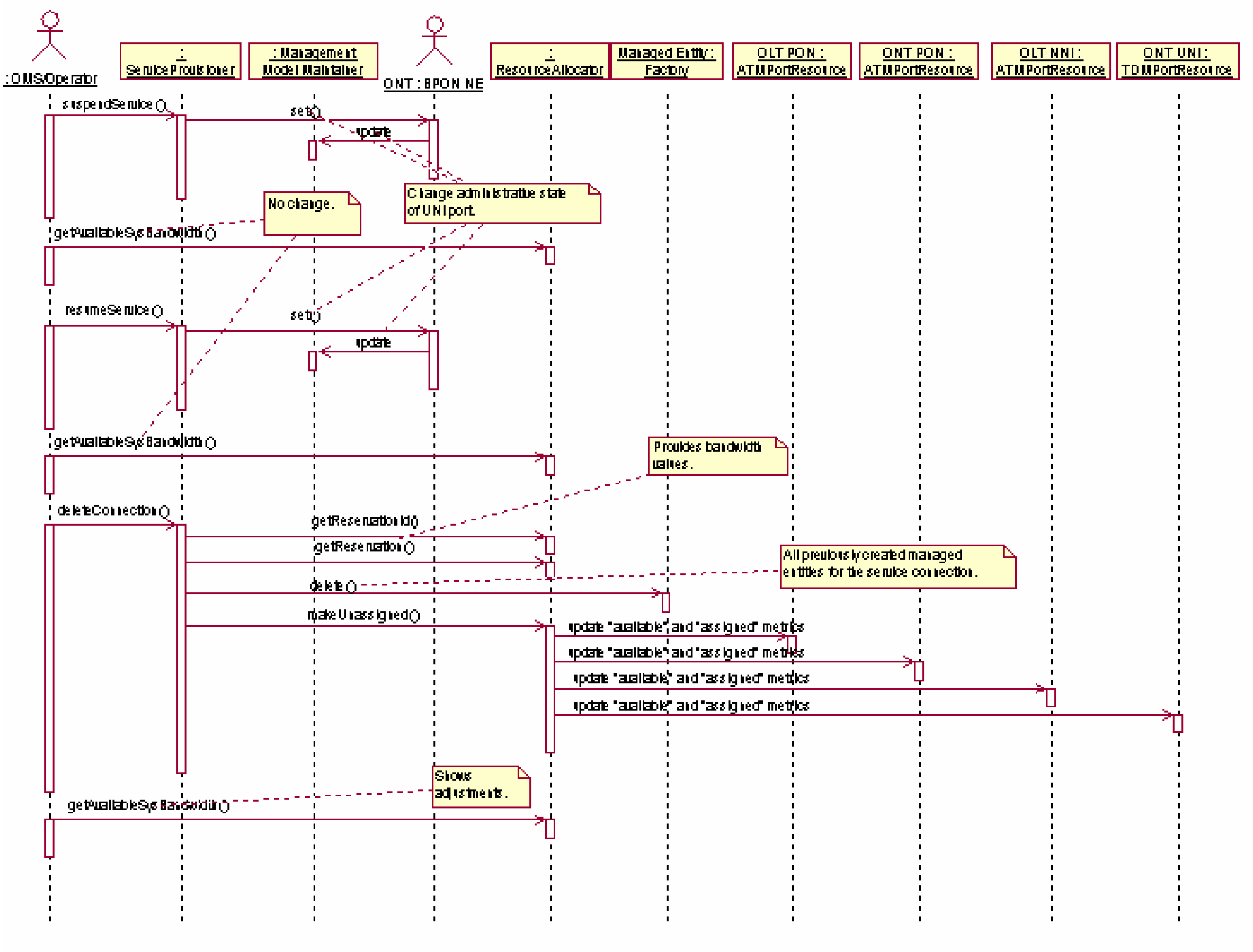

:OMSOperator
: ServiceProvisioner
: Management Model Maintainer
ONT : BPON NE
: ResourceAllocator
Managed Entity : Factory
OLT PON : ATMPortResource
ONT PON : ATMPortResource
OLT NNI : ATMPortResource
ONT UNI : TDMPortResource
suspendService()
set()
update
No change.
Change administrative state of UNI port.
getAvailableSysBandwidth()
resumeService()
set()
update
getAvailableSysBandwidth()
Provides bandwidth values.
deleteConnection()
getReservationId()
getReservation()
delete()
All previously created managed entities for the service connection.
makeUnassigned()
update "available" and "assigned" metrics
update "available" and "assigned" metrics
update "available" and "assigned" metrics
update "available" and "assigned" metrics
Shows adjustments.
getAvailableSysBandwidth()

Figure 6-100 – Suspend, resume and delete connection sequence diagram

Operations

Operation name	Operation purpose
1) provisionConnection	This operation provisions a connection between any two endpoints of a BPON fibre access system.
2) provisionReservation	This operation provisions service between the NNI of an OLT and the UNI of an ONT or between two UNIs based on an outstanding reservation.
3) deleteConnection	The operation tears down the existing service and connections.
4) modifyConnection	This operation provides the capability to modify the existing service.
5) suspendService	This operation disables the flow of user traffic through the service subnetwork connection.
6) resumeService	This operation enables the flow of user traffic through the service subnetwork connection.

Figure 6-101 – Service provisioner operations

Operation signatures

Operation name	Input parameters	Return value	Exceptions
1) provisionConnection	EndpointType (endpoint A), EndpointType (endpoint Z), NameSeqType (network profiles), ServiceInstanceIdType, RegistrationIdType, AdministrativeStateType	ManagedEntityIdType	UnknownNE, UnknownProfiles, UnknownPort, InsufficientBW, ConnectionCountExceeded, CommFailure, EquipmentFailure, ParameterViolation, AccessDenied, InsufficientPONBW, ProfileSuspended, ConnectionAlreadyExists
2) provisionReservation	ReservationIdType, AdministrativeStateType	ManagedEntityIdType	UnknownReservationId, AccessDenied
3) deleteConnection	ManagedEntityIdType	void	UnknownConnection, CommFailure, EquipmentFailure, AccessDenied
4) modifyConnection	ManagedEntityIdType, ManagedEntityIdType (port A), NameSeqType (new network profiles), NameSeqType (new service profiles)	ManagedEntityIdType	UnknownConnection, UnknownProfiles, InsufficientBW, UnknownPort, AccessDenied, ProfileSuspended
5) suspendService	ServiceInstanceIdType, GeneralizedTimeType (start time), GeneralizedTimeType (stop time)	void	UnknownServiceInstance, AccessDenied, InvalidStartTime, InvalidStopTime
6) resumeService	ServiceInstanceIdType	void	UnknownServiceInstance, AccessDenied

Figure 6-102 – Service provisioner signatures

Exceptions

Exception raised	Description
AccessDenied	System is not granted access to this interface object.
CommFailure	There was a DCN link failure between the NE and the supplier management system.
ConnectionAlreadyExists	There already exists a subnetwork connection with the same endpoints.
ConnectionCountExceeded	The maximum number of connections for the OLT or PON port has been exceeded with this request for service provisioning.
EquipmentFailure	The NE currently has a failure condition preventing the requested transaction from being completed.
InsufficientPONBW	The ONT or ONU cannot be ranged or the service connection cannot be provisioned due to insufficient bandwidth on the APONLink.
InsufficientBW	The CAC algorithm indicates that requested service requires too much bandwidth for the OLT.
InvalidStartTime	The new start time is inconsistent with the current trigger time matrix or the new stop time.
InvalidStopTime	The new stop time is inconsistent with the current trigger time matrix or the new start time.
ParameterViolation	This exception is raised when the endpoint parameters do not match the protocol characteristics of the port, or when the values are out of range or invalid duplicates.
ProfileSuspended	The named profile(s) in the invocation have been suspended for use within the supplier management system by the OMS or operator.
UnknownConnection	The subnetwork connection is not known by the supplier management system.
UnknownNE	Identified NE is unknown to the supplier management system.
UnknownPort	The identified port is unknown to the supplier management system.
UnknownProfiles	This exception is raised if the profile name provided is unknown to the supplier management system and cannot be retrieved from the profile object repository.
UnknownReservationId	The supplier management system does not recognize this reservation Id.
UnknownServiceInstance	The service instance is unknown to the supplier management system.

Figure 6-103 – Service provisioner exceptions

6.3.6.5 Reserve resources

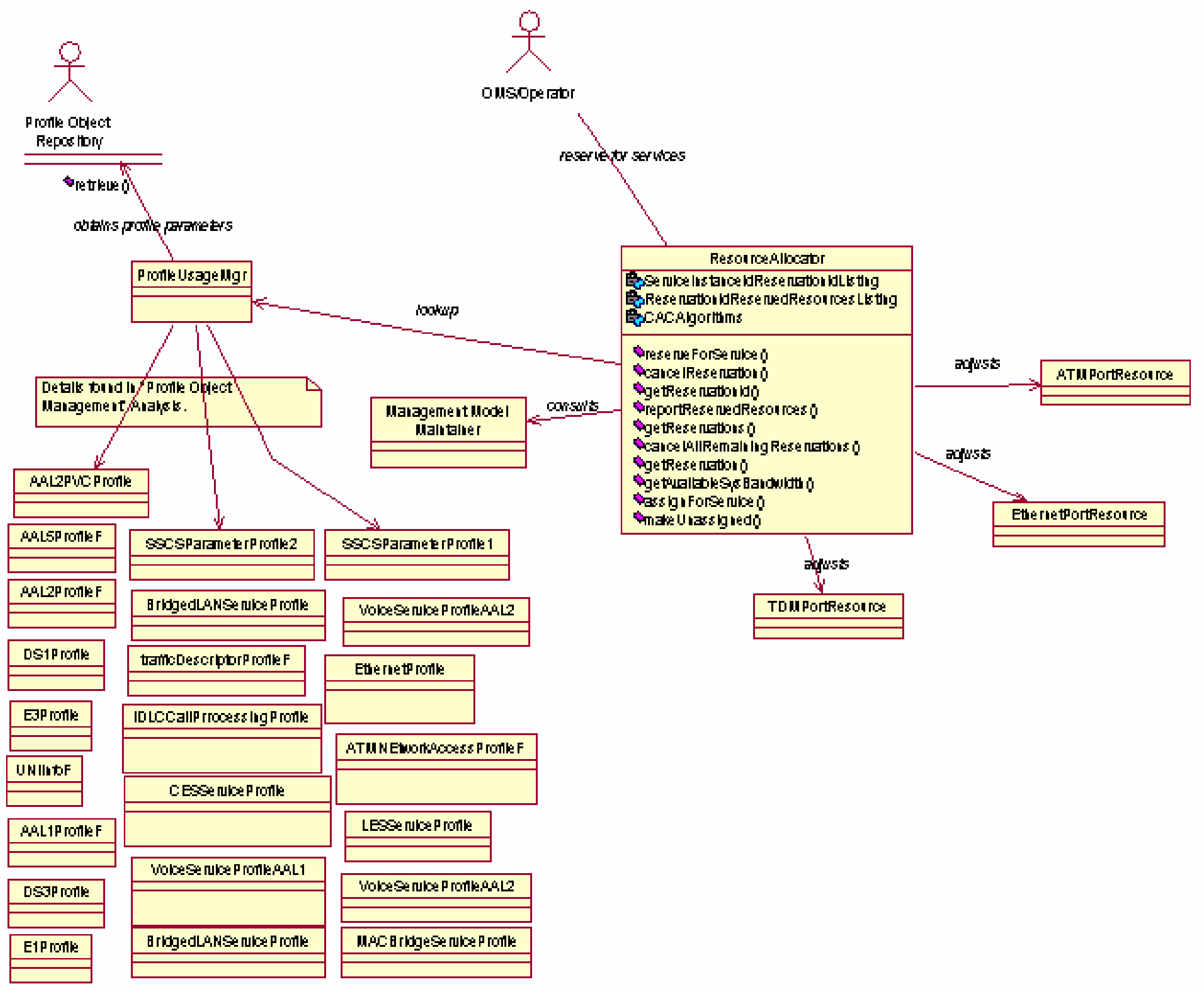


Figure 6-104 – Reserve resources class diagram

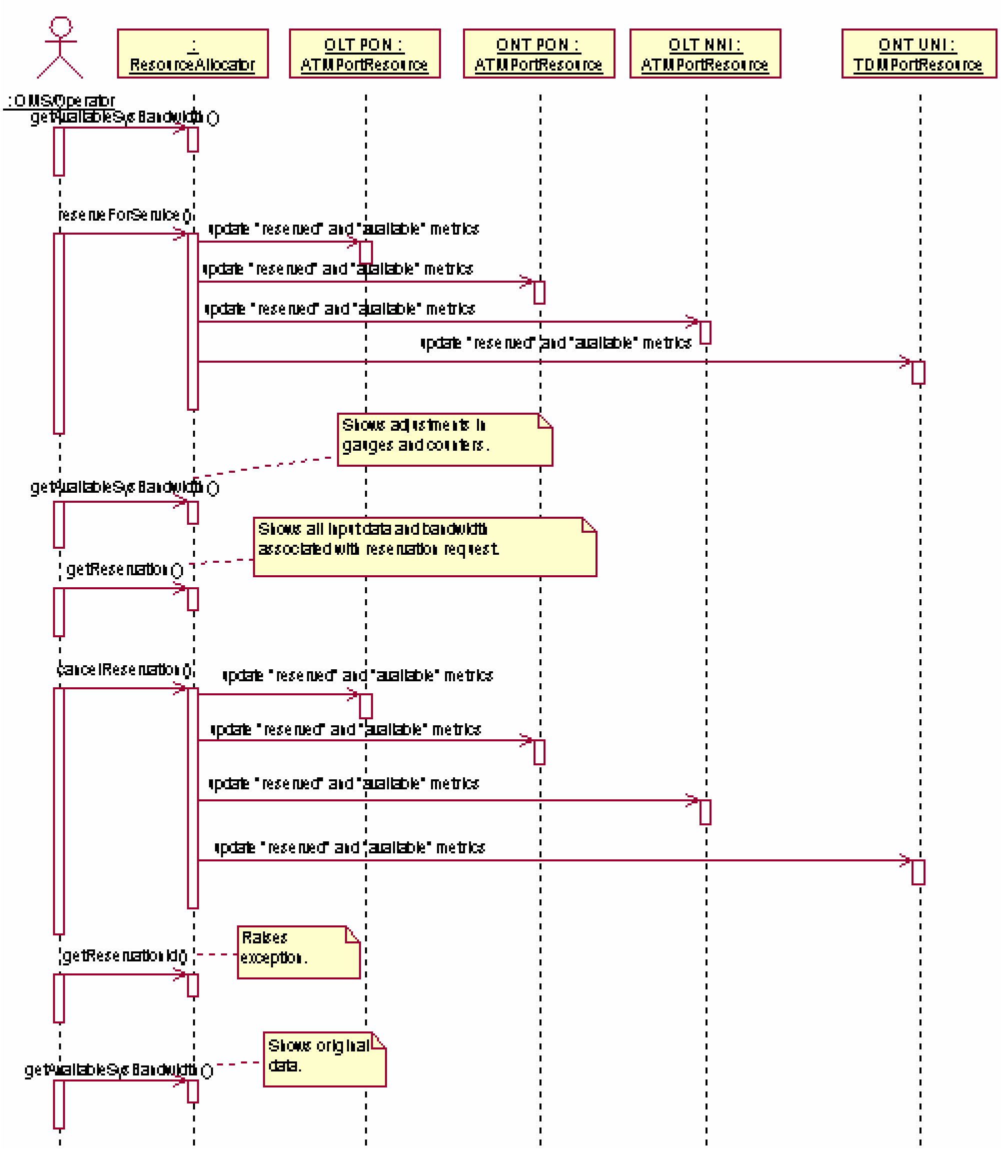

: OMSOperator
: ResourceAllocator
OLT PON : ATMPortResource
ONT PON : ATMPortResource
OLT NNI : ATMPortResource
ONT UNI : TDMPortResource
getAvailableSysBandwidth()
reserveForService()
update "reserved" and "available" metrics
update "reserved" and "available" metrics
update "reserved" and "available" metrics
update "reserved" and "available" metrics
Shows adjustments in gauges and counters.
getAvailableSysBandwidth()
Shows all input data and bandwidth associated with reservation request.
getReservation()
cancelReservation()
update "reserved" and "available" metrics
update "reserved" and "available" metrics
update "reserved" and "available" metrics
update "reserved" and "available" metrics
Raises exception.
getReservationId()
Shows original data.
getAvailableSysBandwidth()

Figure 6-105 – Reserve and cancel reservation sequence diagram

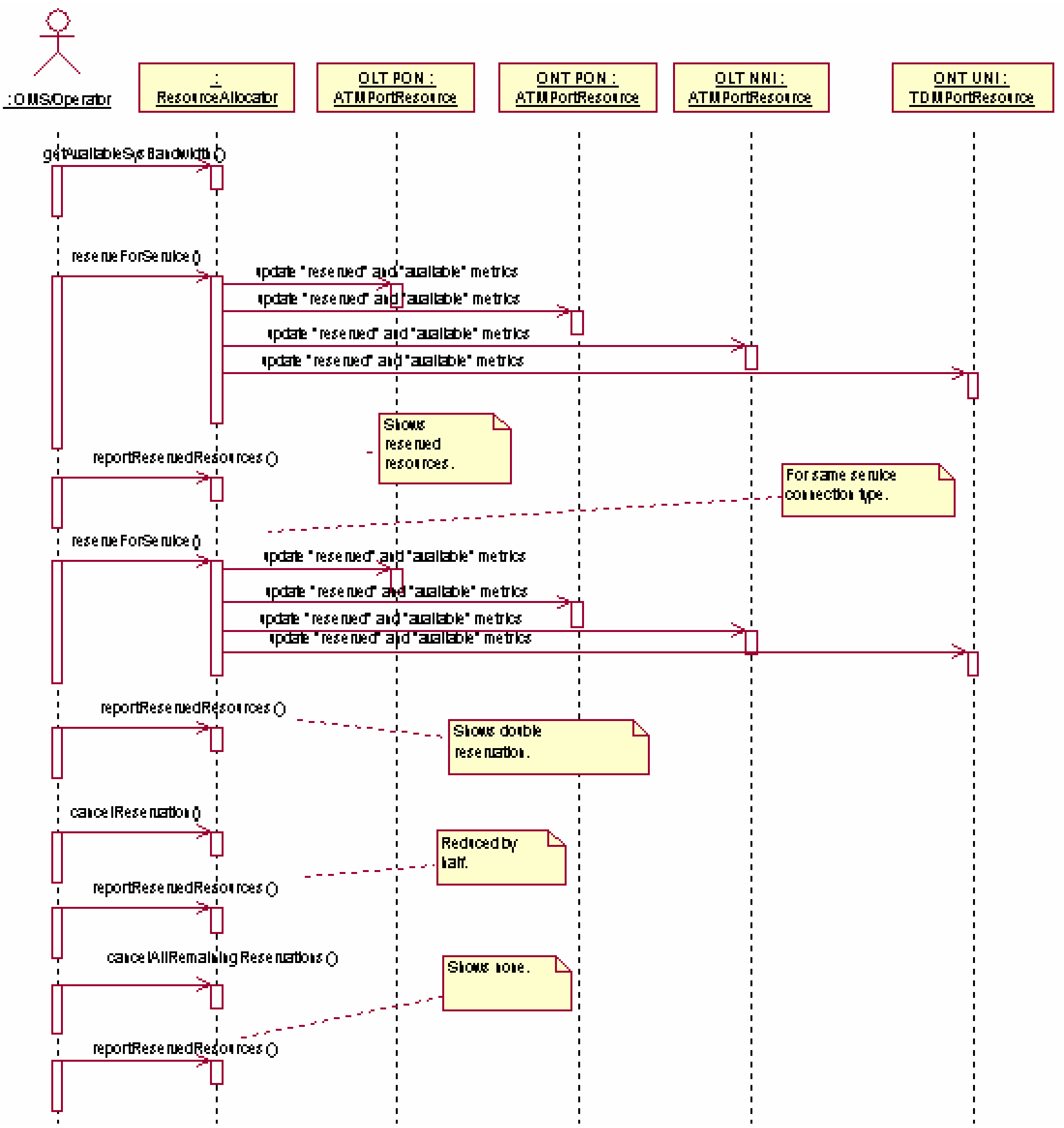

:OMSOperator
: ResourceAllocator
OLT PON : ATMPortResource
ONT PON : ATMPortResource
OLT NNI : ATMPortResource
ONT UNI : TDMPortResource
getAvailableSysBandwidth()
reserveForService()
update "reserved" and "available" metrics
update "reserved" and "available" metrics
update "reserved" and "available" metrics
update "reserved" and "available" metrics
Shows reserved resources.
reportReservedResources()
For same service connection type.
reserveForService()
update "reserved" and "available" metrics
update "reserved" and "available" metrics
update "reserved" and "available" metrics
update "reserved" and "available" metrics
reportReservedResources()
Shows double reservation.
cancelReservation()
Reduced by half.
reportReservedResources()
cancelAllRemainingReservations()
Shows none.
reportReservedResources()

Figure 6-106 – Reserve resources sequence diagram

Operations

Operation name	Operation purpose
1) reserveForService	This operation reserves bandwidth for a network resource such as ONT, ONU or NT whose installation is pending.
2) cancelReservation	This operation is used to delete the reservation and release the resources from the reserved system capacity.
3) getReservationId	This operation is used to display the reservation Id associated with the service instance Id that is assigned for the reserved bandwidth.
4) reportReservedResources	This operation is used by the OMS to display the current reserved bandwidth in the specific headend NE (in this case the OLT).
5) getReservations	This operation is used by OMS to retrieve all the reservations associated with the given NE.
6) cancelAllRemainingReservations	This operation is used to delete all the remaining reservations against capacity associated with a given network element.
7) getReservation	This operation is used to investigate the origins of a reservation of capacity within an NE.
8) getAvailableSysBandwidth	This operation is used to determine the amount of capacity remaining for service connection reservation or assignment for a network element.

Figure 6-107 – Resource allocator operations

Operation signatures

Operation name	Input parameters	Return value	Exceptions
1) reserveForService	EndPointType (endpoint A), EndPointType (endpoint Z), NameSeqType (network profiles), ServiceInstanceIdType	ReservationBandwidthType	UnknownNE, UnknownPort, UnknownProfiles, InsufficientBW, MaxSubtendingNodes Exceeded, ConnectionCountExceeded, CommFailure, AccessDenied, ProfileSuspended
2) cancelReservation	ReservationIdType	AvailableSysBandwidthSeqType	UnknownReservationId, CommFailure, AccessDenied
3) getReservationId	ServiceInstanceIdType	ReservationIdType	UnknownServiceInstance, AccessDenied
4) reportReservedResources	ManagedEntityIdType	ReservedBandwidthSeqType	UnknownNE, AccessDenied
5) getReservations	ManagedEntityIdType (NE)	ReservationIdSeqType	UnknownNE, AccessDenied
6) cancelAllRemaining Reservations	ManagedEntityIdType (NE)	AvailableSysBandwidthSeqType	UnknownNE, CommFailure, AccessDenied
7) getReservation	ReservationIdType	ReservationInfoType	UnknownReservationId, AccessDenied
8) getAvailableSys Bandwidth	ManagedEntityIdType (NE)	AvailableSysBandwidthSeqType	UnknownNE, CommFailure, AccessDenied

Figure 6-108 – Resource allocator signatures

Exceptions

Exception raised	Description
AccessDenied	System is not granted access to this interface object.
CommFailure	There was a DCN link failure between the NE and the supplier management system.
ConnectionCountExceeded	The maximum number of connections for the OLT or PON port has been exceeded with this request for service provisioning.
InsufficientBW	The CAC algorithm indicates that requested service requires too much bandwidth for the OLT.
MaxSubtendingNodesExceeded	The maximum engineered number of subtending nodes for the identified PON interface has been exceeded with this request for service provisioning or reservation.
ProfileSuspended	The named profile(s) in the invocation have been suspended for use within the supplier management system by the OMS or operator.
UnknownNE	Identified NE is unknown to the supplier management system.
UnknownPort	The identified port is unknown to the supplier management system.
UnknownProfiles	This exception is raised if the profile name provided is unknown to the supplier management system and cannot be retrieved from the profile object repository.
UnknownReservationId	The supplier management system does not recognize this reservation Id.
UnknownServiceInstance	The service instance is unknown to the supplier management system.

Figure 6-109 – Resource allocator exceptions

6.3.7 Archiving and bulk transfer

6.3.7.1 Bulk transfer

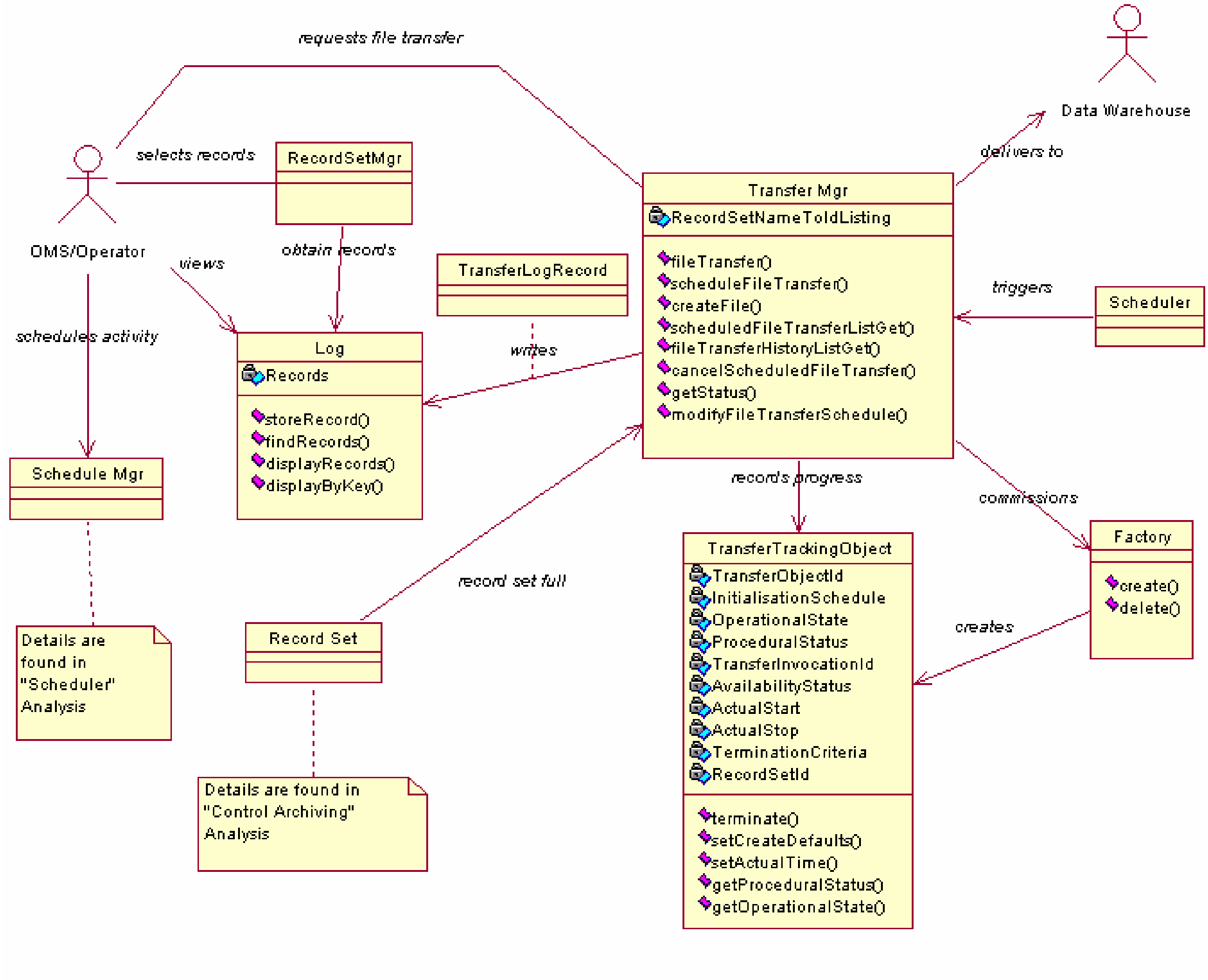


Figure 6-110 – Bulk transfer class diagram

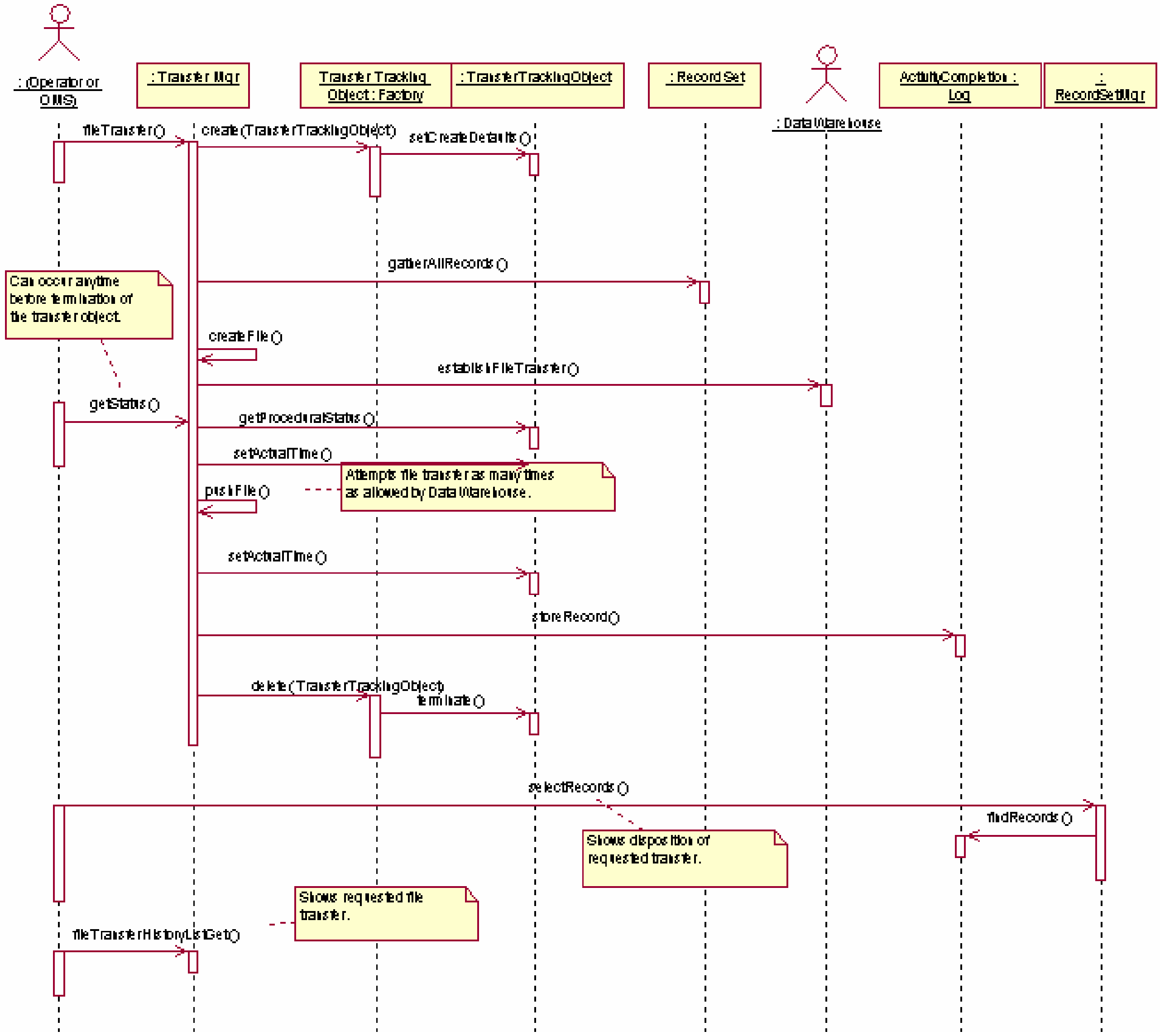


Figure 6-111 – Immediate bulk transfer sequence diagram

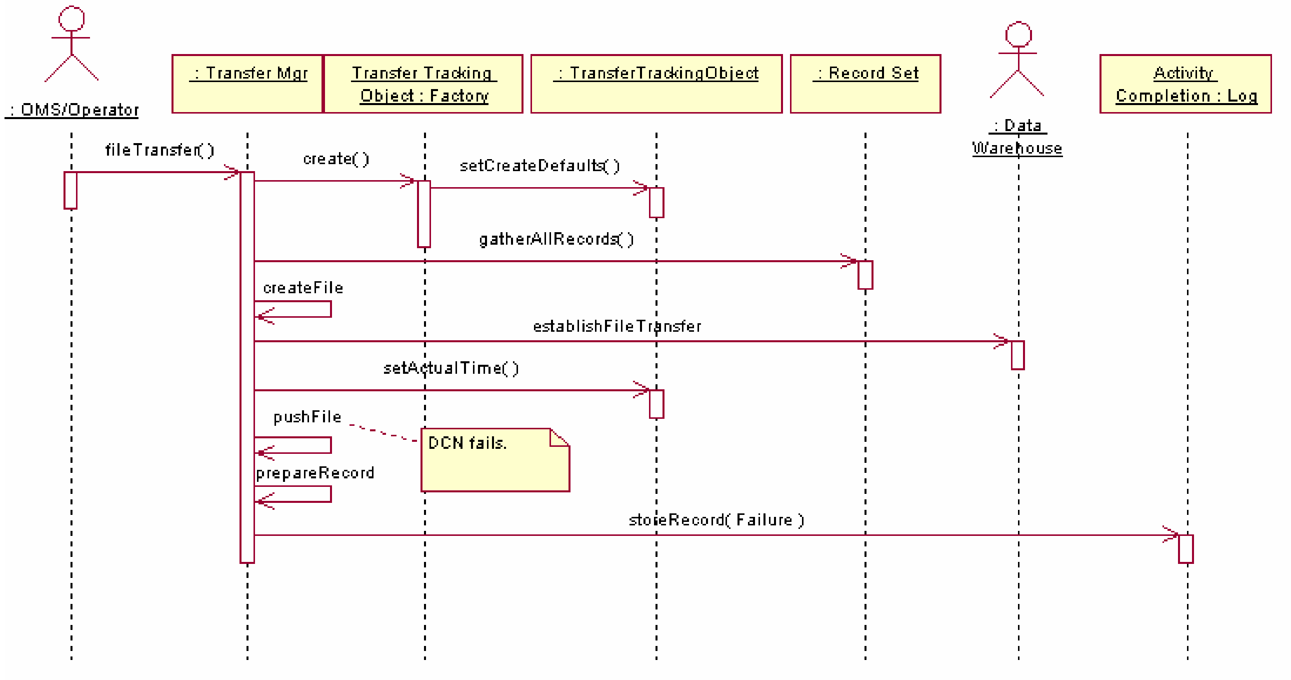


Figure 6-112 – Bulk transfer failure sequence diagram

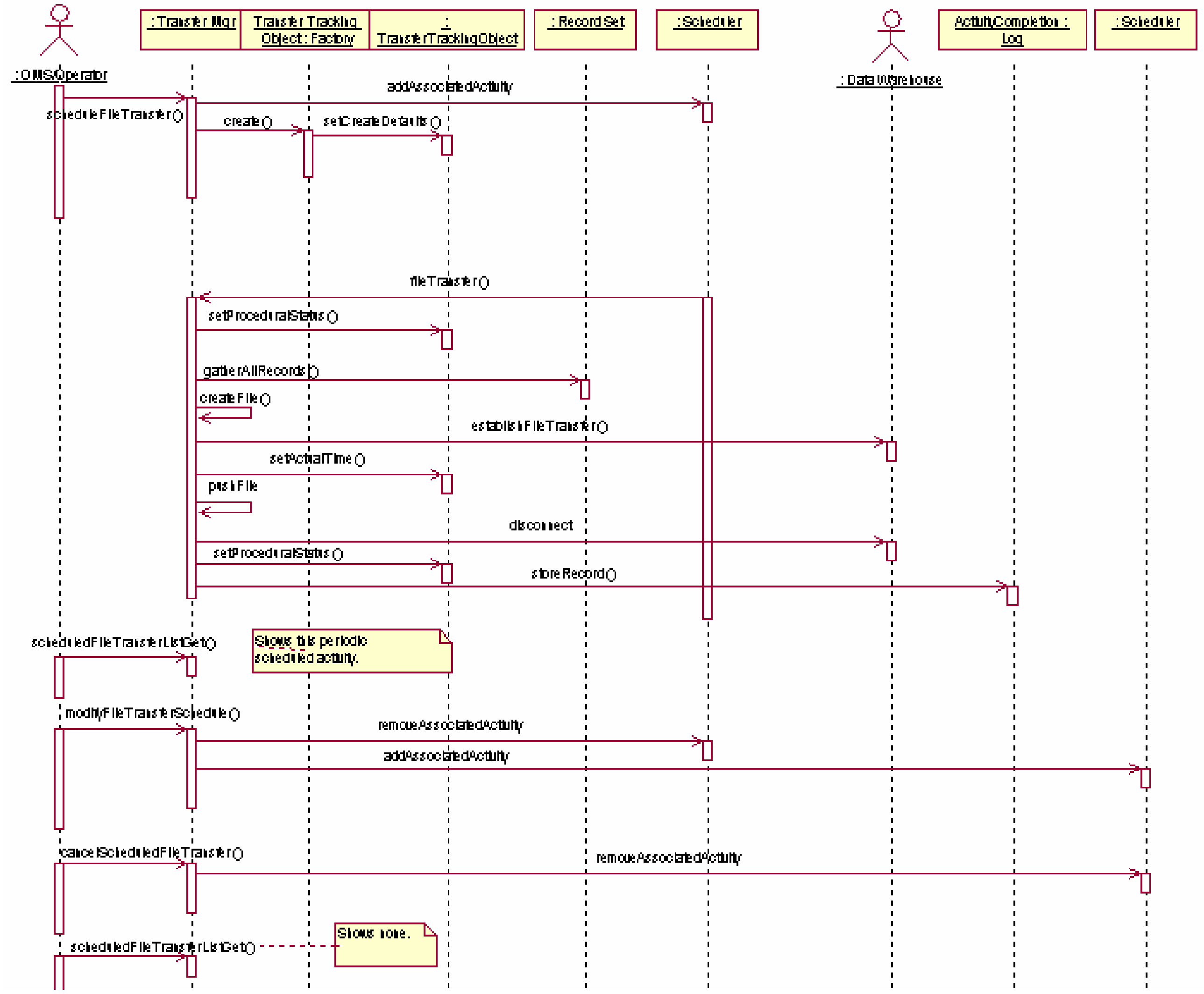


Figure 6-113 – Scheduled bulk transfer sequence diagram

Operations

Operation name	Operation purpose
1) fileTransfer	The file transfer is initiated immediately by this operation.
2) scheduleFileTransfer	The file transfer is scheduled for future initiation by this operation.
3) modifyFileTransferSchedule	The file transfer schedule is modified by this operation.
4) cancelScheduledFileTransfer	The scheduled file transfer is cancelled.
5) getStatus	This operation allows the client to check the status of a transfer before its completion.
6) fileTransferHistoryListGet	This operation is used to retrieve the list of all completed file transfers for the supplier management system.
7) scheduledFileTransferListGet	This operation is used to retrieve the names of all existing scheduled file transfers defined for the supplier management system.

Figure 6-114 – Transfer manager operations

Operation signatures

Operation name	Input parameters	Return value	Exceptions
1) fileTransfer	ManagedEntityIdType, DCNAddressType, UserIdType, PasswordType, FilenameType, boolean (overwrite?)	TransferTrackingObject IdType	AccessDenied, CommFailure, UnknownRecordSet, UnknownDestinationServer
2) scheduleFileTransfer	ManagedEntityIdType, DCNAddressType, UserIdType, PasswordType, FilenameType, boolean (overwrite?), UserLabelType (scheduler name)	TransferTrackingObject IdType	AccessDenied, UnknownRecordSet, UnknownDestinationServer, UnknownScheduler, InvalidScheduler
3) modifyFileTransferSchedule	TransferTrackingObjectIdType, UserLabelType (scheduler name)	void	AccessDenied, UnknownTransferProcess, UnknownScheduler, InvalidScheduler
4) cancelScheduledFileTransfer	TransferTrackingObjectIdType	void	AccessDenied, UnknownTransferProcess
5) getStatus	TransferTrackingObjectIdType	StatusValueType	AccessDenied, UnknownTransferProcess
6) fileTransferHistoryListGet		FileTransferHistorySeq Type	AccessDenied
7) scheduledFileTransferListGet		ScheduledFileTransfer SeqType	AccessDenied

Figure 6-115 – Transfer manager signatures

Exceptions

Exception raised	Description
AccessDenied	System is not granted access to this interface object.
CommFailure	There was a DCN link failure between the NE and the supplier management system.
InvalidScheduler	The scheduler parameters' values are outside defined scope.
UnknownDestinationServer	The identified destination server cannot be accessed by the transfer agent.
UnknownRecordSet	Record set identified in the request is unknown to the supplier management system.
UnknownScheduler	The named scheduler is unknown to the supplier management system.
UnknownTransferProcess	The status of the identified transfer process could not be checked because it is unknown to the supplier management system.

Figure 6-116 – Transfer manager exceptions

6.3.7.2 Control archives

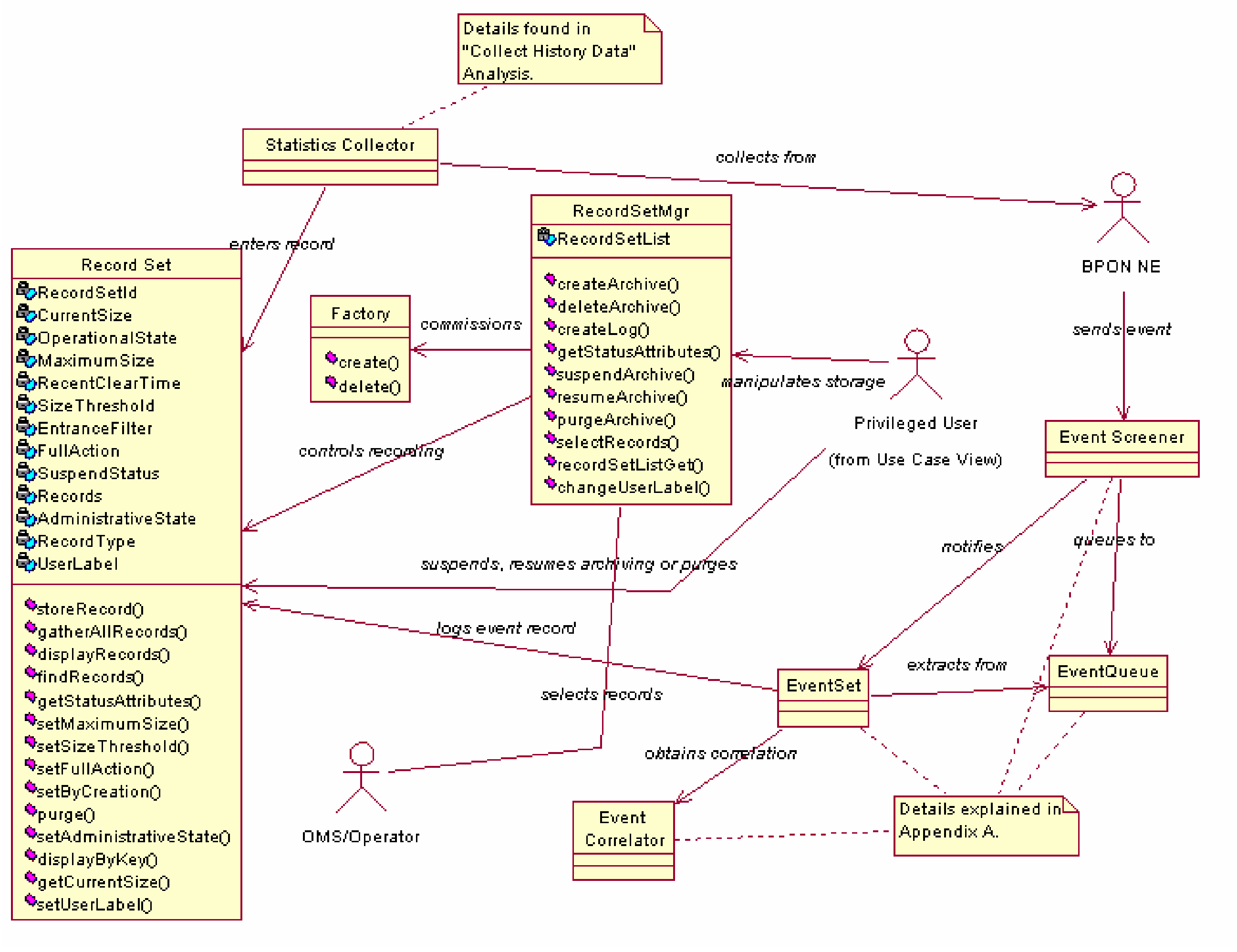


Figure 6-117 – Control archiving class diagram

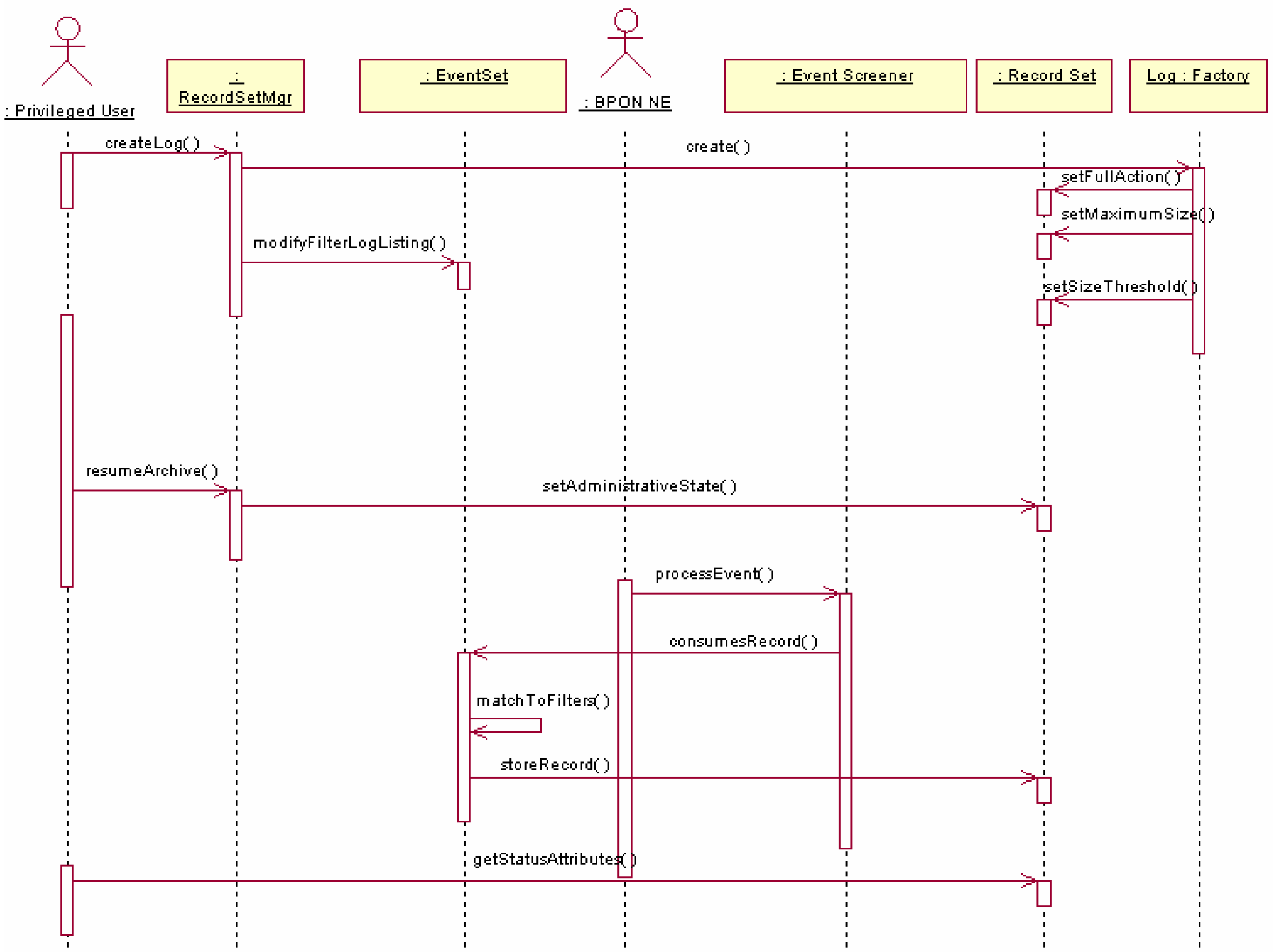


Figure 6-118 – Create log sequence diagram

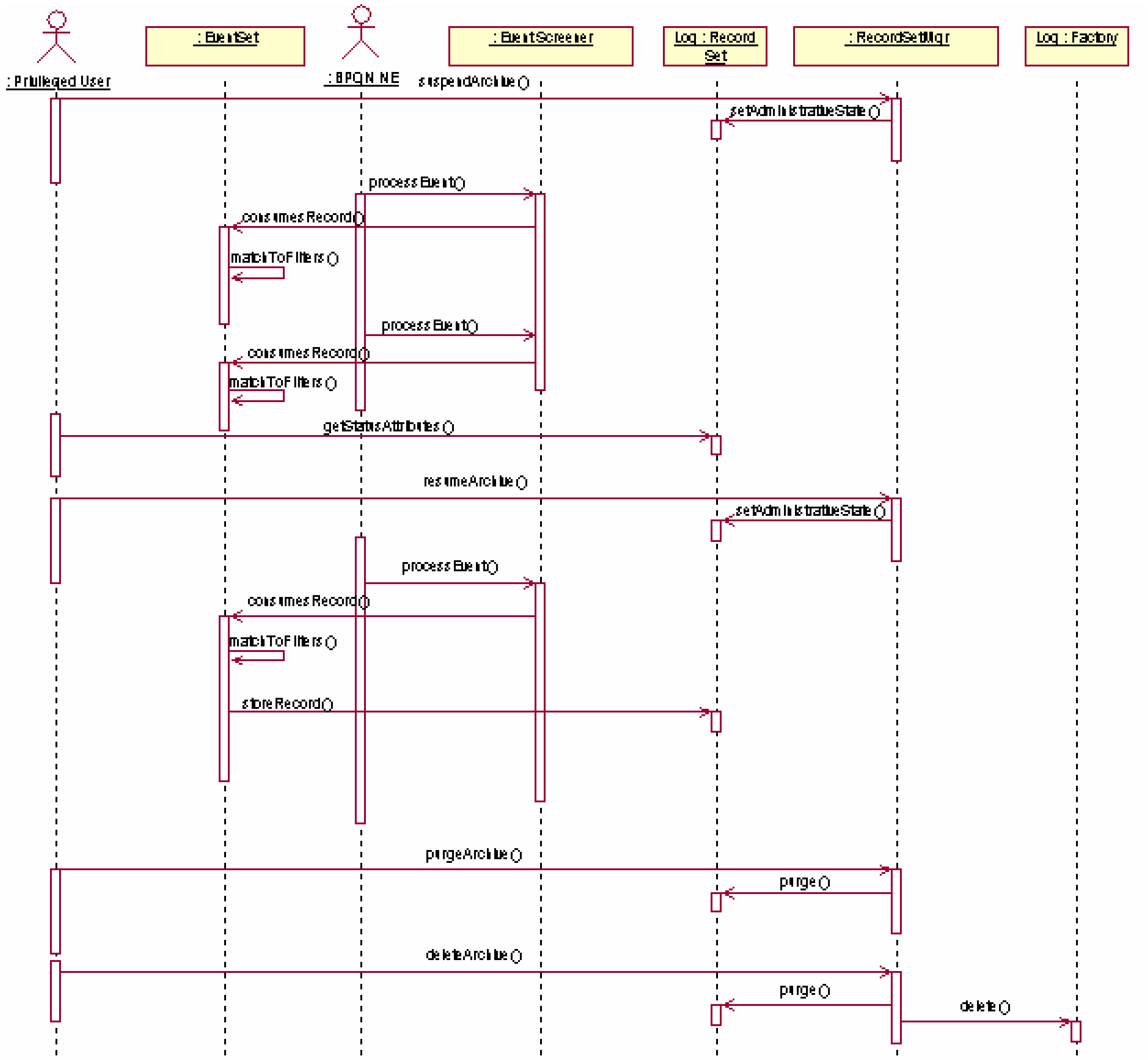


Figure 6-119 – Control log sequence diagram

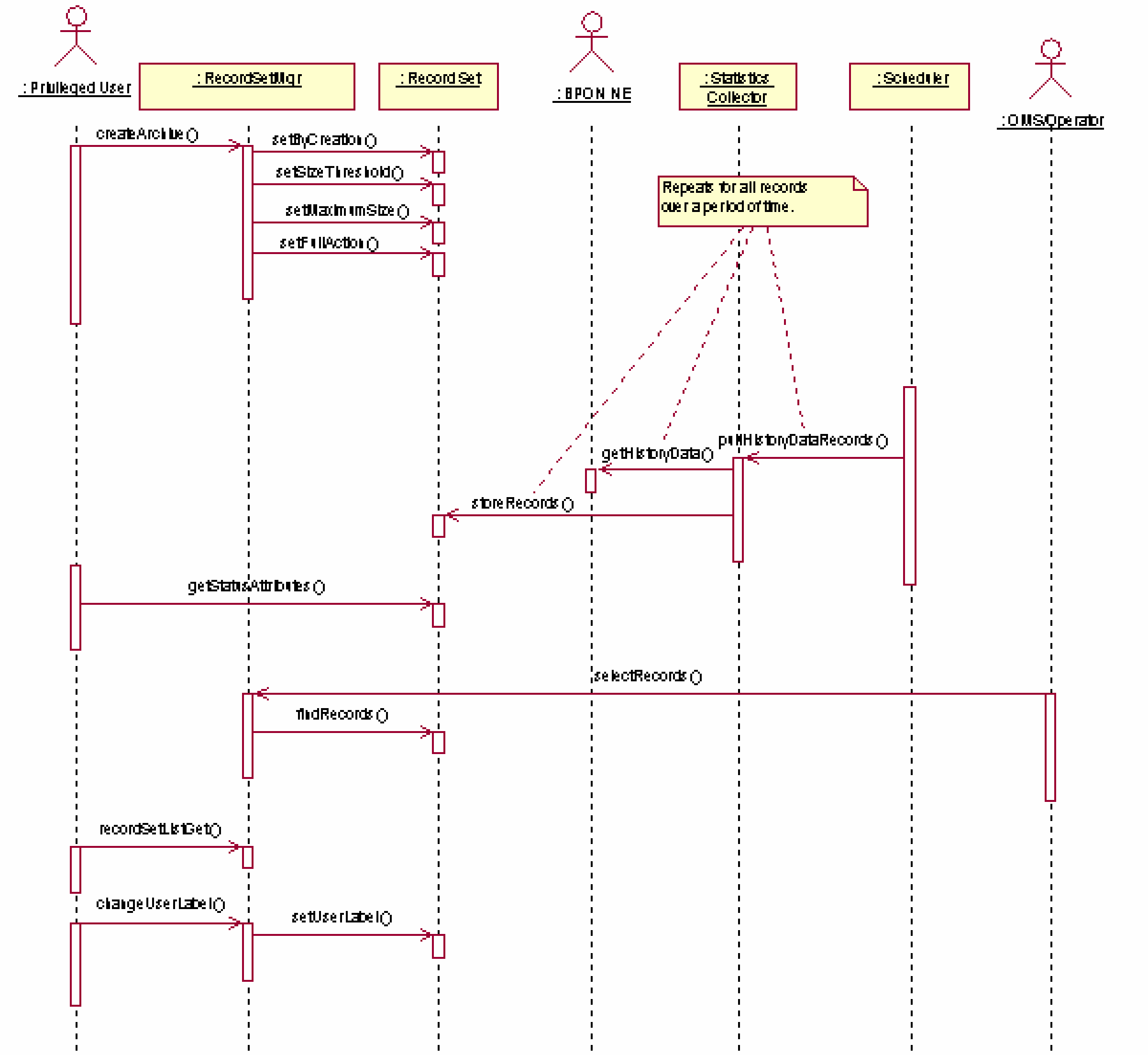


Figure 6-120 – Control statistics archiving sequence diagram

Operations

Operation name	Operation purpose
1) createLog	This operation is used to create a record set in the supplier management system for the purposes of archiving event information.
2) createArchive	This operation is used to create a record set for storing data.
3) getStatusAttributes	At any time the operator or OMS can view the current status of an archive through this operation.
4) suspendArchive	Once the short-term archive has been created and initialized for use, the OMS can suspend its use by invoking this operation.
5) resumeArchive	This operation resumes recording in an archive or initializes the recording within a record set that has been constructed in a locked state.
6) deleteArchive	This operation deletes an archive from the supplier management system.
7) purgeArchive	This operation removes the information contained within a specified archive. However, the archive continues its recording.
8) selectRecords	After the creation of an archive, this operation allows the selection of some (or all) of the records found within it. The selection is based on a filter.
9) recordSetListGet	This operation allows an OMS to get a complete listings of record sets managed by the supplier management system.
10) changeUserLabel	After the creation of a short-term archive, the OMS can change the user label assigned to the archive.

Figure 6-121 – Record set manager operations

Operation signatures

Operation name	Input parameters	Return value	Exceptions
1) createLog	UserLabelType, AdministrativeStateType NameType (selection filter), FullActionType, MaxSizeType, SizeThresholdType	ManagedEntityIdType	RecordSetExists, DuplicateUserLabel, AccessDenied
2) createArchive	UserLabelType, AdministrativeStateType, RecordKindType, MaxSizeType	ManagedEntityIdType	RecordSetExists, DuplicateUserLabel, AccessDenied
3) getStatusAttributes	ManagedEntityIdType	RecordSetStatusType	AccessDenied, UnknownRecordSet
4) suspendArchive	ManagedEntityIdType	void	AccessDenied, UnknownRecordSet
5) resumeArchive	ManagedEntityIdType	void	AccessDenied, UnknownRecordSet
6) deleteArchive	ManagedEntityIdType	void	AccessDenied, UnknownRecordSet
7) purgeArchive	ManagedEntityIdType	void	AccessDenied, UnknownRecordSet
8) selectRecords	FilterType, ManagedEntityIdType	RecordSeqType	UnknownRecordSet, Timeout, NoSuchRecords, AccessDenied, TooManyRecords
9) recordSetListGet	CreationModeType	ManagedEntityIdSeqType	AccessDenied
10) changeUserLabel	ManagedEntityIdType, UserLabelType	void	UnknownRecordSet, AccessDenied, DuplicateUserLabel

Figure 6-122 – Record set manager signatures

Exceptions

Exception raised	Description
AccessDenied	System is not granted access to this interface object.
DuplicateUserLabel	The user label provided in the request has been used to label another archive, i.e., one that is defined by a different set of creation request parameters.
NoSuchRecords	No records among the designated record sets matches the selection criteria.
RecordSetExists	The record set defined by the parameters of the creation request already exists in the supplier management system.
Timeout	The process duration reached a system-defined timeout before the process could complete.
TooManyRecords	The number of records selected for retrieval produces a response to the request that exceeds a predetermined size.
UnknownRecordSet	Record set identified in the request is unknown to the supplier management system.

Figure 6-123 – Record set manager exceptions

6.3.7.3 Performance and traffic monitoring reporting control

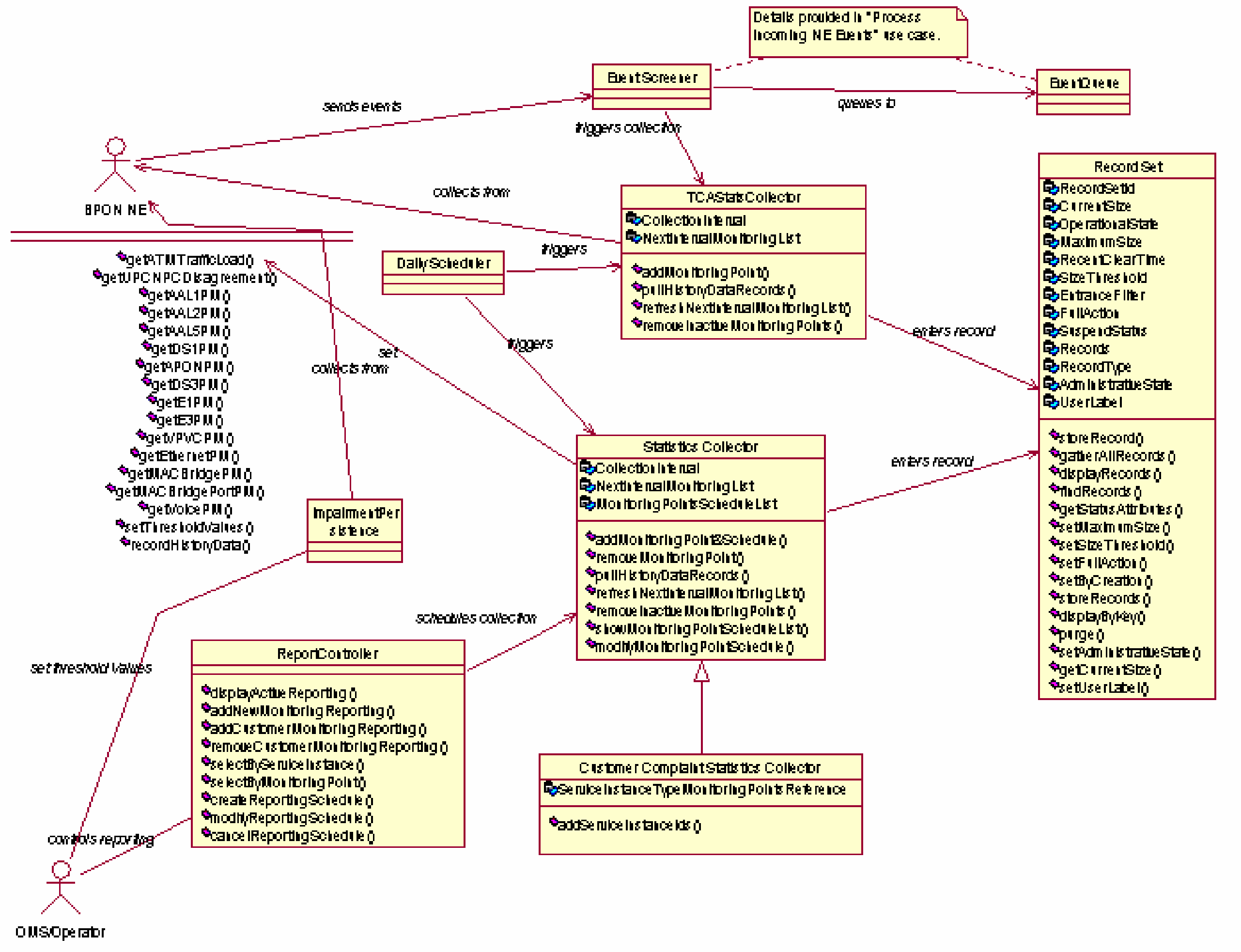


Figure 6-124 – Performance and traffic monitoring reporting control class diagram

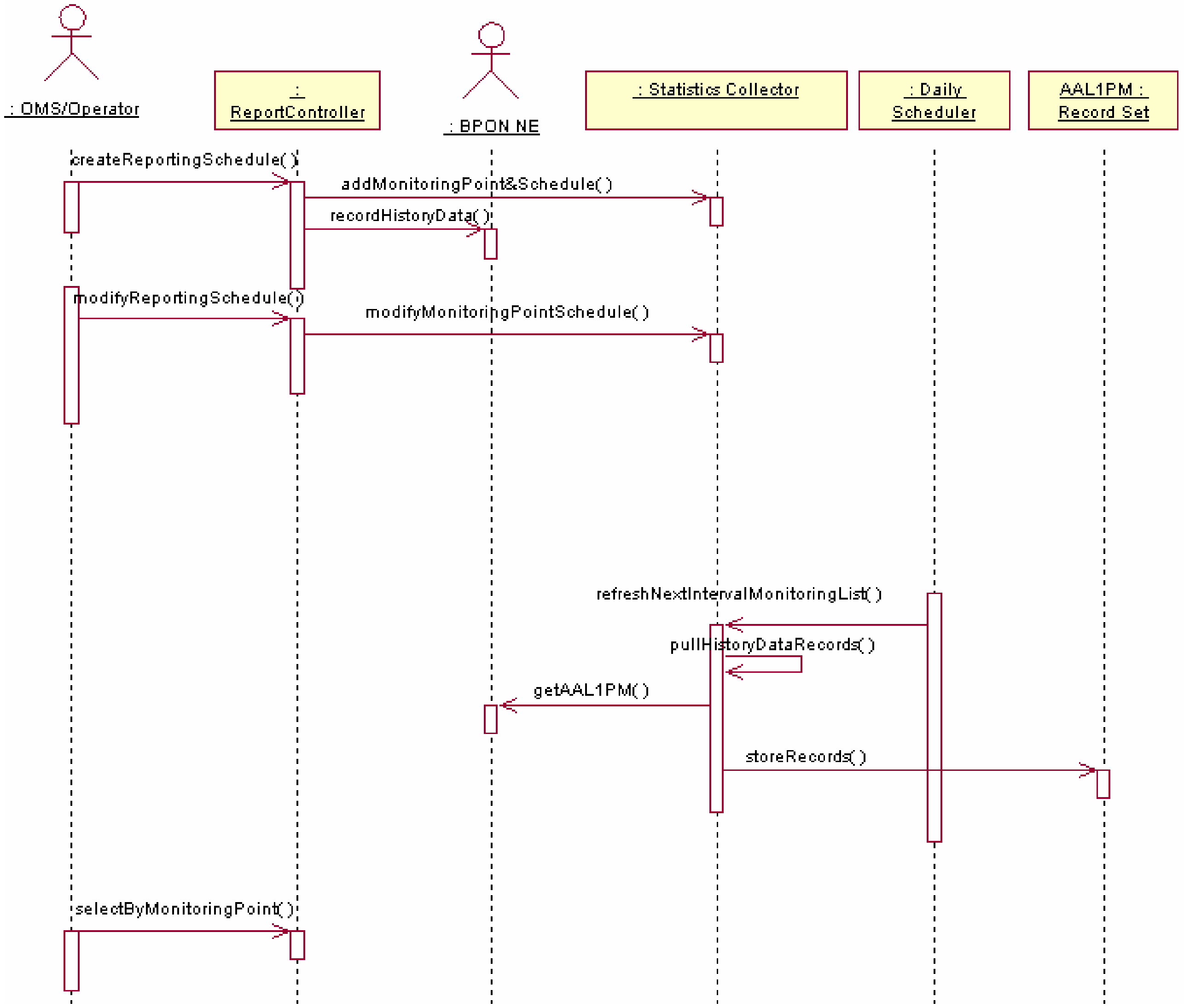

: OMS/Operator
: ReportController
: BPON NE
: Statistics Collector
: Daily Scheduler
AAL1PM : Record Set
createReportingSchedule( )
addMonitoringPoint&Schedule( )
recordHistoryData( )
modifyReportingSchedule( )
modifyMonitoringPointSchedule( )
refreshNextIntervalMonitoringList( )
pullHistoryDataRecords( )
getAAL1PM( )
storeRecords( )
selectByMonitoringPoint( )

Figure 6-125 – Performance and traffic monitoring reporting (scheduled) sequence diagram – AAL1PM example

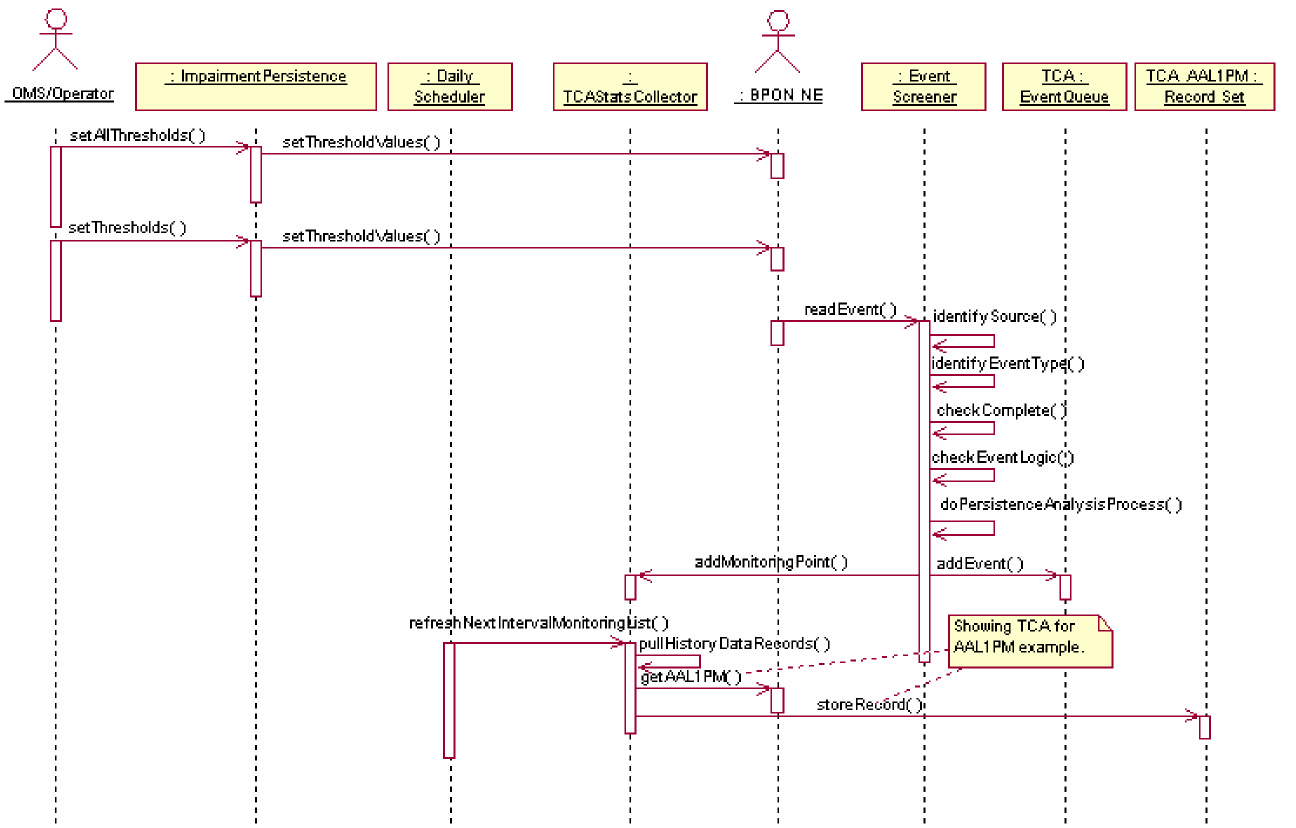


Figure 6-126 – Performance monitoring reporting (TCA triggered) sequence diagram – AAL1PM example

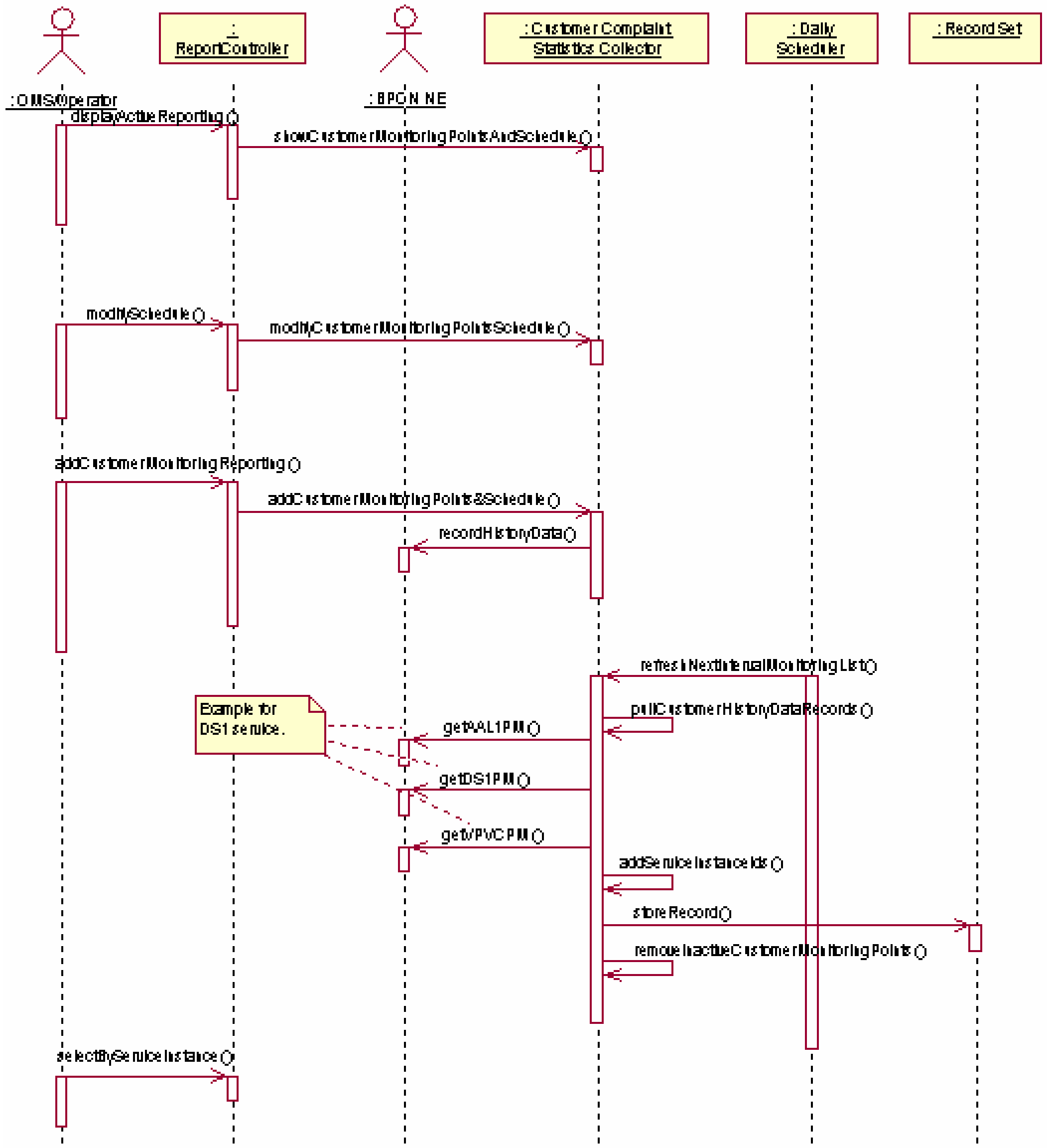

: OMS/Operator
: ReportController
: BPON NE
: Customer Complaint Statistics Collector
: Daily Scheduler
: Record Set
displayActiveReporting()
showCustomerMonitoringPointsAndSchedule()
modifySchedule()
modifyCustomerMonitoringPointsSchedule()
addCustomerMonitoringReporting()
addCustomerMonitoringPoints&Schedule()
recordHistoryData()
refreshNextIntervalMonitoringList()
pullCustomerHistoryDataRecords()
Example for DS1 service.
getAAL1PM()
getDS1PM()
getVPVCPM()
addServiceInstanceIds()
storeRecord()
removeInactiveCustomerMonitoringPoints()
selectByServiceInstance()

Figure 6-127 – Performance and traffic monitoring reporting (customer complaint) sequence diagram

Operations

Operation name	Operation purpose
1) addCustomerMonitoringReporting	This operation causes performance monitoring at specific monitoring point(s) in response to a customer complaint.
2) removeCustomerMonitoringReporting	This operation removes all performance monitoring statistics collection on behalf of a supplied service instance.
3) selectByServiceInstance	This operation retrieves all the performance monitoring statistics available in the supplier management system associated with a given service instance Id.
4) displayActiveReporting	This operation retrieves all the monitoring points for which performance monitoring statistics are currently being collected for a given service instance Id.
5) addNewMonitoringReporting	This operation causes performance monitoring at specific monitoring point(s).
6) selectByMonitoringPoint	This operation gets all the performance statistic records available in the supplier management system associated with the given monitoring point.
7) createReportingSchedule	This operation adds a scheduled collection of performance monitoring statistics for a specific monitoring point.
8) modifyReportingSchedule	This operation modifies the scheduled collection of performance monitoring statistics for a specific monitoring point.
9) cancelReportingSchedule	This operation cancels subsequent scheduled collection of performance monitoring statistics where the scheduled reporting was requested by the operator previously.

Figure 6-128 – Report controller operations

Operation signatures

Operation name	Input parameters	Return value	Exceptions
1) addCustomerMonitoring Reporting	ManagedEntityIdType (NE), ServiceInstanceIdType, ManagedEntityIdType (monitoring point), GeneralizedTimeType (stop time), HistoryDataType, short (granularity period)	void	UnknownServiceInstance, AccessDenied, UnknownNE, UnknownManagedEntity, CollectionPeriodPast, CollectionLimitation, InvalidAssociation, UnknownHistoryDataType, CommFailure
2) removeCustomerMonitoring Reporting	ServiceInstanceIdType	void	UnknownServiceInstance, AccessDenied, CollectionPeriodPast, CommFailure
3) selectByServiceInstance	ServiceInstanceIdType, GeneralizedTimeType (start time), GeneralizedTimeType (stop time),	RecordsSeqType	UnknownServiceInstance, AccessDenied
4) displayActiveReporting	ServiceInstanceIdType	MonitoringPoint SeqType	UnknownServiceInstance, AccessDenied
5) addNewMonitoringReporting	ManagedEntityIdType (NE), ManagedEntityIdType (monitoring point), GeneralizedTimeType (stop time), HistoryDataType, short (granularity period)	void	AccessDenied, UnknownNE, UnknownManagedEntity, CollectionPeriodPast, CollectionLimitation, InvalidAssociation, UnknownHistoryDataType, CommFailure
6) selectByMonitoringPoint	ManagedEntityIdType (monitoring point), GeneralizedTimeType (start time), GeneralizedTimeType (stop time)	RecordsSeqType	UnknownManagedEntity, AccessDenied
7) createReportingSchedule	ManagedEntityIdType (NE), ManagedEntityIdType (monitoring point), HistoryDataType, ServiceInstanceIdType, short (granularity period), UserLabelType (scheduler name)	void	AccessDenied, UnknownNE, UnknownManagedEntity, CollectionLimitation, UnknownScheduler, InvalidAssociation, UnknownHistoryDataType, InvalidScheduler
8) modifyReportingSchedule	ManagedEntityIdType (NE), ManagedEntityIdType (monitoring point), HistoryDataType, ServiceInstanceIdType, UserLabelType (scheduler name)	void	AccessDenied, UnknownNE, UnknownManagedEntity, CollectionLimitation, UnknownScheduler, InvalidAssociation, UnknownHistoryDataType, InvalidScheduler
9) cancelReportingSchedule	ManagedEntityIdType (NE), ManagedEntityIdType (monitoring point), HistoryDataType, ServiceInstanceIdType, UserLabelType (scheduler name)	void	AccessDenied, UnknownNE, UnknownManagedEntity, UnknownScheduler, InvalidAssociation, UnknownHistoryDataType

Figure 6-129 – Report controller signatures

Exceptions

Exception raised	Description
AccessDenied	System is not granted access to this interface object.
CollectionLimitation	The supplier management system cannot collect data for the given time duration and granularity period due to implementation restrictions.
CollectionPeriodPast	When the period end-time is less than or equal to the current time.
CommFailure	There was a DCN link failure between the NE and the supplier management system.
InvalidAssociation	The given profile cannot be applied to a monitoring point.
InvalidScheduler	The Scheduler parameters values are outside defined scope.
UnknownHistoryDataType	The history data type is unknown in the supplier management system.
UnknownManagedEntity	The specified managed entity is unknown to the supplier management system.
UnknownNE	The identified NE is unknown to the supplier management system.
UnknownScheduler	The named scheduler is unknown to the supplier management system.
UnknownServiceInstance	The service instance is unknown to the supplier management system.

Figure 6-130 – Report controller exceptions

Appendix I

Additional UML diagrams

(This appendix does not form an integral part of this Recommendation)

The following class and sequence diagrams are provided as non-normative information with the intention of completing a description of the behaviour within the supplier management system associated with use cases of clause 6 not directly involving the interface shown in Figure 6-1.

I.1 Process incoming NE events and log event records

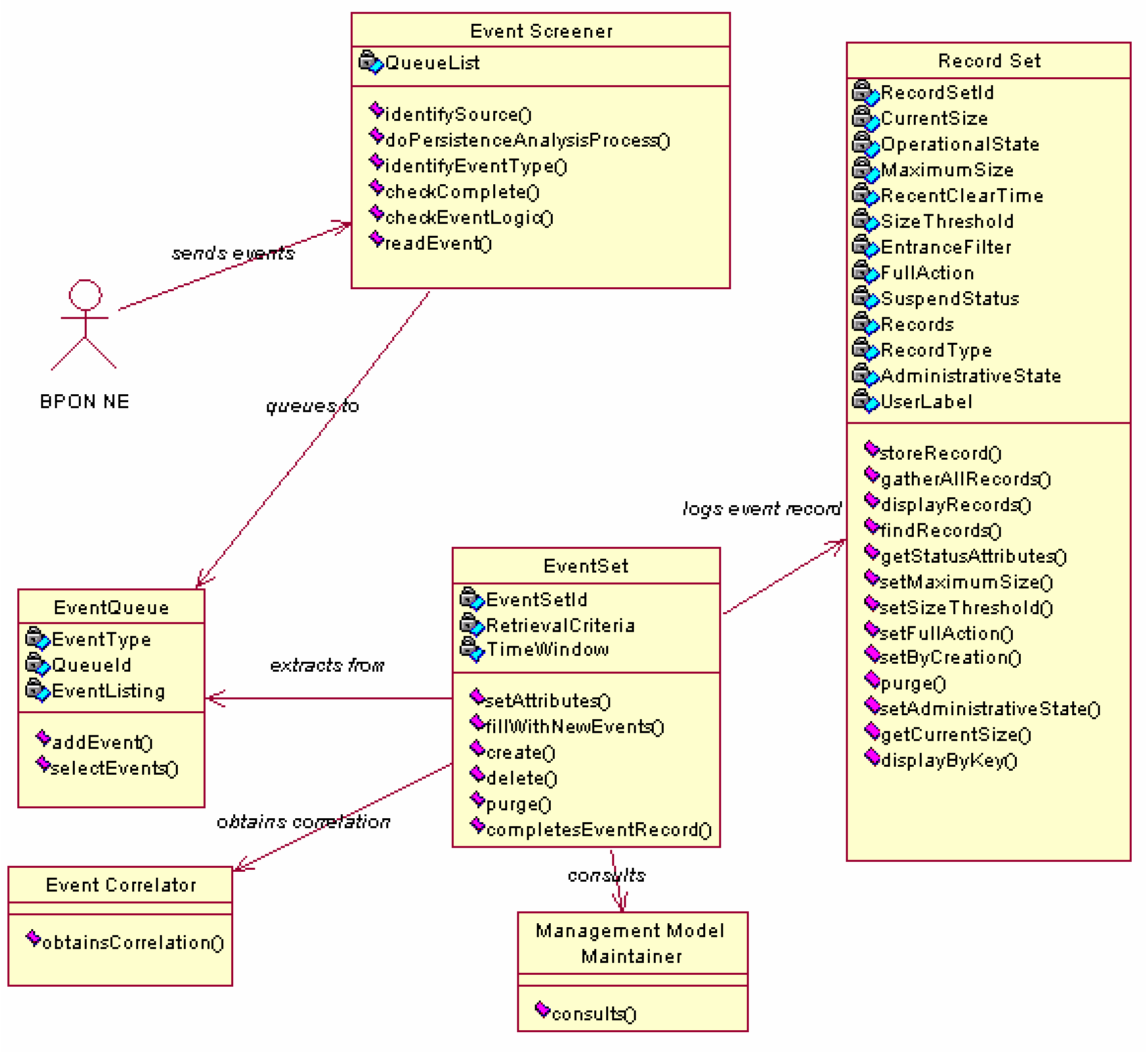


Figure I.1 – Incoming event class diagram

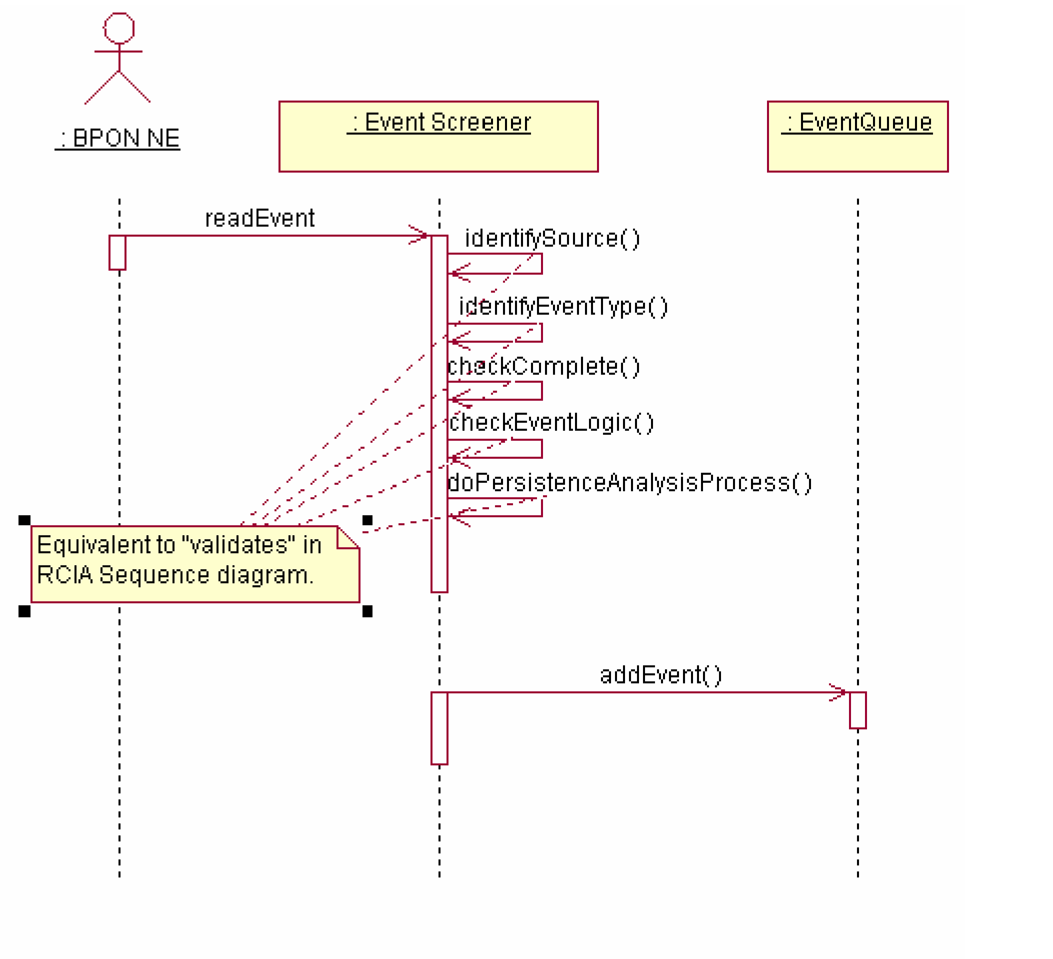


Figure I.2 – Process incoming event sequence diagram

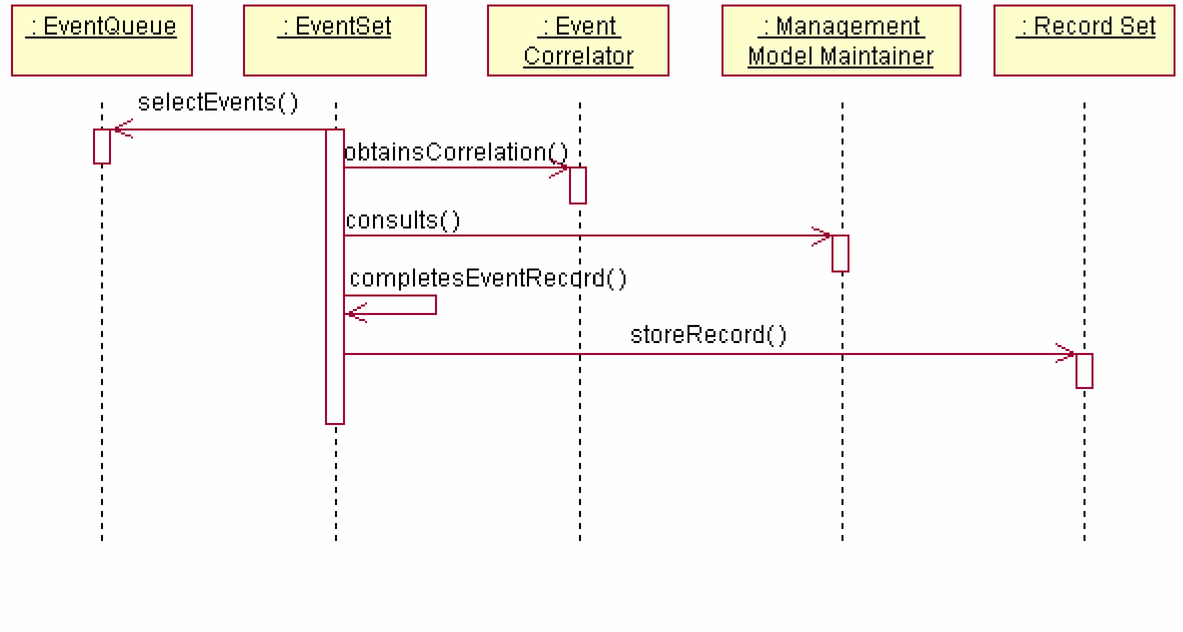


Figure I.3 – Log event sequence diagram

I.2 Root cause alarm analysis

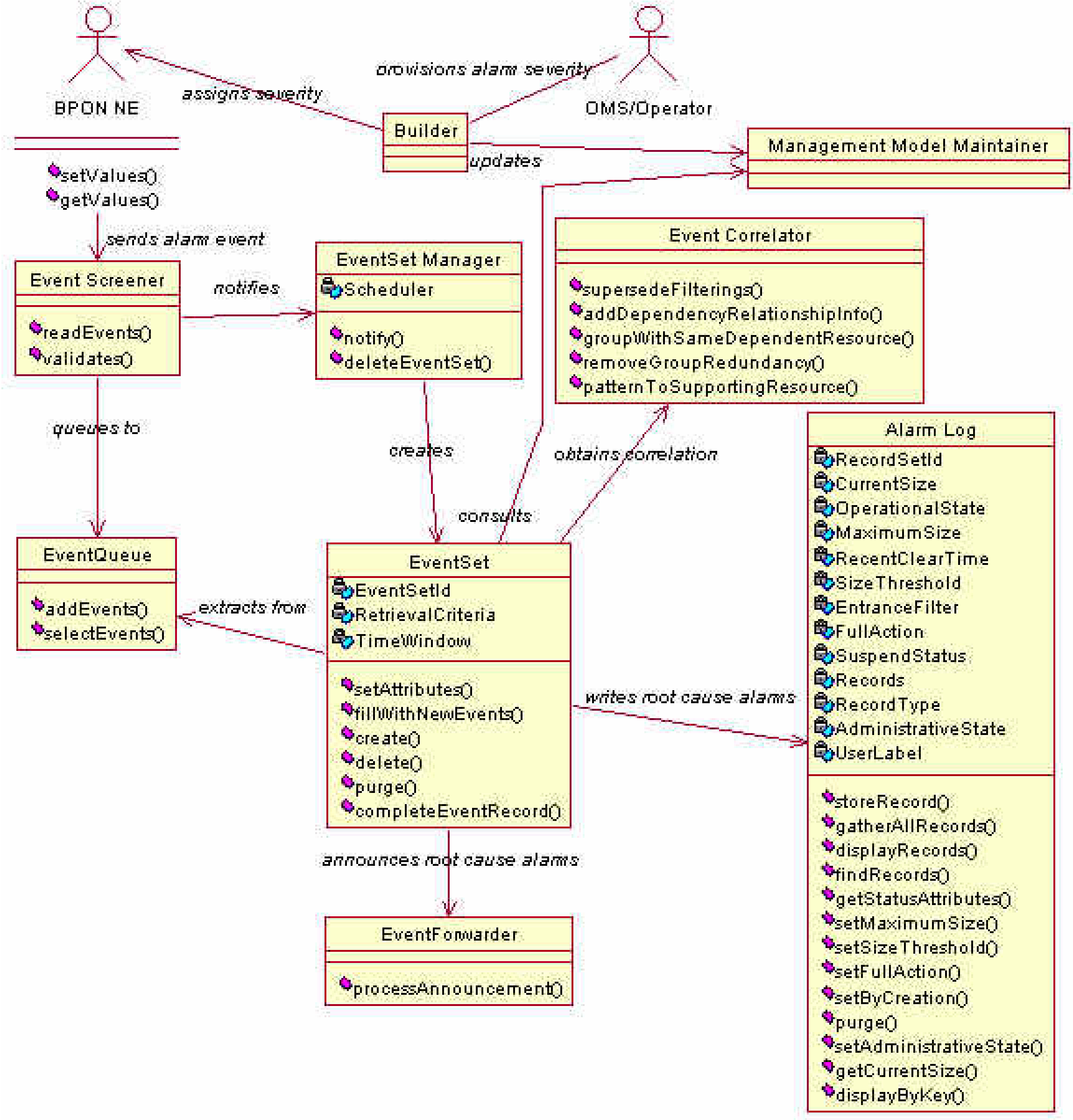


Figure I.4 – Root cause alarm analysis class diagram

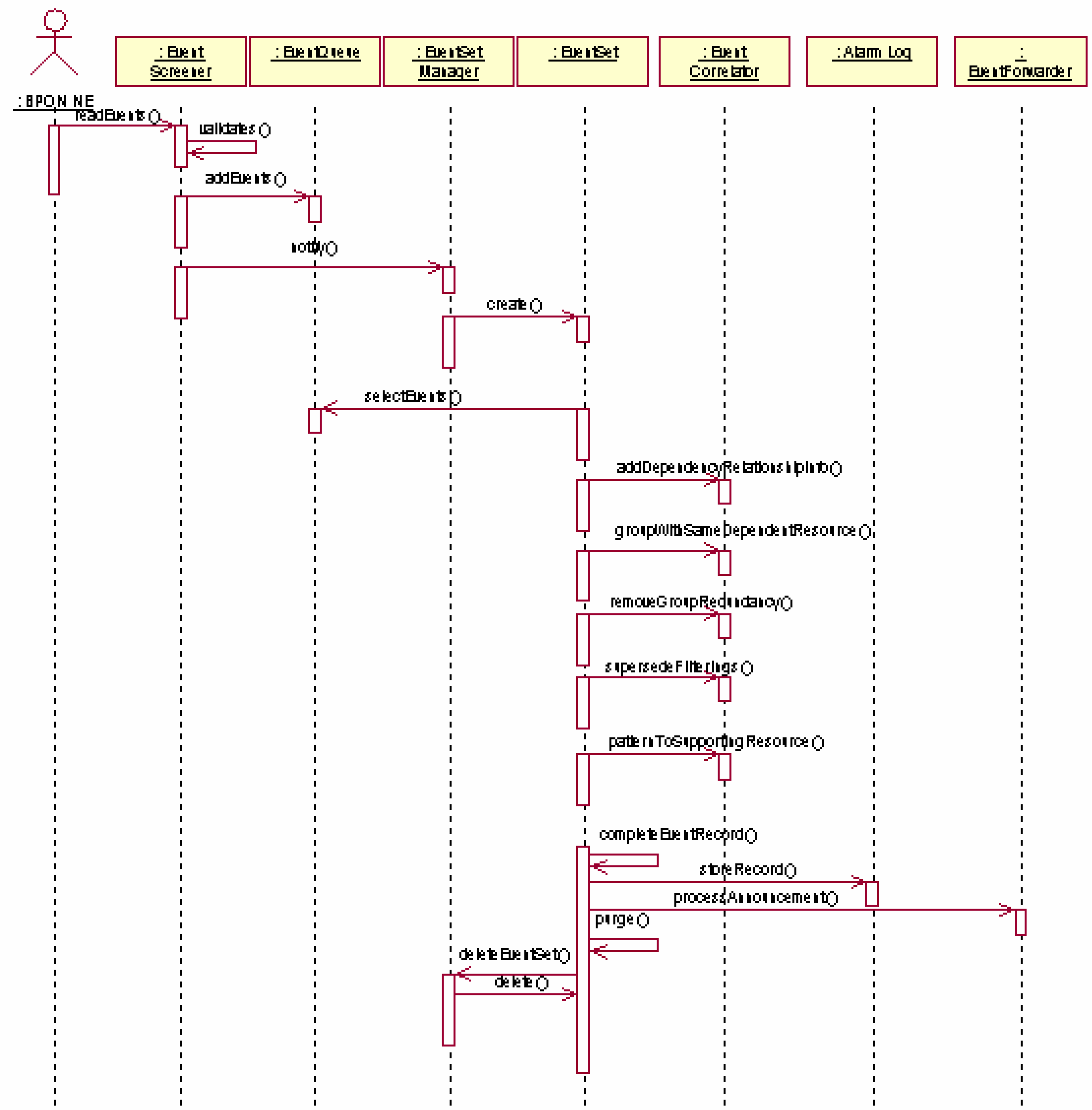


Figure I.5 – Root cause alarm analysis sequence diagram

I.3 Autodiscover NEs and plug-in units

Figure I.6 provides a detailed view of the classes involved in supplier management system autodiscovery. Figures I.7 and I.8 present high-level views of two different ways that the supplier management system could support autodiscovery when a new OLT is registered with the supplier management system. The actual implementation might combine both views. In any case, the supplier management system uses a synchronization function to prepare up-to-date event information for publication to interested client applications through an external event channel. Figure I.9 shows a sequence diagram concerning equipment removal.

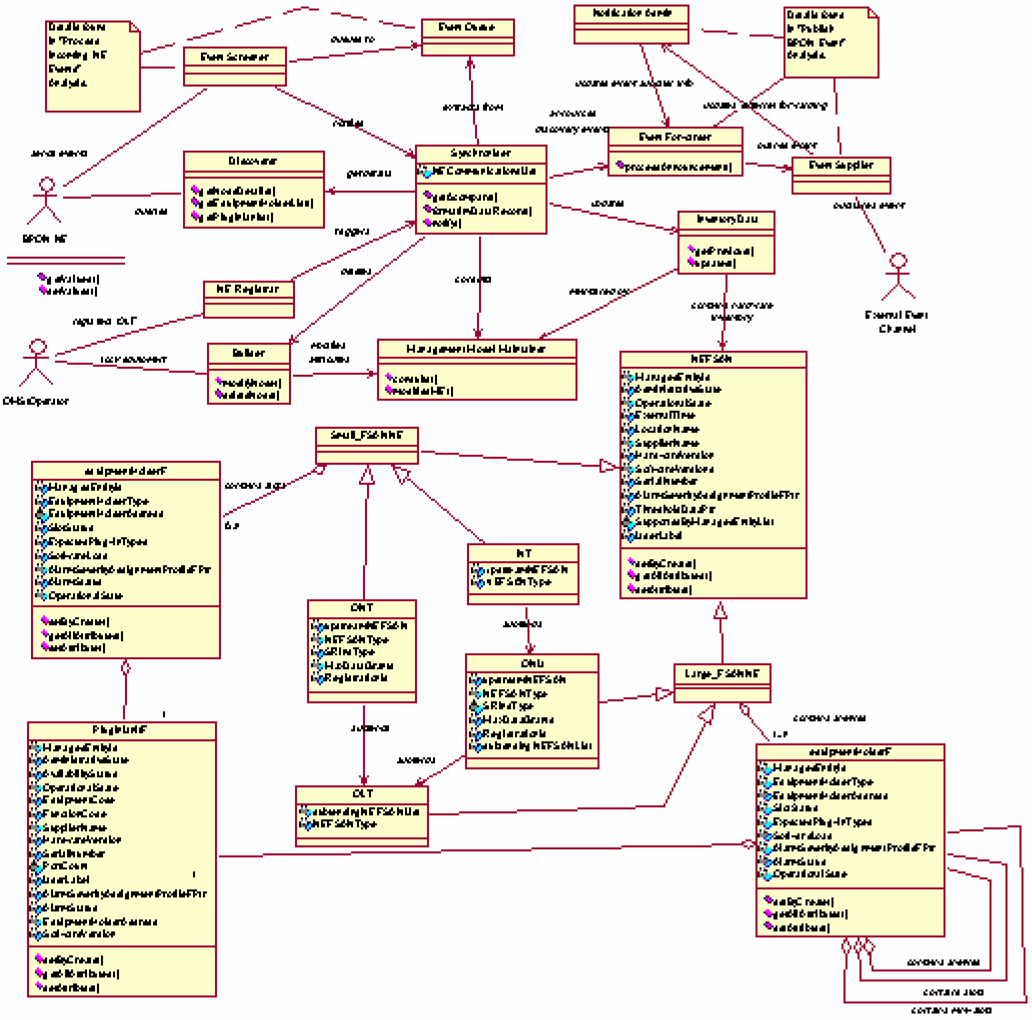


Figure I.6 – Autodiscover NEs and plug-in units class diagram

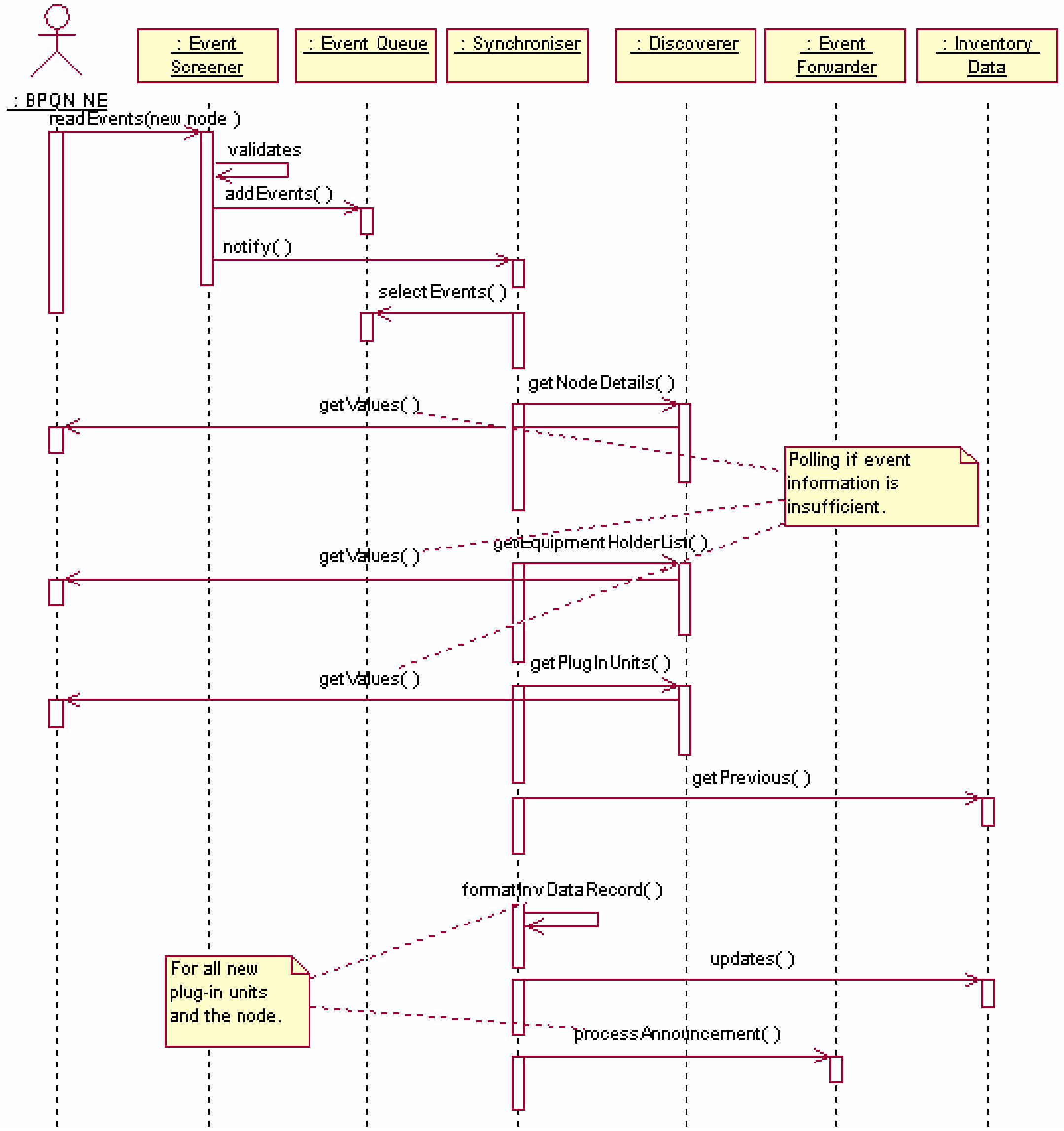


Figure I.7 – New NE event sequence diagram

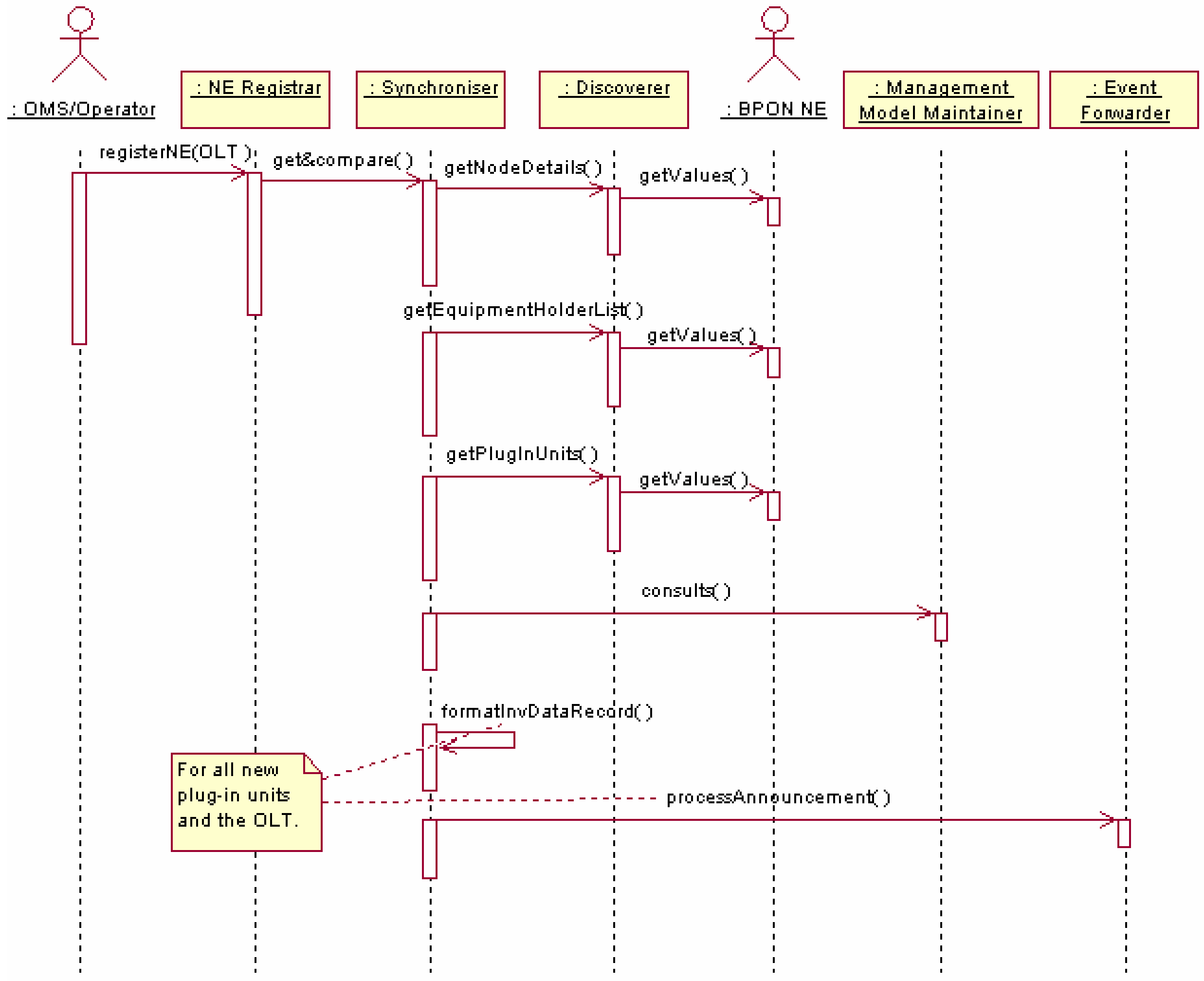


Figure I.8 – Register OLT and autodiscovery sequence diagram

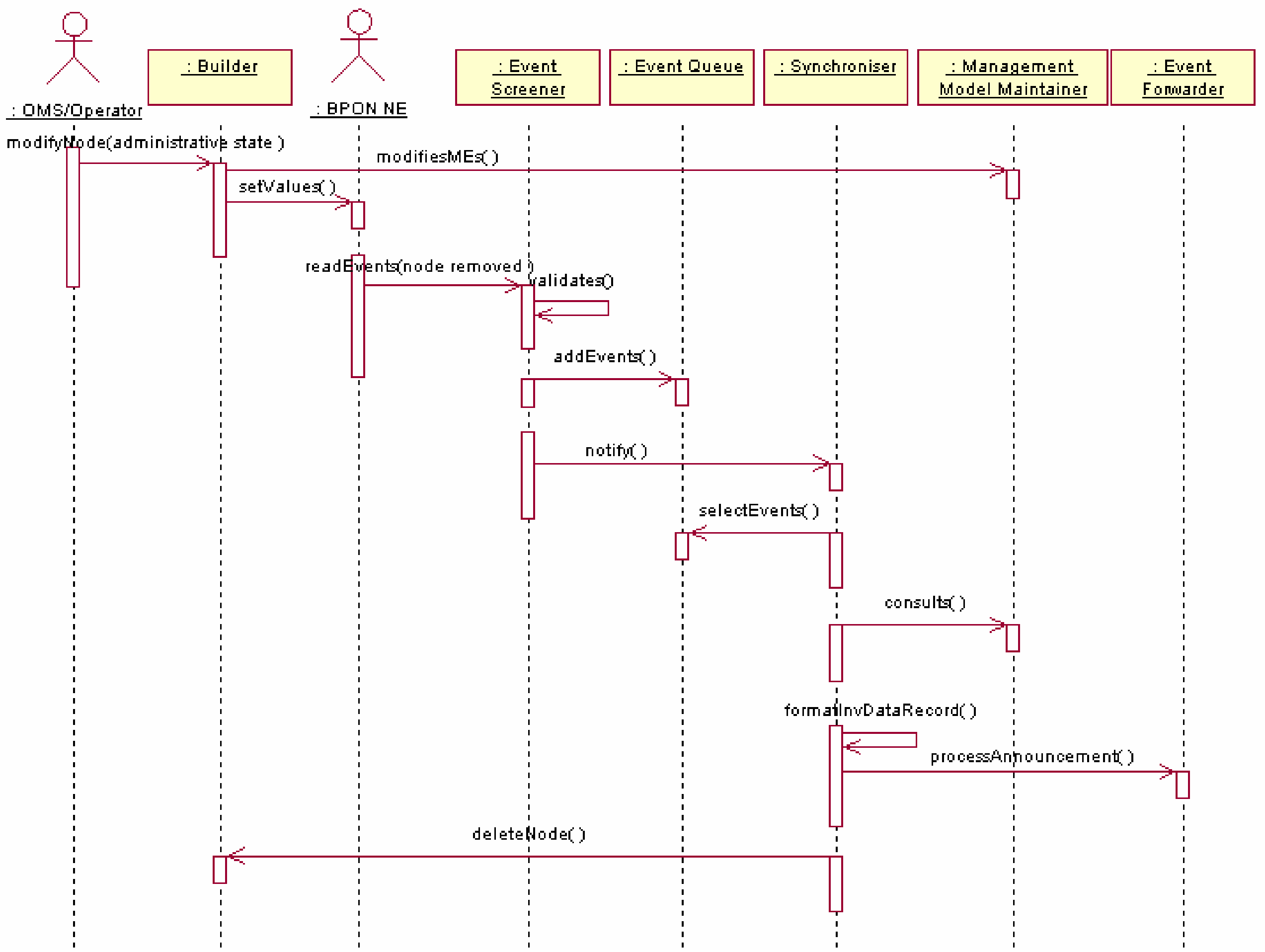


Figure I.9 – Equipment removal sequence diagram

I.4 Collect history data

Figure I.10 provides the class diagram associated with history data collection triggered by routine needs for performance monitoring as well as by customer complaint or detection of threshold crossing alerts for a monitored performance parameter. Figure I.11 provides a sequence diagram that shows separate processes for history data collection triggered by customer complaint and history data collection triggered by all other mechanisms.

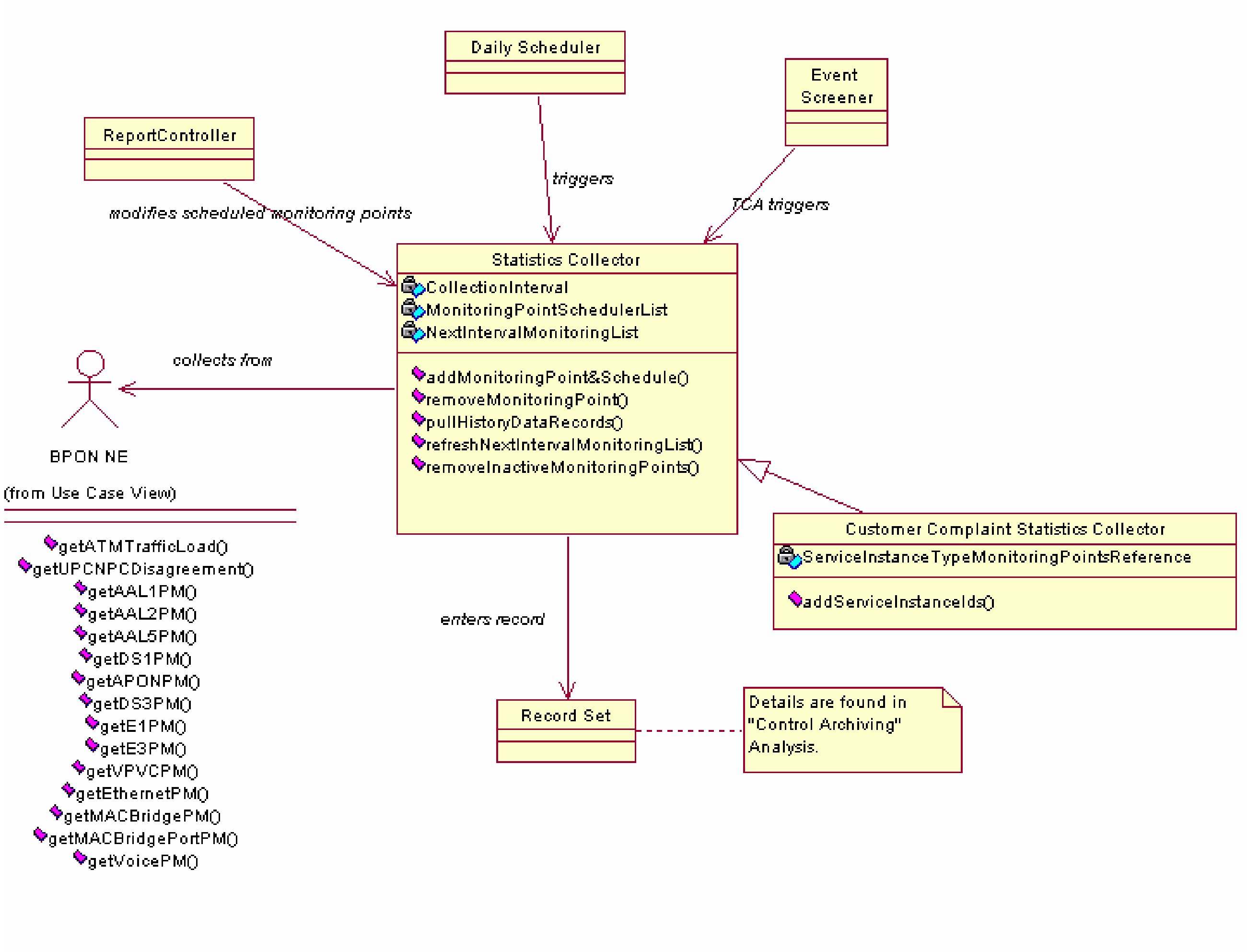


Figure I.10 – Collect history data class diagram

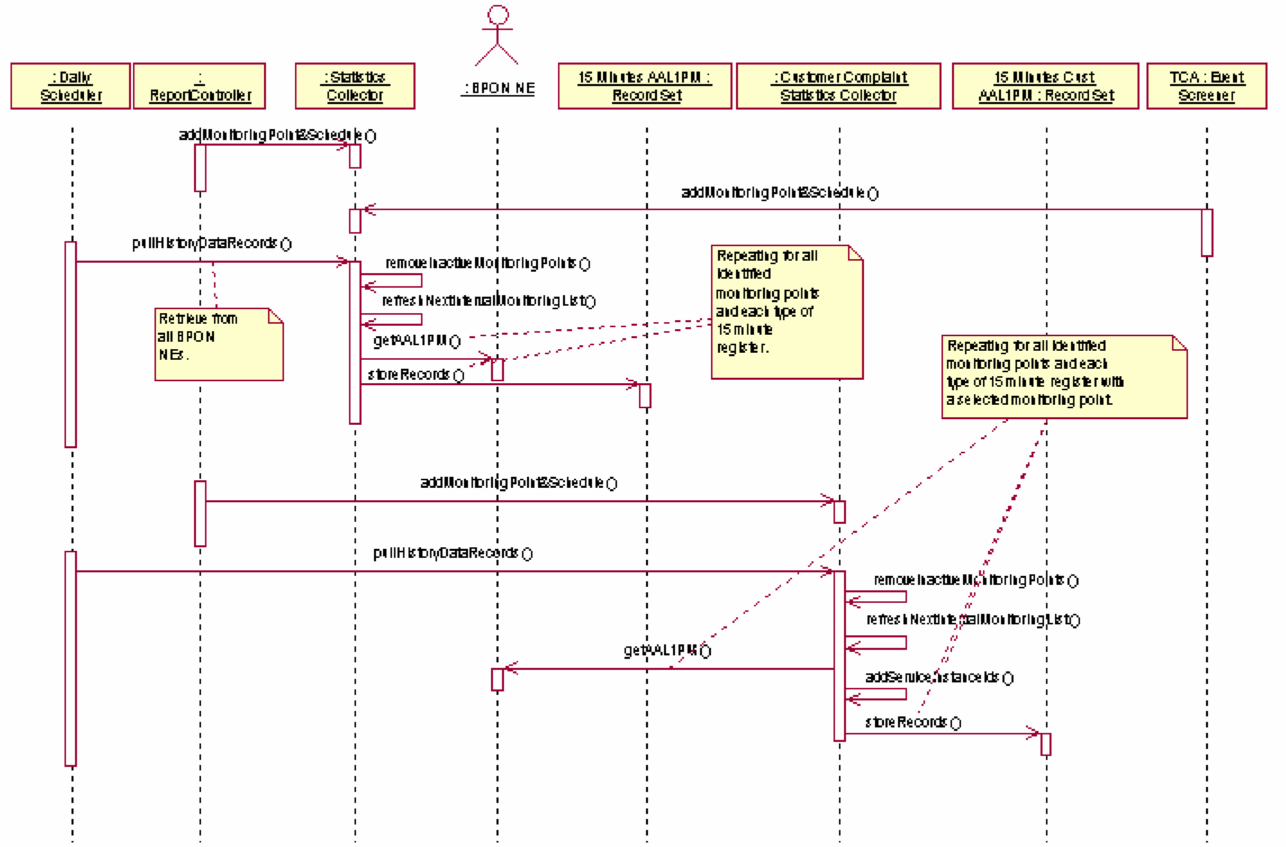

: Daily Scheduler
: ReportController
: Statistics Collector
: BPON NE
15 Minutes AAL1PM : Record Set
: Customer Complaint Statistics Collector
15 Minutes Cust AAL1PM : Record Set
TCA : Event Screener
addMonitoringPoint2Schedule()
addMonitoringPoint2Schedule()
pullHistoryDataRecords()
removeInactiveMonitoringPoints()
refreshNextInternalMonitoringList()
getAAL1PM()
storeRecords()
Retrieve from all BPON NEs.
Repeating for all identified monitoring points and each type of 15 minute register.
Repeating for all identified monitoring points and each type of 15 minute register with a selected monitoring point.
addMonitoringPoint2Schedule()
pullHistoryDataRecords()
removeInactiveMonitoringPoints()
refreshNextInternalMonitoringList()
getAAL1PM()
addServiceInstanceIds()
storeRecords()

Figure I.11 – Collect history data sequence diagram

Appendix II

High level summary class diagrams

(This appendix does not form an integral part of this Recommendation)

The following class diagrams are provided as non-normative information with the intention of completing a description of the behaviour within the supplier management system. Object classes, actors and associations are identified for the use case diagrams of clause 6.2.1.3 where more than one use case is present. The purpose of providing this information is to show how use cases within the supplier management system addressing similar management functionality might employ the same internal object classes. Since these diagrams show primarily internal associations, the diagrams are for information only.

II.1 Event handling

The following simplified class diagram, Figure II.1, shows interactions between external actors and classes internal to the supplier management system when events are processed in the supplier management system. This diagram serves to consolidate and provide consistency to diagrams found within clause 6.3.2. The analysis for the interactions called "provisions service", and "selects records" and "views" involving the actor called "OMS/Operator" in Figure II.1 are found in clauses 6.3.5 and 6.3.6, respectively.

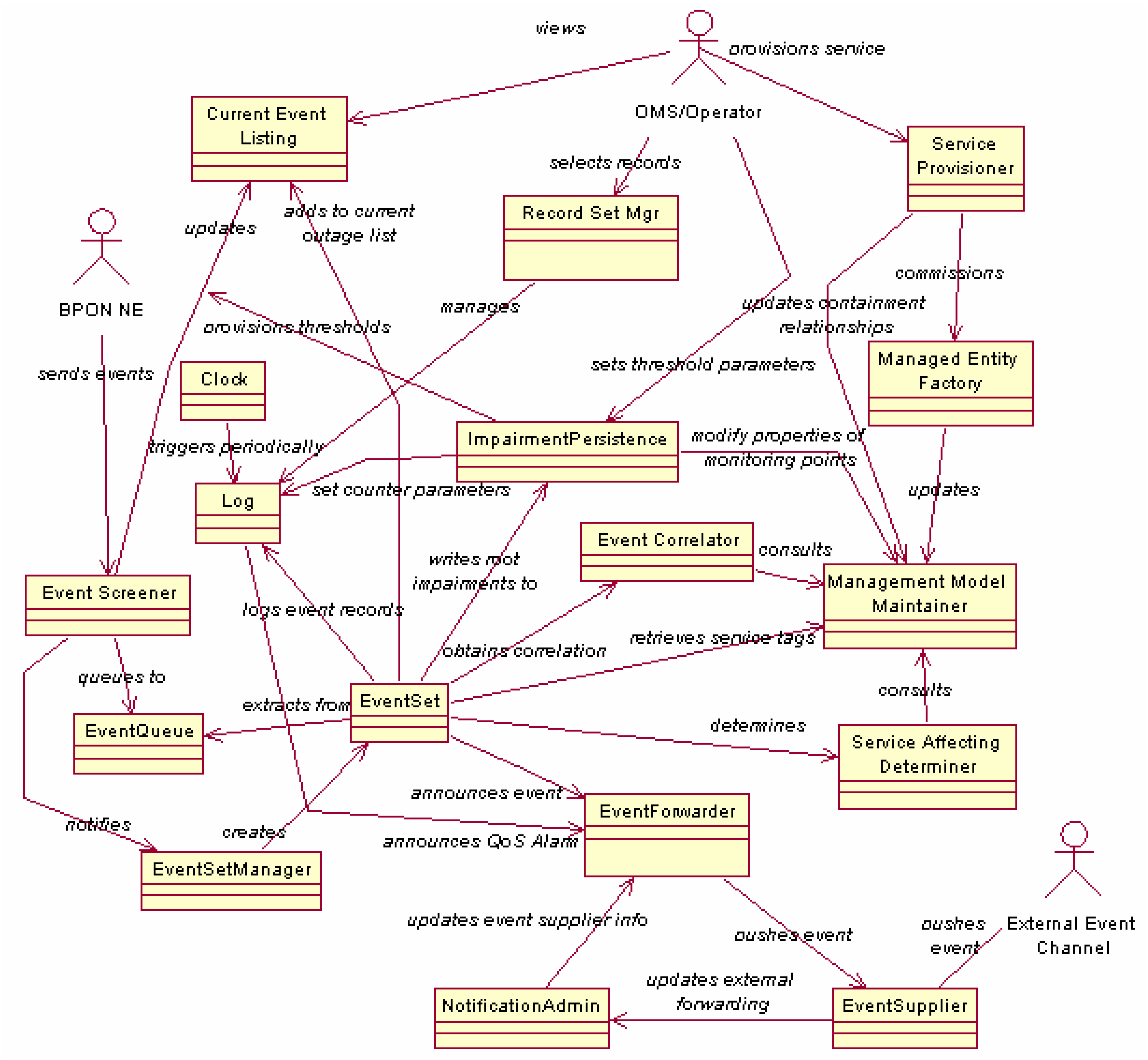


Figure II.1 – High-level event handling class diagram

II.2 Software and configuration data management

The following simplified class diagram show interactions between external actors and classes internal to the supplier management system when software and NE configuration data is managed with the supplier management system. This diagram serves to consolidate and provide consistency to the subsequent diagrams found within clause 6.3.3.

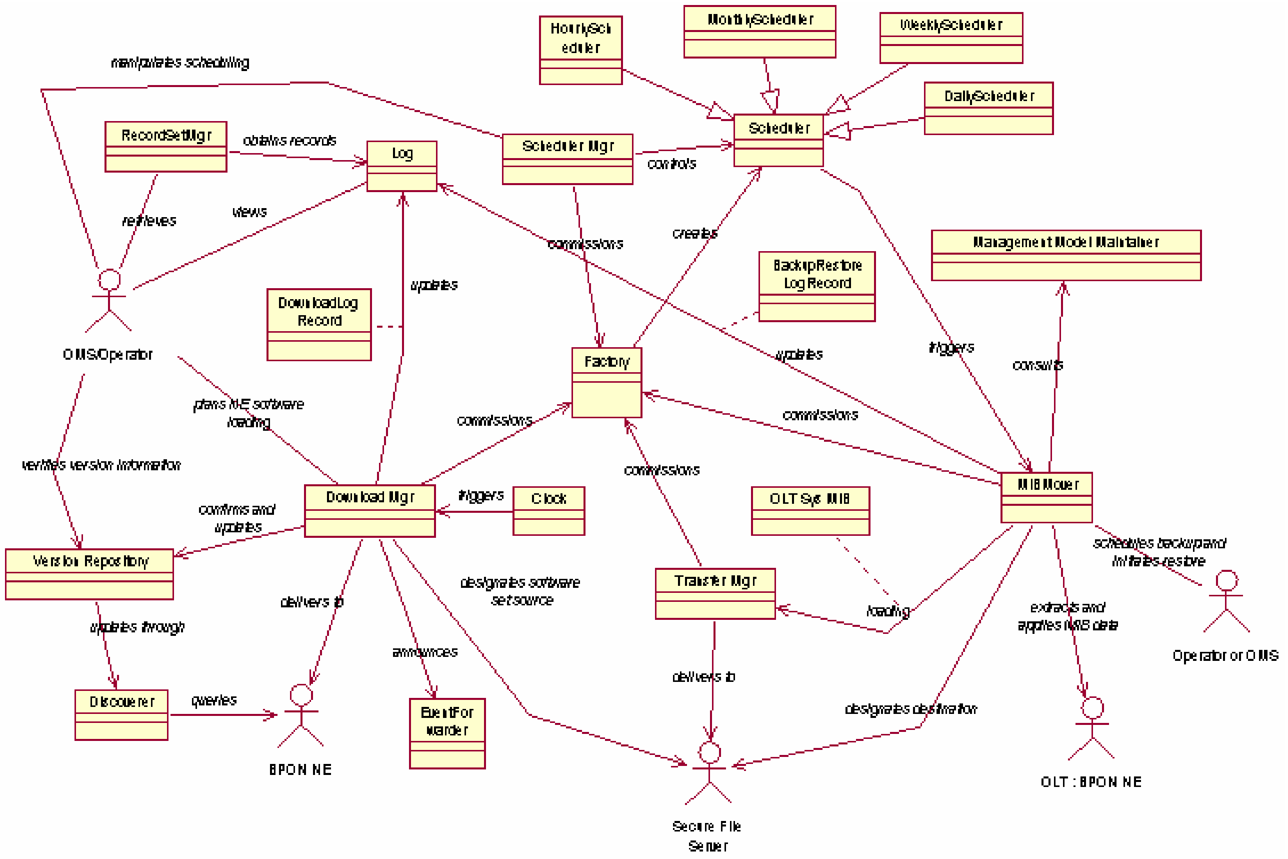


Figure II.2 – High-level software and configuration data class diagram

II.3 Installation

The following simplified class diagram show interactions between external actors and classes internal to the supplier management system when BPON equipment is being installed. This diagram serves to consolidate and provide consistency to the subsequent diagrams found within clause 6.3.5.

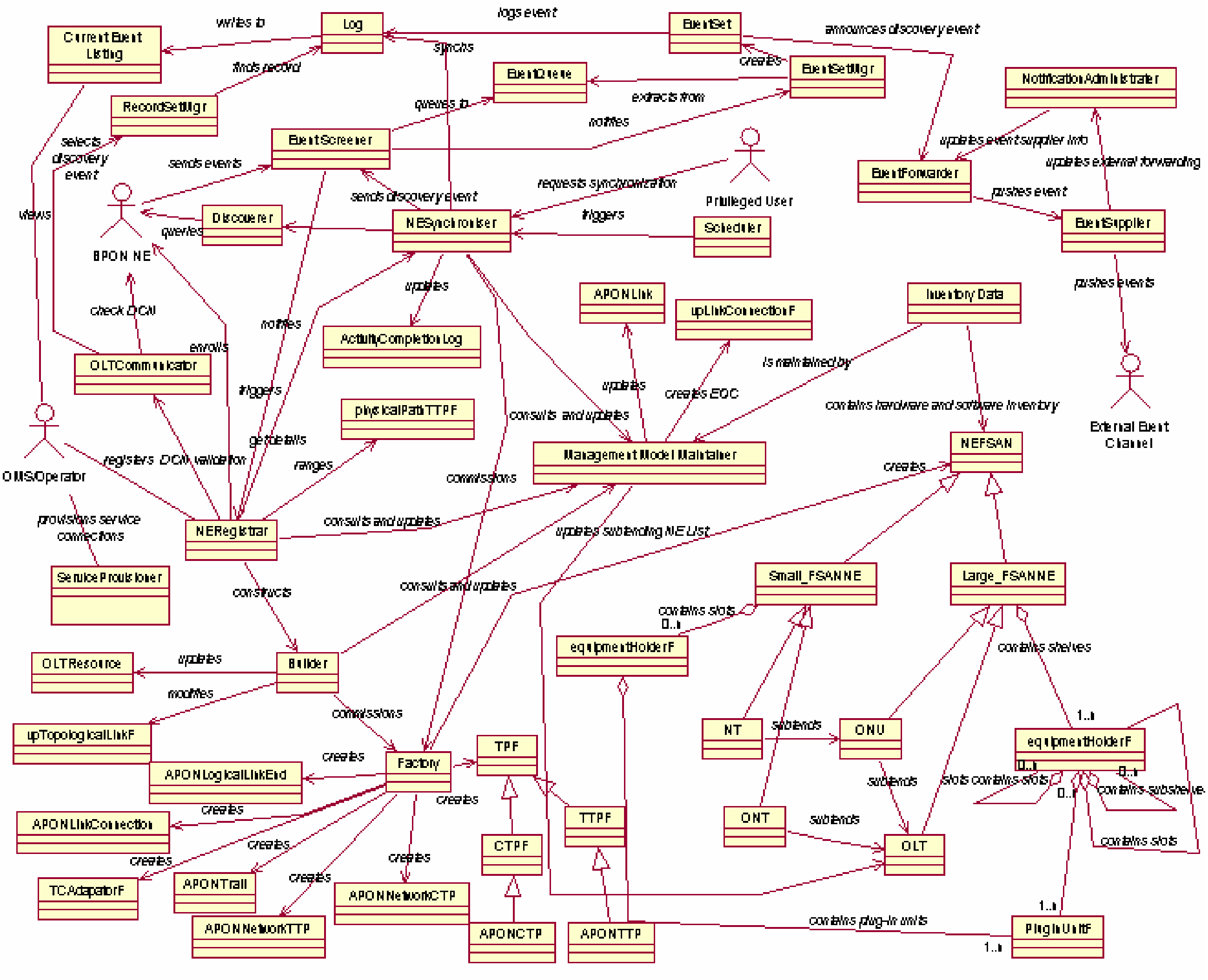


Figure II.3 – Installation class diagram

II.4 Provisioning

Figure II.4 shows interactions between external actors and classes internal to the supplier management system when BPON equipment and services are being provisioned. This diagram serves to consolidate and provide consistency to the subsequent diagrams found within clause 6.3.6.

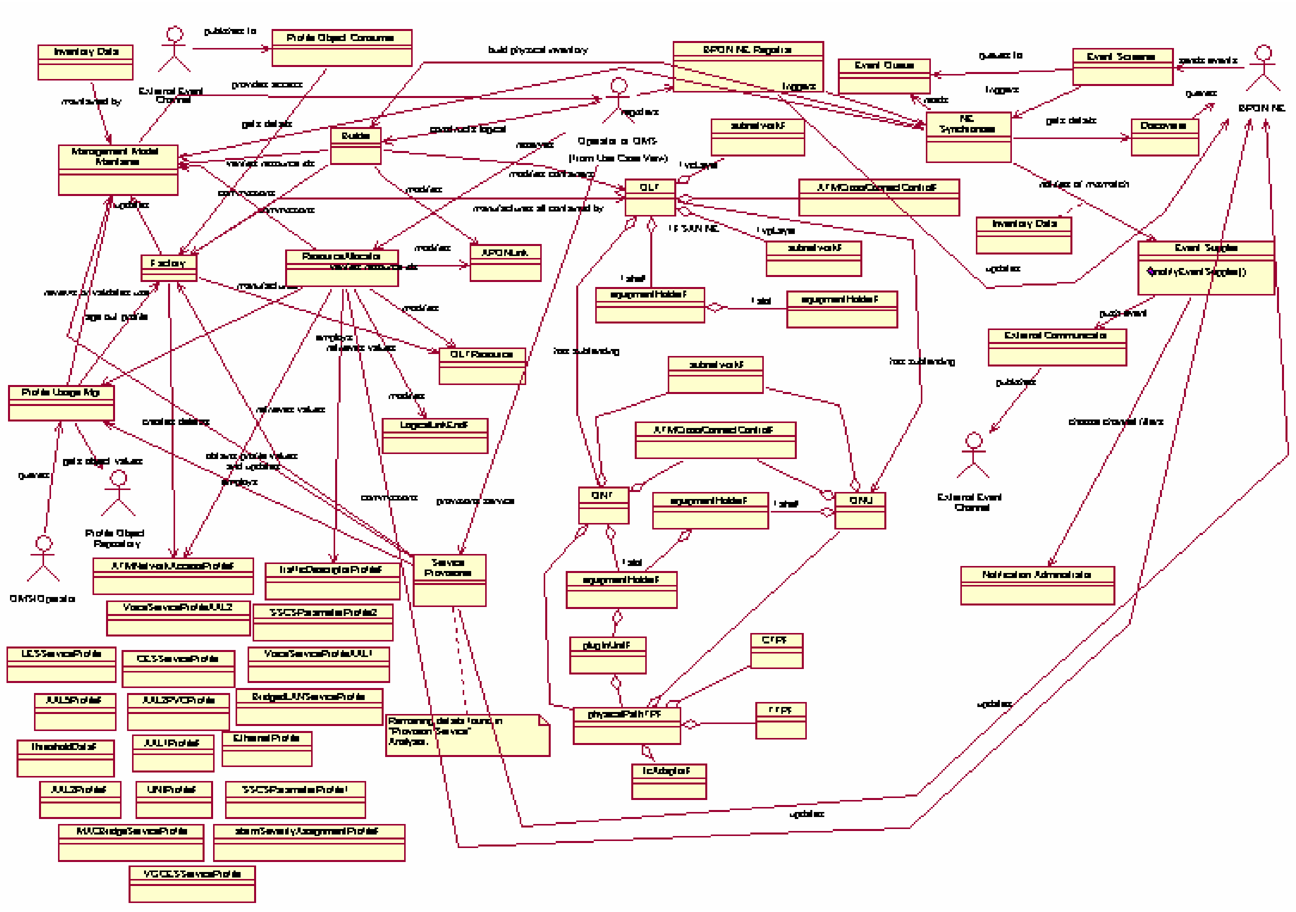


Figure II.4 – Provisioning class diagram

II.5 Archiving and bulk transfer

Figure II.5 shows interactions between external actors and classes internal to the supplier management system when statistics are archived for short periods of time in the supplier management system and eventually transferred, via a file transfer protocol, to long-term archives within an operator data warehouse. This diagram serves to consolidate and provide consistency to the subsequent diagrams found within clause 6.3.7.

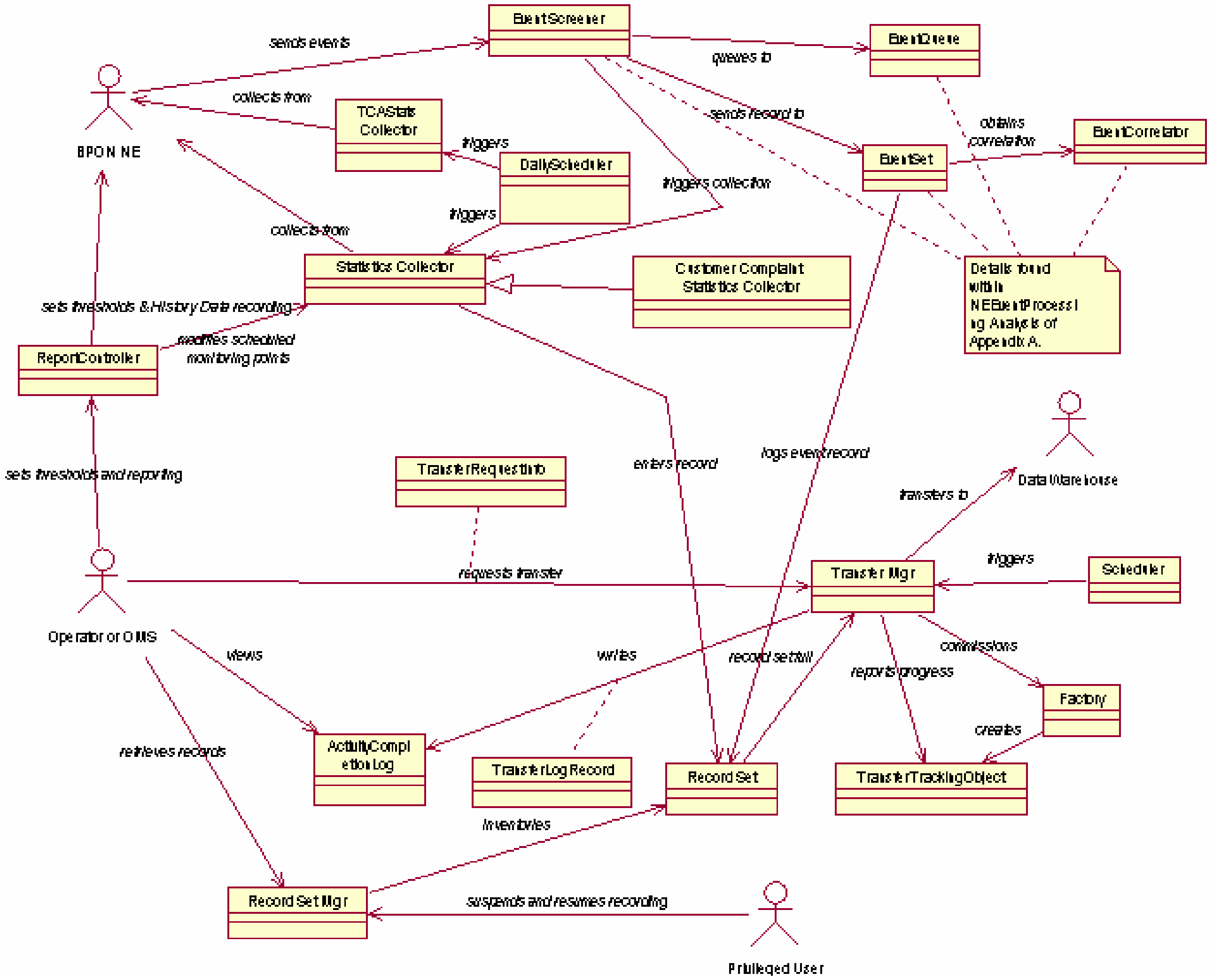


Figure II.5 – Archiving and bulk transfer class diagram

Bibliography

[b-OMG 99-06-01] OMG Document formal/99-06-01, *OMG Modeling Book* (section 1).

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	Telephone transmission quality, telephone installations, local line networks
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, 2008