ETSI TS 104 043 V11.0.0 (2024-06)

Publicly Available Specification (PAS); O-RAN Operations and Maintenance Interface Specification (O-RAN.WG10.O1-Interface-R003-v11.00)

CAUTION

The present document has been submitted to ETSI as a PAS produced by O-RAN Alliance and approved by the ETSI Technical Committee Mobile Standards Group (MSG).

Reference
DTS/MSG-001152

Keywords
interface, maintenance, PAS

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Mobile Standards Group (MSG).

The content of the present document is subject to continuing work within O-RAN and may change following formal O-RAN approval. Should the O-RAN Alliance modify the contents of the present document, it will be re-released by O-RAN with an identifying change of version date and an increase in version number as follows:

version xx.yy.zz

where:

- xx: the first digit-group is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc. (the initial approved document will have xx=01). Always 2 digits with leading zero if needed.
- yy: the second digit-group is incremented when editorial only changes have been incorporated in the document. Always 2 digits with leading zero if needed.
- zz: the third digit-group included only in working versions of the document indicating incremental changes during the editing process. External versions never include the third digit-group. Always 2 digits with leading zero if needed.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

The O-RAN O1 management services follow existing 3GPP standards wherever possible. The focus of the present document is to identify the use cases which conform to existing 3GPP standards, identify gaps in management services for O-RAN and define needed extensions. For identified gaps, the goal is to modify the 3GPP standards to include the needed O-RAN extensions and update the references in the present document as the 3GPP standards evolve to cover the gaps. In cases where the 3GPP standards are not modified, O-RAN extensions are specified in this, and other, O-RAN documents. O-RAN extensions are compatible with 3GPP standards as much as possible to avoid divergence. If extensions and gaps are not specified, it is expected that the management services providers and consumers are conforming to referenced 3GPP specifications.

This O1 Interface Specification specifies the management services (MnS) supported in the O-RAN architecture between O1 compliant Managed Elements (MnS providers) and the SMO (MnS consumer). It defines common MnS descriptions, requirements, procedures, operations, and notifications. In addition, there are complementary O1 Interface Specifications for the Near-RT RIC [i.10], the O-CU-UP and O-CU-CP [i.11] and the O-DU [i.12] that define the O1 specificities, extensions, and restrictions for that particular managed function (MF). O-RAN end-to-end OAM use cases and OAM architectural principles are specified in O-RAN TS O-RAN Operations and Maintenance Architecture [i.13].

For example:

- O1 Interface Specification for a MF may contain the alarms and performance measurements generated by that MF;
- O1 Interface Specification for O-DU may include extensions needed by O-DU for managing O-RU in hierarchical mode;
- O1 Interface Specification for Near-RT RIC may document the O1 MnS services that it does not provide and may reference a related specification containing procedures and APIs for managing xApps.

1 Scope

The present document defines O-RAN OAM interface functions and protocols for the O-RAN O1 interface. The present document studies the functions conveyed over the interface, including management functions, procedures, operations, and corresponding solutions, and identifies existing standards and industry work that can serve as a basis for O-RAN work.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference/.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

[1] ETSI TS 128 314 (V17.0.0): "5G; Management and orchestration; Plug and Connect; Concepts and requirements (3GPP TS 28.314 version 17.0.0 Release 17)".

[2] ETSI TS 128 315 (V17.0.0): "5G; Management and orchestration; Plug and Connect; Procedure flows (3GPP TS 28.315 version 17.0.0 Release 17)".

[3] ETSI TS 128 532 (V17.3.0): "5G; Management and orchestration; Generic management services (3GPP TS 28.532 version 17.3.0 Release 17)".

[4] ETSI TS 128 537 (V17.2.0): "5G; Management and orchestration; Management capabilities (3GPP TS 28.537 version 17.2.0 Release 17)".

[5] ETSI TS 128 545 (V17.0.0): "5G; Management and orchestration; Fault Supervision (FS) (3GPP TS 28.545 version 17.0.0 Release 17)".

[6] ETSI TS 128 550 (V17.1.0): "5G; Management and orchestration; Performance assurance (3GPP TS 28.550 version 17.1.0 Release 17)".

[7] ETSI TS 128 622 (V17.1.1): "Universal Mobile Telecommunications System (UMTS); LTE; 5G; Telecommunication management; Generic Network Resource Model (NRM) Integration Reference Point (IRP); Information Service (IS) (3GPP TS 28.622 version 17.1.1 Release 17)".

[8] ETSI TS 132 341 (V17.0.0): " Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; Telecommunication management; File Transfer (FT) Integration Reference Point (IRP); Requirements (3GPP TS 32.341 version 17.0.0 Release 17)".

[9] ETSI TS 132 342 (V17.0.0): "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; Telecommunication management; File Transfer (FT) Integration Reference Point (IRP); Information Service (IS) (3GPP TS 32.342 version 17.0.0 Release 17)".

[10] ETSI TS 132 404 (V17.0.0): "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; Telecommunication management; Performance Management (PM); Performance measurements; Definitions and template (3GPP TS 32.404 version 17.0.0 Release 17)".

[11] 3GPP TS 32.421 (V17.2.0): "Telecommunication management; Subscriber and equipment trace; Trace concepts and requirements".

[12] 3GPP TS 32.422 (V17.4.0): "Telecommunication management; Subscriber and equipment trace; Trace control and configuration management".

[13] 3GPP TS 32.423 (V17.2.0): "Telecommunication management; Subscriber and equipment trace; Trace data definition and management".

[14] ETSI TS 132 432 (V17.0.0): "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; Telecommunication management; Performance measurement: File format definition (3GPP TS 32.432 version 17.0.0 Release 17)".

[15] O-RAN TS O-RAN.WG1.OAD: "O-RAN Architecture Description".

[16] O-RAN TS O-RAN.WG11.Security-Protocols-Specification: "O-RAN Security Protocols Specifications".

[17] O-RAN TS O-RAN.WG11.Security-Requirements-Specifacation: "O-RAN Security Requirements and Controls Specification".

[18] ONAP - Service: VES Event Listener Specification V7.2.1, January 16, 2021.

[19] IETF RFC 6022 (October 2010): "YANG Module for NETCONF Monitoring".

[20] IETF RFC 6241 (June 2011): "Network Configuration Protocol (NETCONF)".

[21] IETF RFC 7950 (August 2016): "The YANG 1.1 Data Modeling Language".

[22] IETF RFC 7951 (August 2016): "JSON Encoding of Data Modeled with YANG".

[23] ETSI TS 128 623 (V17.2.2): " Universal Mobile Telecommunications System(UMTS); LTE; 5G; Telecommunication management; Generic Network Resource Model (NRM) Integration Reference Point (IRP); Solution Set (SS) definitions (3GPP TS 28.623 version 17.2.2 Release 17)".

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, O-RAN cannot guarantee their long-term validity.

The following referenced documents are not necessary for the application of the present document, but they assist the user with regard to a particular subject area.

[i.1] 3GPP TR 21.905 (V17.0.0): Vocabulary for 3GPP Specifications".

[i.2] ETSI TS 128 316 (V17.0.0): "5G; Management and orchestration; Plug and Connect; Data formats (3GPP TS 28.316 version 17.0.0 Release 17)".

[i.3] 3GPP TS 28.531 (V17.1.0): "Management and orchestration; Provisioning".

[i.4] ETSI TS 128 533 (V17.2.0): "5G; Management and orchestration; Architecture framework (3GPP TS 28.533 version 17.2.0 Release 17)".

[i.5] 3GPP TS 28.552 (V17.4.0): "Management and orchestration; 5G performance measurements".

[i.6] Void.

[i.7] ETSI TS 128 632 (V17.0.0): "Universal Mobile Telecommunications System (UMTS); LTE; Telecommunication management; Inventory Management (IM) Network Resource Model (NRM) Integration Reference Point (IRP); Information Service (IS) (3GPP TS 28.632 version 17.0.0 Release 17)".

[i.8] ETSI TS 132 346 (V17.0.0): "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; Telecommunication management; File Transfer (FT) Integration Reference Point (IRP): Solution Set (SS) definitions (3GPP TS 32.346 version 17.0.0 Release 17)".

[i.9] ETSI TS 137 320 (V17.1.0): "Universal Mobile Telecommunications System(UMTS); LTE; 5G; Radio measurement collection for Minimization of Drive Tests (MDT); Overall description; Stage 2 (3GPP TS 37.320 version 17.1.0 Release 17)".

[i.10] O-RAN TS O-RAN.WG3.O1-Interface-for-NearRT-RIC: "O1 Interface Specification for Near Real Time RAN Intelligent Controller".

[i.11] O-RAN TS O-RAN.WG5.O-CU-O1.0: "O1 Interface Specification for O-CU-UP and O-CU-CP".

[i.12] O-RAN TS O-RAN.WG5.WG5.O-DU-O1.0: "O1 Interface Specification for O-DU".

[i.13] O-RAN TS O-RAN.WG10.WG10.OAM-Architecture: "O-RAN Operations and Maintenance Architecture".

[i.14] O-RAN TS O-RAN.WG10.Information Model and Data Models.0: "O-RAN Information Model and Data Models Specification".

[i.15] Void.

[i.16] Void.

[i.17] Void.

[i.18] Recommendation ITU-T X.733: "Information technology - Open Systems Interconnection - Systems Management: Alarm reporting function".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in 3GPP TR 21.905 [i.1] apply.

NOTE: A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [i.1].

3.2 Symbols

For the purposes of the present document, the symbols given in 3GPP TR 21.905 [i.1] apply.

NOTE: A symbol defined in the present document takes precedence over the definition of the same symbol, if any, in 3GPP TR 21.905 [i.1].

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [i.1] and the following apply:

NOTE: An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [i.1].

3GPP 3rd Generation Partnership Project

ASN.1	Abstract Syntax Notation One
CM	Configuration Management
CRUD	Create, Read, Update, Delete
FS	Fault Supervision
FTPES	File Transfer Protocol with Explicit SSL/TLS encryption
GPB	Google Protocol Buffers
HTTP	HyperText Transfer Protocol
HTTPS	HTTP Secure
ID	IDentifier
IETF	Internet Engineering Task Force
IOC	Information Object Class
IP	Internet Protocol
JSON	JavaScript Object Notation
MDT	Minimization of Drive Testing
ME	Managed Element
MF	Managed Function
MnS	Management Service
MOC	Managed Object Class
MOI	Managed Object Instance
Near-RT RIC	O-RAN Near Real Time RAN Intelligent Controller
NETCONF	NETwork CONFiguration protocol
NF	Network Function
NGRAN	Next Generation Radio Access Network
NMS	Network Management System
NR	New Radio
NRM	Network Resource Model
O-CU-CP	O-RAN Central Unit – Control Plane.
O-CU-UP	O-RAN Central Unit – User Plane
O-DU	O-RAN Distributed Unit
O-RAN	Open Radio Access Network
O-RU	O-RAN Radio Unit
ONAP	Open Network Automation Platform
PM	Performance Management or Performance Measurements
PNF	Physical Network Function
RAN	Radio Access Network
RCEF	RRC Connection Establishment Failure
REST	REpresentational State Transfer
RFC	Request For Comments
RLF	Radio Link Failure
RRC	Radio Resource Control
SA5	Services & System Aspects Working Group 5 Telecom Management
SBMA	Services Based Management Architecture

NOTE: See ETSI TS 128 533 [i.4], clause 4.

SDO	Standards Defining Organization
SMO	Service Management and Orchestration
SFTP	SSH File Transfer Protocol
SSH	Secure Shell
TLS	Transport Layer Security
TR	Technical Report
TRS	Trace Recording Session
TS	Technical Specification
UE	User Equipment
URI	Uniform Resource Identifier
VES	VNF Event Stream
VNF	Virtualized Network Function
XML	eXtensible Markup Language

4 General Requirements

4.1 Service Management and Orchestration (SMO)

REQ-SMO-FUN-1: O-RAN compliant SMOs shall support the O1 interfaces as defined in the present document.

4.2 Transport Layer Security (TLS)

TLS requirements specified in O-RAN Security Protocol Specifications [16] clauses 4.2, 4.3 and 4.4 shall apply.

4.3 HyperText Transfer Protocol (HTTP)

REQ-HTP-FUN-1: Management Service providers and consumers that use HTTP shall support HTTP v1.1 or higher.

REQ-HTP-FUN-2: Management Service providers and consumers that use HTTP should support HTTP v2.0.

4.4 Secure Shell (SSH)

SSH requirements specified in O-RAN Security Protocol Specifications [16] clause 4.1 shall apply.

4.5 Least Privilege Access Control

Least privilege access control requirements specified in O-RAN Security Requirements Specification [17] clause 5.2.2 shall apply.

4.6 Confidentiality, Integrity and Authenticity

Confidentiality, integrity and authenticity requirements specified in O-RAN Security Requirements Specification [17] clause 5.2.2 shall apply.

5 O1 Notifications

5.1 General

An O1 notification is a JSON encoded asynchronous notification sent from a MnS provider to a MnS consumer over the O1 interface using REST/HTTPS.

An O1 notification shall be in one of the following formats:

- SDO O1 format
- VES O1 format

An SDO O1 format notification is an O1 notification formatted as specified by a Standards Defining Organization (SDO). Currently, O1 supports SDO O1 format notifications that are either 3GPP-specified or O-RAN-specified. SDO O1 format notifications are formatted as specified by the SDO and sent without a VES header.

3GPP-specified O1 notifications are specified in ETSI TS 128 532 [3], clause 11 and clause 12.

O-RAN-specified O1 notifications are specified in the O-RAN Information Model and Data Models Specification [i.14].

O-RAN-specified O1 notifications should follow 3GPP naming and format where possible to reduce the number of variants that need to be supported. Specifically, O-RAN-specified O1 notifications should:

- be named "o1NotifyXxx";
- include the common 3GPP notification fields objectClass, objectInstance, notificationId, notificationType, eventTime and systemDN;
- include an additionalText and/or additionalInformation field when appropriate.

A VES O1 format notification is an O1 notification formatted as specified by VES Event Listener Specification [18], consisting of a common event header and domain-specific event fields. VES O1 format notifications are categorized into 2 types, based on domain:

- Harmonized VES
- Legacy VES

Harmonized VES refers to the stndDefined VES event specified in VES Event Listener Specification [18] that allows a VES event to carry, as its payload, a notification specified by an SDO. In the case of O-RAN O1 Interface Specification, a harmonized stndDefined VES event carries either a 3GPP-specified O1 notification or an O-RAN specified O1 notification as its payload.

Legacy VES refers to any VES event specified in the VES Event Listener Specification [18], except for stndDefined. Legacy VES events are fully defined in [18] and do not rely on an SDO to specify the content of the payload. The Legacy VES events supported by O1 Interface Specification is PNF Registration.

Legacy VES events are supported for backward compatibility. However, harmonized VES events are preferred. Use of harmonized VES events results in less notification variants for the providers and the consumers because a harmonized VES O1 format notification is effectively an SDO O1 format notification wrapped in a VES common event header.

Two attributes are used to communicate the notification format between MnS provider and MnS consumer:

- o1NotifyFormatCapabilities indicates whether the MnS provider supports the capability to send notifications in SDO O1 format, VES O1 format or both. This attribute is set by the MnS provider at the Managed Element level, meaning the capability is for all O1 notifications sent by that MnS provider. It is not per notification type. This attribute is read-only for the MnS consumer.
- o1NotifyFormatConfig indicates whether the MnS consumer wants to receive notifications in SDO O1 format or VES O1 format. This attribute is optional to be supported by MnS provider. This attribute is configured by the MnS consumer at the Managed Element level, meaning the configuration is for all O1 notifications sent by that MnS provider. It is not per notification type. If the MnS provider supports both formats, the MnS provider sets the value for this attribute to the default value of VES O1 format when the MOI is created and the MnS consumer is permitted to change the value to SDO O1 format if desired. Otherwise, if the MnS provider only supports one notification format, this attribute is absent.

Configuration attributes are specified in the O-RAN Information Model and Data Models Specification [i.14].

It is not necessary to have an attribute to indicate whether harmonized VES or legacy VES is sent for VES format because the domain of the event is provided in the VES common event header and the schema of the event is provided by the Network Function at onboarding time.

5.2 O-RAN Defined O1 Notification

5.2.1 Requirements

REQ-ON-FUN-1: O-RAN defined O1 PNF and VNF registration notification shall be JSON encoded for sending via REST/HTTPS.

REQ-ON-FUN-2: Schema for O-RAN defined O1 notification shall be specified using OpenAPI.

REQ-ON-FUN-3: If VES O1 format is configured to be used, O-RAN defined O1 notification shall be presented in harmonized VES format and schemaReference shall refer to O-RAN defined schema in O-RAN public repository when it is available.

NOTE 1: O-RAN public repository is not created yet.

NOTE 2: Before the schema for the O-RAN defined notification is available in the O-RAN public repository, the schemaReference in the VES O1 format for O-RAN defined O1 notification does not need to be a path to the public repository.

5.2.2 stndDefinedNamespace name space for O-RAN

O-RAN defines following name space for VES O1 format-harmonized VES format: OR-PnfRegistration.

For O-RAN defined performance measurements, the short form of measurement name has prefix "OR.". The source of the definition is clear, so there is no need to have a separate O-RAN name space for performance measurement.

O-RAN defined performance measurements should use 3GPP-PerformaceMeasurement name space and refer to 3GPP schema.

6 Management Services

6.1 Provisioning Management Services

6.1.0 Overview

Provisioning management services allow a Provisioning MnS Consumer to configure attributes of managed objects on the Provisioning MnS Provider that modify the Provisioning MnS Provider's capabilities in its role in end-to-end network services and allows a Provisioning MnS Provider to report configuration changes to the Provisioning MnS Consumer. NETCONF is used for the Provisioning Management Services to Create Managed Object Instance, Delete Managed Object Instance, Modify Managed Object Instance Attributes and Read Managed Object Instance Attributes. A RESTful/HTTP notification with data modelled using YANG is used to notify the Provisioning MnS subscribed Consumers when a configuration change occurs.

Stage 1 Provisioning management services are specified in 3GPP TS 28.531 [i.3] clause 6.3.

Stage 2 Provisioning operations and notifications are specified in ETSI TS 128 532 [3] clause 11.1.1.

Stage 3 Provisioning operations for YANG/NETCONF solution set are specified in ETSI TS 128 532 [3] clause 12.1.3.

Stage 3 Provisioning notifications for "YANG/Netconf-based- solution set" with data modelled using YANG in a RESTful notification is specified in ETSI TS 128 532 [3] clause 12.1.3.

For the VES header support, refer to ETSI TS 128 532 [3] clause 12.1.2. The media type of the notification, as specified by the "Content-Type" header in the HTTP POST request, shall be "application/json".

NOTE: In the payload, the data is encoded according to ETSI TS 128 532 [3] clause 12.1.3.2.5 (except for the content type in the header). Consumption of the payload is implementation dependent.

IETF reference documents for NETCONF and YANG include IETF RFC 6241 [20] and IETF RFC 7950 [21].

6.1.1 General NETCONF Requirements

REQ-GNC-FUN-1: The provisioning management service provider and consumer shall support the following NETCONF operations as specified in IETF RFC 6241 [20]:

- get
- get-config
- edit-config
- lock
- unlock

- close-session
- kill-session

Other operations are optional.

REQ-GNC-FUN-2: The provisioning management service provider and consumer shall support the following NETCONF capabilities:

- writable-running
- rollback-on-error
- validate
- xpath

Other capabilities are optional.

REQ-GNC-FUN-3: The provisioning management service provider and consumer shall support a running datastore for NETCONF. Support for a candidate datastore is optional.

REQ-GNC-FUN-4: The provisioning management service provider and consumer shall support YANG1.1, defined in IETF RFC 7950 [21], including coexistence with YANG Version 1 as specified therein.

REQ-GNC-FUN-5: The provisioning management service provider shall have the capability to establish a NETCONF session with its authorized consumer upon request from the consumer.

REQ-GNC-FUN-6: The provisioning management service provider shall support an established NETCONF session until the authorized consumer terminates the session.

NOTE: The consumer may want to perform multiple provisioning management services operations during a single NETCONF Session.

REQ-GNC-FUN-7: The provisioning management service provider shall have the capability to terminate a NETCONF session with its authorized consumer when requested to do so by the authorized consumer.

REQ-GNC-FUN-8: The provisioning management service provider shall have the capability to make provisioning operation results persistent over a reset.

REQ-GNC-FUN-9: The provisioning management service provider and consumer shall support NETCONF over SSH or NETCONF over TLS.

REQ-GNC-FUN-10: The provisioning management service provider shall support /netconf-state/schemas subtree and <get-schema> RPC defined in IETF RFC 6022 [19] for all supported YANG modules.

6.1.2 Create Managed Object Instance

6.1.2.1 Description

Provisioning MnS Consumer sends a synchronous provisioning update request to the Provisioning MnS Provider to create a Managed Object Instance (MOI) on the Provisioning MnS Provider and set its attribute values.

6.1.2.2 Requirements

The mapping of operations specified in ETSI TS 128 532 [3], clauses 12.1.3.1.1 and 12.1.3.1.2 shall apply.

6.1.2.3 Procedures

```
@startuml
Title Create MOI
autonumber "[0]"
participant "Provisioning MnS Consumer" as NMS
participant "Provisioning MnS Provider" as ME
NMS –> ME: NETCONF edit-config create
Note over ME : Create MOI
ME --> NMS: NETCONF rpc-reply <OK> or <rpc-error>
@enduml
```

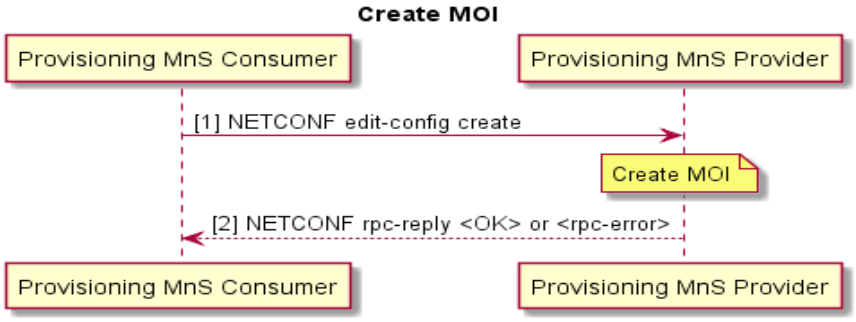

Figure 6.1.2.3-1: Create MOI

Pre-Conditions:

- NETCONF session has been established with Provisioning MnS Provider. NETCONF session has authorized privileges into the identified section of the data store.
- Optionally, target data store has been locked.

Procedure:

1) Provisioning MnS Consumer sends NETCONF edit-config create operation to Provisioning MnS Provider:
   a) Provisioning MnS Provider creates the MOI(s) in the target data store as specified in the edit-config operation.
2) Provisioning MnS Provider returns NETCONF response.

6.1.3 Modify Managed Object Instance Attributes

6.1.3.1 Description

Provisioning MnS Consumer sends synchronous provisioning updates to the Provisioning MnS Provider to modify the attributes of a MOI on the Provisioning MnS Provider.

6.1.3.2 Requirements

The mapping of operations specified in ETSI TS 128 532 [3] clauses 12.1.3.1.1 and 12.1.3.1.4 shall apply.

6.1.3.3 Procedures

```
@startuml
Title Modify MOI Attributes
autonumber "[0]"
participant "Provisioning MnS Consumer" as NMS
participant "Provisioning MnS Provider" as ME
NMS –> ME: NETCONF edit-config create, replace or delete
Note over ME : Modify MOI
ME --> NMS: NETCONF rpc-reply <OK> or <rpc-error>
@enduml
```

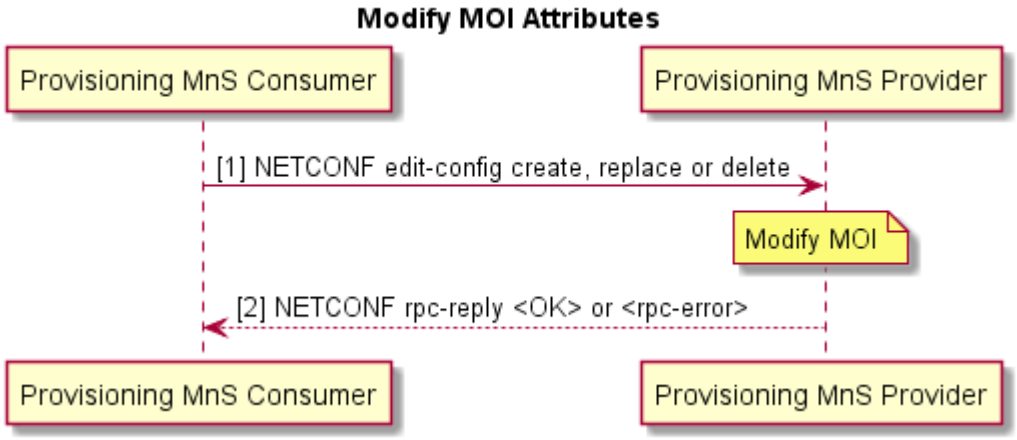

Figure 6.1.3.3-1: Modify MOI Attributes

Pre-Conditions:

- NETCONF session has been established with Provisioning MnS Provider. NETCONF session has authorized privileges into the identified section of the data store.
- Optionally, target data store has been locked.

Procedure:

1) Provisioning MnS Consumer sends NETCONF edit-config create, replace, or delete operation to Provisioning MnS Provider:
   a) Provisioning MnS Provider modifies the MOI(s) in the target data store as specified in the edit-config operation.
2) Provisioning MnS Provider returns NETCONF response.

6.1.4 Delete Managed Object Instance

6.1.4.1 Description

Provisioning MnS Consumer sends synchronous provisioning updates to the Provisioning MnS Provider to delete a MOI and its children on the Provisioning MnS Provider.

6.1.4.2 Requirements

The mapping of operations specified in ETSI TS 128 532 [3] clauses 12.1.3.1.1 and 12.1.3.1.5 shall apply.

6.1.4.3 Procedures

```
@startuml
Title Delete MOI
autonumber "[0]"
participant "Provisioning MnS Consumer" as NMS
participant "Provisioning MnS Provider" as ME
NMS -> ME: NETCONF edit-config delete or remove
Note over ME : Delete MOI
ME --> NMS: NETCONF rpc-reply <OK> or <rpc-error>
@enduml
```

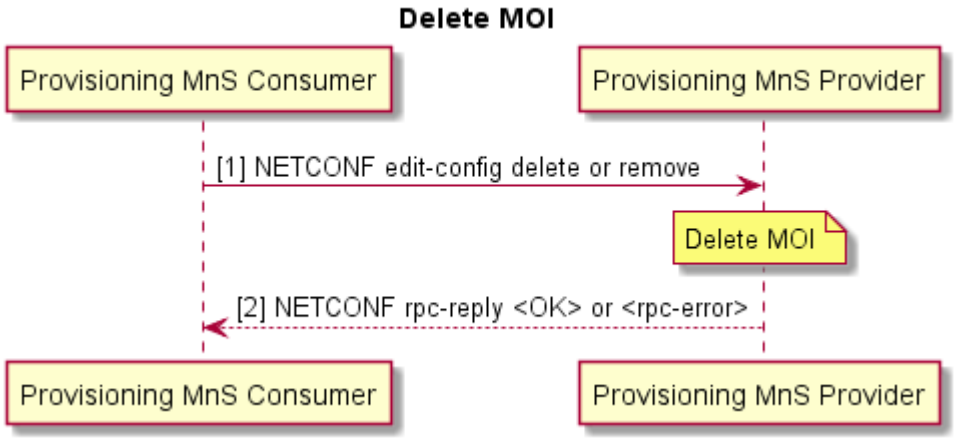

Figure 6.1.4.3-1: Delete MOI

Pre-Conditions:

- NETCONF session has been established with Provisioning MnS Provider. NETCONF session has authorized privileges into the identified section of the data store.
- Optionally, target data store has been locked.

Procedure:

1) Provisioning MnS Consumer sends NETCONF edit-config delete or remove operation to Provisioning MnS Provider:
   a) Provisioning MnS Provider deletes the MOI(s) in the target data store as specified in the edit-config operation.
2) Provisioning MnS Provider returns NETCONF response.

6.1.5 Read Managed Object Instance Attributes

6.1.5.1 Description

Provisioning MnS Consumer sends synchronous provisioning request to the Provisioning MnS Provider to return the values of attributes of its MOI(s) on the Provisioning MnS Provider.

6.1.5.2 Requirements

The mapping of operations specified in ETSI TS 128 532 [3] clauses 12.1.3.1.1 and 12.1.3.1.3 shall apply.

6.1.5.3 Procedures

```
@startuml
Title Read MOI Attributes
autonumber "[0]"
participant "Provisioning MnS Consumer" as NMS
participant "Provisioning MnS Provider" as ME
NMS -> ME : NETCONF get or get-config
Note over ME : Retrieve config
ME --> NMS: NETCONF rpc-reply <data>
@enduml
```

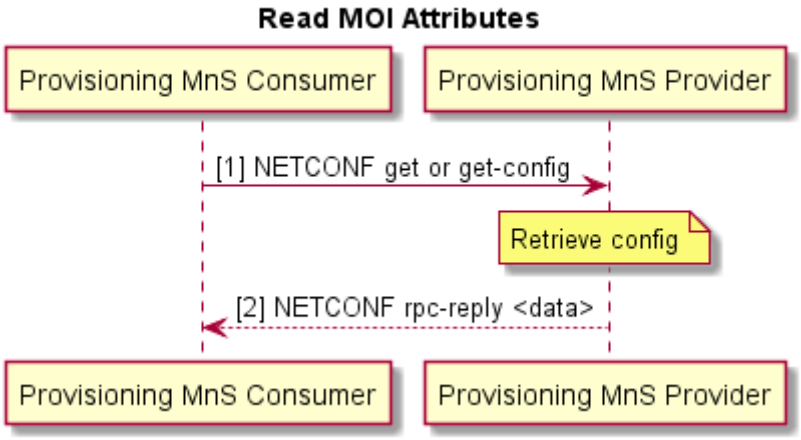

Figure 6.1.5.3-1: Read MOI Attributes

Pre-Conditions:

- NETCONF session has been established with Provisioning MnS Provider. NETCONF session has authorized privileges into the identified section of the data store.

Procedure:

1) Provisioning MnS Consumer sends NETCONF get or get-config operation to Provisioning MnS Provider:

   a) Provisioning MnS Provider retrieves the MOI(s) and its attributes from the target data store as specified in the get or get-config operation.

2) Provisioning MnS Provider returns the data in the NETCONF response.

6.1.6 Notify Managed Object Instance Changes

6.1.6.1 Description

Provisioning MnS Provider sends an asynchronous notifyMOIChanges Notification to the Provisioning MnS Consumer to report configuration changes to one or more MOIs on the Provisioning MnS Provider. Refer to ETSI TS 128 532 [3], clause 12.1.3.2.5 for details.

6.1.6.2 Requirements

The mapping of notifications specified in ETSI TS 128 532 [3], clause 11.1.1.11 shall apply.

6.1.6.3 Procedures

```
@startuml
Title Notify Managed Object Instance Changes
Autonumber
participant "Provisioning MnS Consumer" as NMS
participant "Provisioning MnS Provider" as ME
Note over ME : One or more config changes occur
ME ->> NMS : <<HTTP/TLS>> notifyMOIChanges Notification
Note over NMS : Reconcile Database
@enduml
```

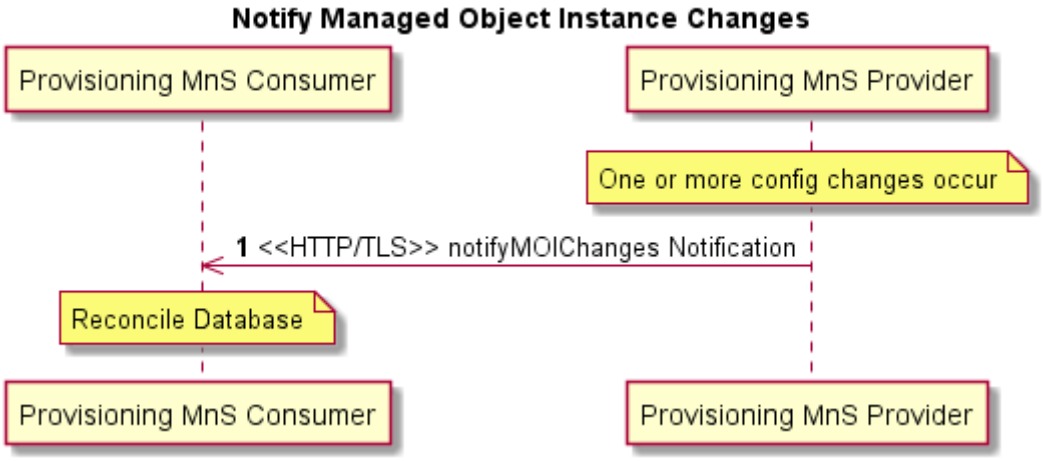

Figure 6.1.6.3-1: Notify Managed Object Instance Changes

Pre-conditions:

- One or more MOIs are created, deleted or modified in the running data store of the Provisioning MnS Provider.
- Provisioning MnS Consumer has subscribed for notifyMOIChanges notifications.

Procedure:

1) Provisioning MnS Provider sends notifyMOIChanges notification to the Provisioning MnS Consumer over HTTP/TLS. Mutual certificate authentication is performed.

Post-condition:

- Provisioning MnS Consumer reconciles its copy of the Provisioning MnS Provider configuration database with the change.

6.1.6.4 Operations and Notifications

A Provisioning MnS notification shall be in one of the following formats:

- SDO O1 format:
  - An O1supported 3GPP-specified Provisioning notification, as specified in ETSI TS 128 532 [3].
- VES O1 format:
  - A Harmonized VES event, as specified in the VES Event Listener Specification [18], containing stndDefinedFields with a "data" element that contains an O1supported 3GPP-specified Provisioning notification, as specified in ETSI TS 128 532 [3].

The O1-supported 3GPP-specified CM notification is:

- notifyMOIChanges

A single notifyMOIChanges notification can report one or more MOI creations, MOI deletions and/or MOI attribute value changes in one notification.

The attribute name value pairs in the CM notifications are provided using YANG 1.1 encoded in JSON format as specified in IETF RFC 7951 [22].

6.1.7 Subscription Control

6.1.7.1 Description

Subscription Control allows a MnS Consumer to subscribe to notifications emitted by a MnS Provider.

Starting with 3GPP Release 16, dedicated operations for Management Services Use Cases are supported by IOCs with attributes that can be read and/or set using generic provisioning mechanisms. For Subscription Control, the Subscribe and Unsubscribe operations are replaced with a NtfSubscriptionControl IOC as specified in ETSI TS 128 622 [7]. NtfSubscriptionControl IOC contains attributes that allow a MnS Consumer to set the recipient address for the notifications and identify the scope of notifications desired. Optionally, the types of notifications desired, and notification filtering may also be provided. If filtering of the notifications is supported, only those notifications that match the specified value would be sent. For example, notifyNewAlarm notifications can be filtered to send only those with severity set to major or critical.

6.1.7.2 Requirements

NtfSubscriptionControl IOC definition shall be as specified in ETSI TS 128 622 [7], clause 4.3.22 with attribute definitions specified in ETSI TS 128 622 [7], clause 4.4.1.

YANG models for NtfSubscriptionControl shall be as specified in ETSI TS 128 623 [23], clause D.2.6a.

6.1.7.3 Procedures

NtfSubscriptionControl instances may be created and deleted by the system or pre-installed. Optionally, the NtfSubscriptionControl MOIs can be created and deleted, and attributes modified using NETCONF/YANG by the management service consumer following the procedures described in this Provisioning MnS clause.

6.1.7.4 Operations and Notifications

Subscription Control can be used to subscribe to alarm notifications specified in ETSI TS 128 622 [7], clause 4.4.1 notificationTypes. Subscription Control can be used to subscribe to heartbeat notifications as specified in ETSI TS 128 622 [7], Figure 4.2.1-5; i.e. by creating the HeartbeatControl MOI as a child of the NtfSubscriptionControl MOI.

6.1.8 NETCONF Session Establishment

6.1.8.1 Description

Provisioning MnS Consumer uses the NETCONF Session Establishment procedure to establish a NETCONF session on the Provisioning MnS Provider.

6.1.8.2 Requirements

Requirements for NETCONF session establishment specified in IETF RFC 6241 [20] shall apply.

6.1.8.3 Procedure

The procedure to establish a NETCONF session is shown below.

```
@startuml
Title NETCONF Session Establishment
autonumber "[0]"
participant "Provisioning MnS Consumer" as SMO
participant "Provisioning MnS Provider" as ME
SMO <-> ME : SSH or TLS session establishment
SMO -> ME : NETCONF Hello
ME --> SMO : NETCONF Hello <sessionId> <capabilitiesList>
@enduml
```

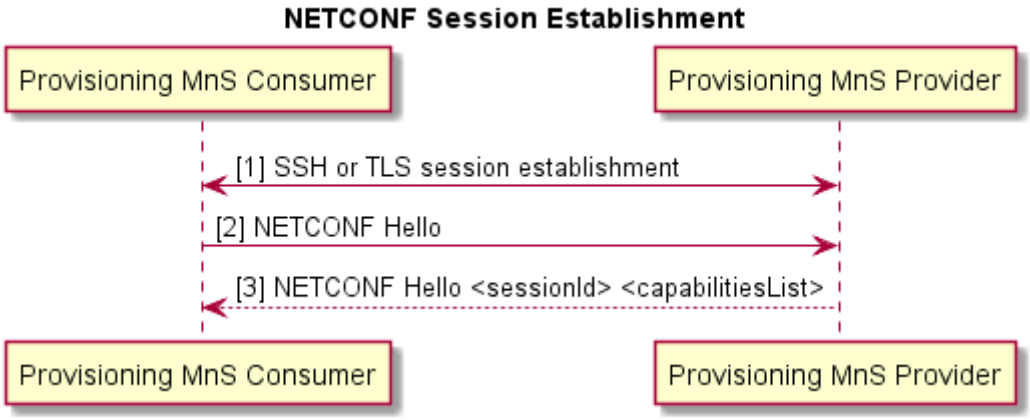

Figure 6.1.8.3-1: NETCONF Session Establishment

6.1.9 NETCONF Session Termination

6.1.9.1 Description

Provisioning MnS Consumer uses the NETCONF Session Termination procedure to gracefully terminate a NETCONF session on a Provisioning MnS Provider.

6.1.9.2 Requirements

NETCONF session termination shall be as specified in IETF RFC 6241 [20], section 7.8.

6.1.9.3 Procedure

The procedure to terminate a NETCONF session is shown below.

```
@startuml
Title NETCONF Session Termination
autonumber "[0]"
participant "Provisioning MnS Consumer" as SMO
participant "Provisioning MnS Provider" as ME
SMO -> ME : NETCONF close-session
ME --> SMO : NETCONF rpc-reply <OK>
@enduml
```

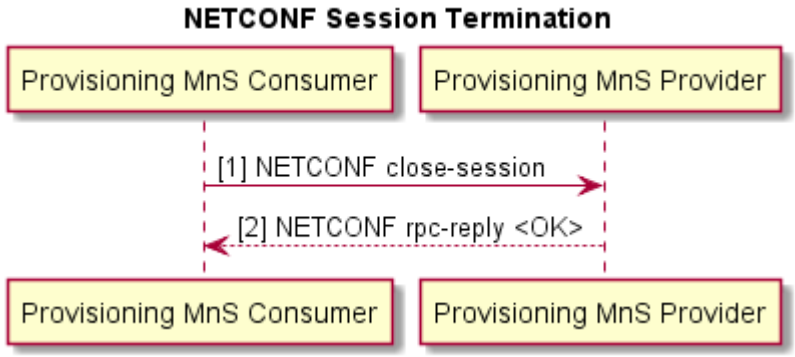

Figure 6.1.9.3-1: NETCONF Session Termination

6.1.10 Lock Data Store

6.1.10.1 Description

Provisioning MnS Consumer uses the Lock Data Store procedure to lock a target data store on a Provisioning MnS Provider. This procedure is optional, but recommended, to prevent unpredictable behavior during configuration changes.

6.1.10.2 Requirements

NETCONF lock data store should be as specified in IETF RFC 6241 [20], section 7.5.

6.1.10.3 Procedure

The procedure to lock a data store is shown below.

```
@startuml
Title Lock Data Store
autonumber "[0]"
participant "Provisioning MnS Consumer" as SMO
participant "Provisioning MnS Provider" as ME
SMO -> ME : NETCONF lock <targetDS>
Note over ME : Lock target DS
ME --> SMO : NETCONF rpc-reply <OK>
@enduml
```

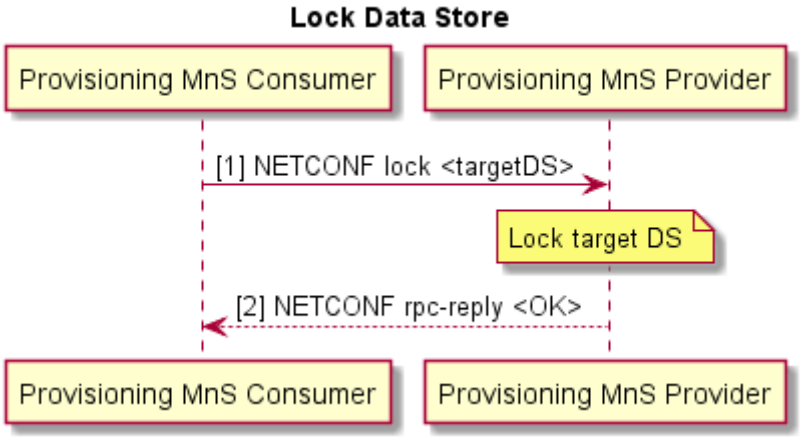

Figure 6.1.10.3-1: Lock Data Store

6.1.11 Unlock Data Store

6.1.11.1 Description

Provisioning MnS Consumer uses the Unlock Data Store procedure to unlock a target data store on a Provisioning MnS Provider.

6.1.11.2 Requirements

NETCONF unlock data store should be as specified in IETF RFC 6241 [20], section 7.6.

6.1.11.3 Procedure

The procedure to unlock a data store is shown below.

```
@startuml
Title Unlock Data Store
autonumber "[0]"
participant "Provisioning MnS Consumer" as SMO
participant "Provisioning MnS Provider" as ME
SMO -> ME : NETCONF unlock <target DS>
Note over ME : Unlock target DS
ME --> SMO : NETCONF rpc-reply <OK>
@enduml
```

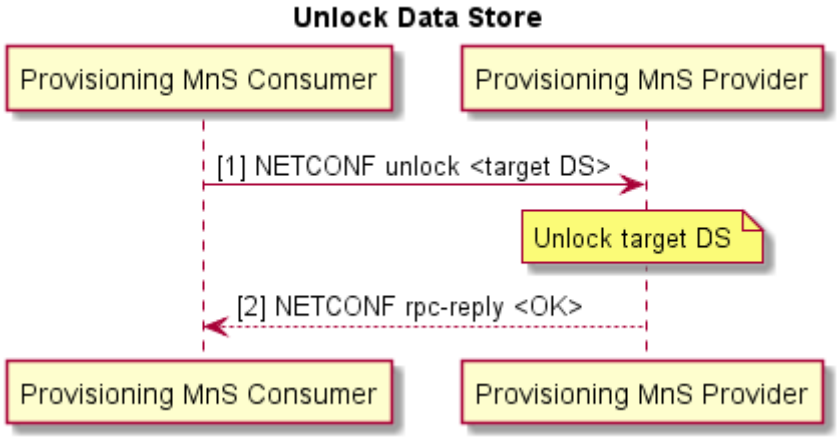

Figure 6.1.11.3-1: Unlock Data Store

6.1.12 Commit

6.1.12.1 Description

Provisioning MnS Consumer uses the Commit procedure to commit a configuration change to the running data store of the Provisioning MnS Provider. This is necessary to make the configuration change effective if it was made in the candidate data store. If the configuration change was made in the running data store, the commit procedure is not used.

6.1.12.2 Requirements

Requirements for NETCONF commit specified in IETF RFC 6241 [20], section 8.4 shall apply.

6.1.12.3 Procedure

The procedure to commit a configuration change is shown below.

```
@startuml
Title Commit
autonumber "[0]"
participant "Provisioning MnS Consumer" as SMO
participant "Provisioning MnS Provider" as ME
SMO -> ME : NETCONF commit
Note over ME : Commit change to running DS
ME --> SMO: NETCONF rpc-reply <OK>
@enduml
```

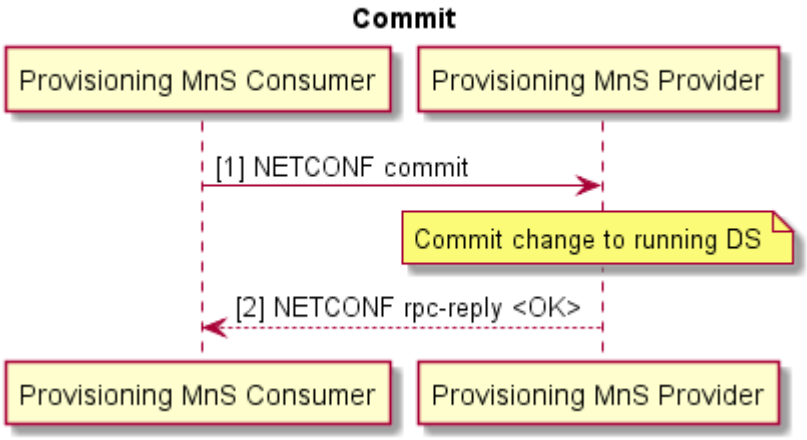

Figure 6.1.12.3-1: Commit

6.2 Fault Supervision Management Services

6.2.0 Overview

Fault supervision management services allow a Fault Supervision MnS Provider to report errors and events to a Fault Supervision MnS Consumer and allows a Fault Supervision MnS Consumer to perform fault supervision operations on the Fault Supervision MnS Provider, such as get alarm list.

Stage 1 Fault Supervision MnS is specified in ETSI TS 128 545 [5].

Stage 2 Fault Supervision notifications are specified in ETSI TS 128 532 [3].

Stage 2 AlarmList IOC and AlarmRecord data type are specified in ETSI TS 128 622 [7].

Stage 3 Solution Sets for XML, JSON and YANG are specified in ETSI TS 128 623 [23].

6.2.1 Fault Notification

6.2.1.1 Description

Fault Supervision MnS Provider sends asynchronous Fault notification event to Fault Supervision MnS Consumer when an alarm occurs, is cleared, or changes severity.

6.2.1.2 Requirements

The following fault supervision data report service requirements specified in ETSI TS 128 545 [5] clause 5.2.5 shall apply:

- **REQ-FSDR_NF-FUN-1** for sending alarm notifications
- **REQ-FSDR_NF-FUN-3** for alarm notification subscription
- **REQ-FSDR_NF-FUN-4** for alarm notification unsubscription
- **REQ-FSDR_NF-FUN-6** for reading the alarm list
- **REQ-FSDR_NF-FUN-8** for reading the alarm list with a filter
- **REQ-FSDR_NF-FUN-9** for sending changed alarm notifications
- **REQ-FSDR_NF-FUN-10** for sending cleared alarm notifications
- **REQ-FSDR_NF-FUN-11** for sending new alarm notifications

- **REQ-FSDR_NF-FUN-12** for sending alarm list rebuilt notification

The following requirements from ETSI TS 128 545 [5] clause 5.2.5 may apply:

- **REQ-FSDR_NF-FUN-5** for filtering the alarm notifications that are reported

NOTE: Filtering is best done at the SMO level.

6.2.1.3 Procedures

Procedures are defined in ETSI TS 128 545 [5] clause 9.1.

6.2.1.4 Operations and Notifications

A Fault Supervision MnS notification shall be in one of the following formats:

- SDO O1 format:
  - An O1-supported 3GPP-specified Fault Supervision notification, as specified in ETSI TS 128 532 [3].
- VES O1 format:
  - A Harmonized VES event, as specified in the VES Event Listener Specification [18], containing stndDefinedFields with a "data" element that contains an O1-supported 3GPP-specified Fault notification, as specified in ETSI TS 128 532 [3].

The O1-supported 3GPP-specified Fault Supervision notifications are:

- notifyNewAlarm
- notifyChangedAlarmGeneral and/or notifyChangedAlarm
- notifyClearedAlarm
- notifyAlarmListRebuilt

NotifyChangedAlarm only supports reporting the severity change. NotifyChangedAlarmGeneral permits the producer to report the severity change and any other attribute changes associated with this alarm in a single notification. The other 3GPP Fault Supervision notifications specified in ETSI TS 128 532 [3] are optional.

6.2.2 Fault Supervision Control

6.2.2.1 Description

Starting with 3GPP Release 16, dedicated operations for Management Services Use Cases are supported by IOCs with attributes that can be read and/or set using generic provisioning mechanisms. For Fault Supervision, an AlarmList IOC is specified in ETSI TS 128 622 [7] that represents the capability to store and manage alarm records. There is one AlarmList per Fault Supervision MnS Provider, created by the Provider. The AlarmList contains one AlarmRecord for each active alarm. The AlarmRecords in the AlarmList can be read by the Fault Supervision MnS Consumer, with an optional filter to retrieve selected AlarmRecords based on the value of attributes in the AlarmRecord. For example, Fault Supervision MnS Consumer is able to retrieve only those AlarmRecords with perceivedSeverity = CRITICAL.

6.2.2.2 Requirements

The following fault supervision data control service requirements from ETSI TS 128 545 [5], clause 5.2.6 may apply to the Fault Supervision MnS Provider:

- **REQ-FSDC_NF-FUN-1** to support alarm acknowledgement.

NOTE 1: There is no Use Case that requires a NF to acknowledge an alarm. This operation is best done at the SMO level.

- NF that does not support the alarm acknowledgement from the MnS Consumer shall consider cleared alarms as automatically acknowledged so that they may be removed from the AlarmList.

- **REQ-FSDC_NF-FUN-2** to support manual alarm clearing.

NOTE 2: Manual clearing of alarms is only for ADMC (Automatically Detected, Manually Cleared) alarms.

- NF that supports ADMC alarms should support the manual alarm clearing operation.

- **REQ-FSDC_NF-FUN-4** to support acknowledgement state change notifications.

NOTE 3: There is no Use Case that requires a NF to acknowledge an alarm. This operation is best done at the SMO level.

- NF that supports the alarm acknowledgement should support the acknowledgement state change notifications.

AlarmList IOC definition shall be as specified in ETSI TS 128 622 [7], clauses 4.3.26 and 4.3.27 with attribute definitions in specified in ETSI TS 128 622 [7], clause 4.4.1.

YANG solution set for AlarmList IOC shall be as specified in ETSI TS 128 623 [23], clause D.2.9.

6.2.2.3 Procedures

NETCONF protocol and YANG data models are used to get and set the attributes of the AlarmRecords in the AlarmList.

Refer to Provisioning management services clause for procedures to read MOI attributes and modify MOI attributes using NETCONF.

6.2.2.4 Void

6.3 Performance Assurance Management Services

6.3.0 Overview

Performance Assurance Management Services allow a Performance Assurance MnS Provider to report file-based (bulk) and/or streaming (real time) performance data to a Performance Assurance MnS Consumer and allows a Performance Assurance MnS Consumer to perform performance assurance operations on the Performance Assurance MnS Provider, such as selecting the measurements to be reported and setting the frequency of reporting.

Use cases are specified in ETSI TS 128 550 [6], clause 5.1.

Stage 2 notifyFileReady notification is specified in ETSI TS 128 532 [3].

Stage 2 PerfMetricJob IOC is specified in ETSI TS 128 622 [7].

Stage 3 Solution Sets for XML, JSON and YANG are specified in ETSI TS 128 623 [23].

Stage 2 and 3 for streaming data reporting service are specified in ETSI TS 128 532 [3].

6.3.1 Performance Data File Reporting

6.3.1.1 Description

Performance Assurance MnS Provider sends asynchronous FileReady notification event to Performance Assurance MnS Consumer when PM File(s) is ready for retrieval. The FileReady notification contains information needed to retrieve the file such as filename and the location where the file can be retrieved.

Performance Assurance MnS Consumer retrieves the PM File(s) from the location specified in the notifyFileReady notification.

6.3.1.2 Requirements

Requirements specified in ETSI TS 128 550 [6], clause 5.2.2 shall apply.

6.3.1.3 Procedures

Procedure is specified in ETSI TS 128 550 [6], clause 5.1.1.2.

```
@startuml
Title PM Data File Reporting and Retrieval
participant "Performance Assurance MnS Consumer" as NMS
participant "Performance Assurance MnS Provider" as ME
Note over ME : 1 New PM data file available
ME ->> NMS : 2 <<HTTP/TLS>> notifyFileReady Notification
NMS -> ME : 3 <<Secure File Transfer Protocol>> Get PM File(s)
@enduml
```

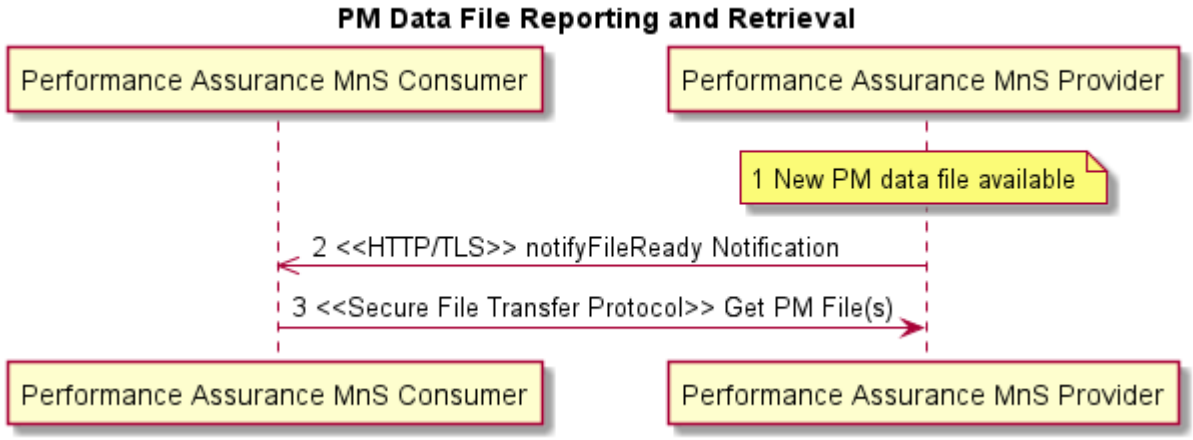

Figure 6.3.1.3-1: PM Data File Reporting and Retrieval

Pre-condition:

- Performance Assurance MnS Consumer has subscribed to File Ready notifications.

Procedure:

1) A new PM data file is available on the Performance Assurance MnS Provider.

2) Performance Assurance MnS Provider sends notifyFileReady notification to Performance Assurance MnS Consumer over HTTP/TLS. Mutual certificate authentication is performed.

3) Performance Assurance MnS Consumer sets up a secure file transfer protocol connection to the location specified in the notifyFileReady notification and gets the PM data file(s). Secure file transfer protocols are specified in ETSI TS 128 537 [4], clause 7.1.3.

6.3.1.4 Operations and Notifications

A File Ready notification shall be in one of the following formats:

- SDO O1 format:
  - An O1-supported 3GPP-specified notifyFileReady notification, as specified in ETSI TS 128 532 [3].
- VES O1 format:
  - A Harmonized VES event, as specified in the VES Event Listener Specification [18], containing stndDefinedFields with a "data" element that contains an O1-supported 3GPP-specified File Ready notification, as specified in ETSI TS 128 532 [3].

The O1-supported 3GPP-specified File Ready notification is:

- notifyFileReady.

6.3.1.5 PM File Generation and Reporting

PM file generation and reporting shall be as specified in ETSI TS 128 532 [3], clause 11.6.

6.3.1.6 PM File Content

PM file content shall be as specified in ETSI TS 128 532 [3], clause 11.3.2.1.2.

6.3.1.7 PM File Naming

PM file naming shall be as specified in ETSI TS 128 532 [3], clause 11.3.2.1.4.

6.3.1.8 PM File XML Format

PM file XML format shall be as specified in ETSI TS 128 532 [3], clause 12.3.2 and/or in ETSI TS 132 432 [14], clause 4.1.

6.3.1.9 5G Performance Measurements

3GPP defined 5G performance measurements are specified in 3GPP TS 28.552 [i.5]. In addition to the 3GPP-defined measurements, it is possible to have O-RAN defined measurements and vendor supplied measurements. Clause 6.3.4 provides requirements for O-RAN defined measurements. O-RAN defined measurements are named with an "OR." prefix. Vendor supplied measurements are named with a "VS." prefix.

6.3.2 Performance Data Streaming

6.3.2.1 Description

Performance Assurance MnS Provider steams high volume asynchronous streaming performance measurement data to Performance Assurance MnS Consumer at a configurable frequency. A secure WebSocket connection is established between the Performance Assurance Provider and the Performance Assurance Consumer. The connection supports the transmission of one or more streams of PM data. Each stream of PM data is configured as a PerfMetricJob (see clause 6.3.3 of the present document). The provider supplies information about the supported streams to the consumer during the connection establishment. The connection may be established to support one or more streams. Streams can be added or removed from the connection as the PerfMetricJobs are added or deleted. The connectionID that carries the streaming PM data is provided to the Performance Assurance Provider during the establishment of the WebSocket connection by the Performance Assurance Consumer.

6.3.2.2 Requirements

Requirements for Streaming PM specified in ETSI TS 128 550 [6], clause 5.2.3 shall apply.

6.3.2.3 Procedures

Use Cases for Streaming PM are specified in ETSI TS 128 550 [6], clause 5.1.1.3. Operations and notifications specified in ETSI TS 128 532 [3], clause 11.5 are applicable to both Streaming PM and Streaming Trace.

```
@startuml
Title Performance Data Streaming
Autonumber
participant "Performance Assurance MnS Consumer" as NMS
participant "Performance Assurance MnS Provider" as ME
Note over ME : Performance Data Streaming Job Configured
ME ->> NMS : <<HTTP/TLS>> establish Streaming Connection
NMS ->> ME : <<HTTP/TLS>> Connection Established
loop (while performance job is active)
ME ->> NMS : <<WebSocket>> report stream data via performance data stream unit
End
|||
@enduml
```

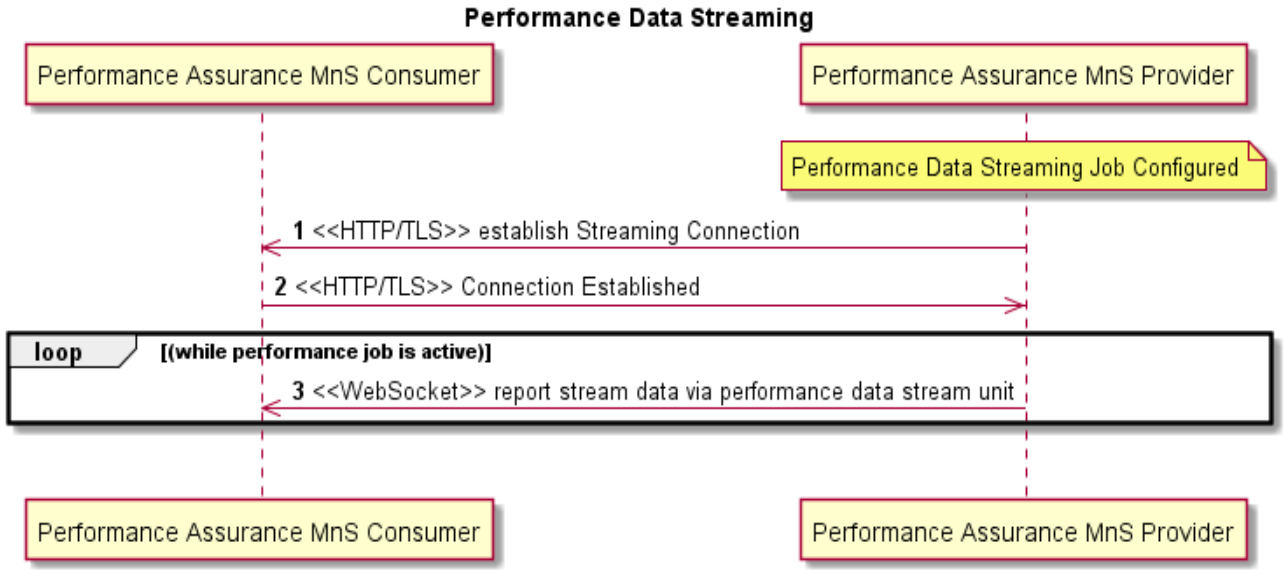

Figure 6.3.2.3-1: Perf Data Streaming Connection Establishment and Data Transmission

Pre-condition:

- Performance Assurance MnS Provider is configured to produce PerfMetricJob to be delivered via streaming PM to the Performance Assurance Consumer.

Procedure:

1) Performance Assurance MnS Provider requests to establish a WebSocket connection to begin streaming PM data and provides MetaData about the streams that are to be sent on the connection.

2) Performance Assurance Consumer accepts the request to upgrade the connection to a WebSocket.

3) Performance Assurance MnS Provider transmits binary encoded data to consumer while performance job is active.

6.3.2.4 Operations and Notifications

ETSI TS 128 532 [3], clause 11.5.1 defines the following operations that an O-RAN compliant NF that supports streaming PM shall support. These are the same operations as listed for streaming trace in clause 6.4.6.1 of the present document. They are repeated here, as it is possible that a NF may support different levels of streaming for trace and performance assurance:

- establishStreamingConnection operation is specified in ETSI TS 128 532 [3], clause 11.5.1.1. Establishing the streaming connection is initiated via an HTTPS POST followed by an HTTP GET (upgrade) to establish the WebSocket connection.

- terminateStreamingConnection operation is specified in ETSI TS 128 532 [3], clause 11.5.1.2. This operation is accomplished via a WebSocket Close Frame to tear down the streaming connection when all stream jobs on this connection have been terminated. The delivery of WebSocket Close Frame is provided by the underlying TCP.

- reportStreamData operation is specified in ETSI TS 128 532 [3], clause 11.5.1.3. The streamData field contains the streaming PM data which is encoded according to the format defined in ETSI TS 128 550 [6] Annex G which provides the ASN.1 definition of the Performance Data Stream Units. The delivery of WebSocket Close Frame is provided by the underlying TCP.

If O-RAN NF supports the capability of sending multiple PM streams across the WebSocket connection, the following operations shall be supported:

- addStream operation is specified in ETSI TS 128 532 [3], clause 11.5.1.4. This operation is used when a new Performance Assurance Stream (PM job started) is added on the Performance Assurance Provider to be delivered to this consumer and the NF supports multiple streams per connection. The addStream operation is accomplished via an HTTP POST.

- deleteStream operation is specified in ETSI TS 128 532 [3], clause 11.5.1.5. This operation is used when a Performance Assurance Stream (PM job stopped) is deleted from the connection between the Performance Assurance Provider and the Performance Assurance Consumer. The deleteStream operation is accomplished via an HTTP DELETE.

The following operations specified in ETSI TS 128 532 [3], clause 11.5.1 may be supported by O-RAN NFs:

- getConnectionInfo operation is specified in ETSI TS 128 532 [3], clause 11.5.1.6. This operation allows the performance data streaming service provider to get information from the performance data streaming service consumer on the streams active on the connection.

- getStreamInfo operation is specified in ETSI TS 128 532 [3], clause 11.5.1.7. This operation allows the performance data streaming service provider to get the information for one or more streams from the streaming consumer (i.e. stream target).

No notifications have been defined for Performance Data Streaming.

6.3.2.5 PM Streaming Data Generation and Reporting

ETSI TS 128 550 [6], Annex C lists all the Performance Data Stream Unit Content Items. Annex C of the present document provides a description of the establishment of the WebSocket connection and the subsequent operations provided as part of the data streaming service. The example utilizes the trace service, but the operations around the establishment and tear down of the connection are the same for streaming PM and streaming Trace. The WebSocket connection remains until all streams configured to be provided between the PA Provider and the PA Consumer have been terminated.

6.3.2.6 PM Streaming Data Format

PM Streaming data shall be delivered according to the format specified in the input parameters of the establishStreamConnection operation specified in ETSI TS 128 532 [3], clause 11.5.1.1.2.

6.3.3 Measurement Job Control

6.3.3.1 Description

Starting with 3GPP Release 16, Performance Assurance Control supported by IOCs with attributes that can be read and/or set using generic provisioning mechanisms in the Measurement Job Control Service. Measurement jobs can be created and terminated by creating and deleting a PerfMetricJob MOI. Measurement jobs can be queried by getting the attributes of a PerfMetricJob MOI. Measurement jobs can be temporarily suspended or resumed by modifying the administrativeState attribute of a PerfMetricJob MOI to LOCKED or UNLOCKED.

6.3.3.2 Requirements

Requirements for measurement job control specified in ETSI TS 128 550 [6], clause 5.2.1 shall apply.

PerfMetricJob IOC definition shall be as specified in ETSI TS 128 622 [7], clause 4.3.31 with attribute definitions in specified in ETSI TS 128 622 [7], clause 4.4.1. SupportedPerfMetricGroup datatype shall be as specified in ETSI TS 128 622 [7], clause 4.3.32. ReportingCtrl shall be as specified in ETSI TS 128 622 [7], clause 4.3.33.

YANG solution set for PerfMetricJob IOC shall be as specified in ETSI TS 128 623 [23], clause D.2.4.

6.3.3.3 Procedures

Procedures for measurement job creation, termination, query, suspend and resume are specified in ETSI TS 128 622 [7], clause 4.3.31.

NETCONF protocol and YANG data models are used to create MOI, delete MOI, modify attributes and get attributes of a PerfMetricJob. Refer to Provisioning management services clause for detailed procedures on how to perform these operations using NETCONF.

6.3.3.4 Void

6.3.4 O-RAN Defined Performance Measurements

6.3.4.1 Requirements

REQ-OPM-FUN-1: O-RAN specific measurements shall be defined using the template specified in ETSI TS 132 404 [10].

REQ-OPM-FUN-2: The Measurement Name for O-RAN defined measurements shall not exceed 64 characters in length and should be constrained to 32 characters maximum.

REQ-OPM-FUN-3: Measurement Name of O-RAN defined measurements shall begin with OR prefix to indicate that O-RAN is the source of the measurement. When a measurement is accepted in 3GPP, the OR prefix shall be deleted.

REQ-OPM-FUN-4: Short form of the measurement name in the Measurement Type for an O-RAN defined measurement shall begin with "OR." to indicate that O-RAN is the source of the measurement definition. When a measurement is accepted in 3GPP, the OR prefix shall be deleted.

REQ-OPM-FUN-5: In case O-RAN extends the definition of an existing 3GPP measurement, a new O-RAN measurement shall be defined. 3GPP measurement name shall be part of new defined O-RAN measurement name. 3GPP definition for the measurement which new O-RAN measurement is based on shall be referred when possible.

NOTE: Informative Annex A provides examples of how O-RAN O-DU measurements could be specified following the template in ETSI TS 132 404 [10].

6.4 Trace Management Services

6.4.0 Overview

Trace management services allow a Trace MnS Provider to report file-based or streaming trace records to the Trace MnS Consumer. Trace Control provides the ability for the Trace Consumer to start a trace session by configuring a Trace Job via the Trace Control IOC or by establishing a trace session that propagates trace parameters to other trace management providers via signaling. There are multiple levels of trace that can be supported on the provider as described in 3GPP TS 32.421 [11], clause 4.1. The Trace Provider may be configured to support file-based trace reporting or streaming trace reporting.

Trace Management Services specified in 3GPP TS 32.421 [11], 3GPP TS 32.422 [12] and 3GPP TS 32.423 [13] and supported on an applicable O-RAN ME include Call Trace, Minimization of Drive Testing (MDT), RRC Connection Establishment Failure (RCEF) and Radio Link Failure TCE (RLF). All of these services follow a similar management paradigm. Trace Sessions are configured on the provider with information on where and how to send the trace information to the consumer. The provider creates trace records within a trace session as the trigger mechanism occurs. Trace records are produced and provided to the consumer until the trace session is terminated.

File-based trace collects trace records in files that are available to the consumer with a time delay. In the case of streaming trace, the data is sent in bursts across a WebSocket connection to the consumer, maintaining the relevance of the data while minimizing transport overhead.

Stage 1 Trace Management Service is specified in 3GPP TS 32.421 [11]. Use cases for trace are specified in clause 5.8 and elaborated in 3GPP TS 32.421 [11], Annex A. General Trace Requirements are found in 3GPP TS 32.421 [11], clause 5.1.

Stage 2 Trace Operations are found in 3GPP TS 32.422 [12] for 5G support of Call Trace and for streaming trace.

Stage 2 Trace Control IOC for management-based control is specified in ETSI TS 128 622 [7]. Stage 2 for signaling based activation is found in 3GPP TS 32.422 [12].

Stage 3 definitions of trace record content for all trace types, XML trace file format, and streaming trace GPB record definition are found in 3GPP TS 32.423 [13].

Stage 3 Trace Control IOC mapping for management-based control is specified in ETSI TS 128 623 [23], clause D.2.10.

Stages 2 and 3 definitions for streaming data reporting are specified in ETSI TS 128 532 [3].

6.4.1 Call Trace

6.4.1.1 Trace Data Reporting

6.4.1.1.1 Description

Trace Data can be reported from the Trace Provider to the Trace Consumer via trace files or via a streaming interface. For management-based activation, Trace Data is collected after the TraceJob is configured on the Trace Provider, the Trace Session is activated, and the triggering event occurs. For signaling-based activation, the Trace Recording Session starts when the NF receives trace control and configuration parameters via one of the signalling messages specified in 3GPP TS 32.422 [12], clause 4.2.3.12.

When the Trace Provider collects trace data to a file, the file is periodically provided to the Trace Consumer. When the provider supports streaming trace, the trace is sent to the consumer via data bursts which are sent frequently enough to retain the relevance of the data while conserving transport resources. The WebSocket connection carrying the streaming trace is preserved for the duration of the streaming trace.

6.4.1.1.2 Requirements

Requirements for Trace data specified in 3GPP TS 32.421 [11], clause 5.2 shall apply to both file-based and streaming trace.

6.4.1.1.3 Procedures

Trace Data is binary encoded and reported in Trace Records. The procedures for reporting data are specified in 3GPP TS 32.422 [12], clause 7. File-based trace reporting procedures are found in 3GPP TS 32.422 [12], clauses 7.1.1 and 7.2.1. Streaming trace reporting procedures are found in 3GPP TS 32.422 [12], clauses 7.1.2 and 7.2.2. Trace Record Contents are specified in 3GPP TS 32.423 [13], clause 4. The Trace Record content is the same for trace jobs controlled by management-based activation and signaling-based activation. The raw trace record content is the same for file-based trace and streaming trace. Trace data is binary encoded in ASN.1. File-based trace is delivered in XML format with trace records encoded in ASN.1. Streaming trace is delivered in GPB encoded data bursts with the trace record payload containing ASN.1 encoded data.

Procedures for naming the trace data file are found in 3GPP TS 32.423 [13], Annex B. File Naming Convention is fully specified in 3GPP TS 32.423 [13], clause B.1.

Trace files are produced in XML format. The XML format is specified in 3GPP TS 32.423 [13], clause A2.2. Example XML files are provided in 3GPP TS 32.423 [13], Annex D.

If a trace file cannot be created, a trace failure notification file XML schema can be sent. The XML schema is provided in 3GPP TS 32.422 [12], clause A.5 and the naming convention for the file containing the failure is specified in clause A.4.

For streaming trace, raw trace data is collected on the node and sent to the trace collector. The trace data is binary encoded. The format of the streaming trace data is provided in 3GPP TS 32.423 [13]. The reportStreamData operation is specified in ETSI TS 128 532 [3], clause 12.5.1.1.4.

6.4.1.2 Trace Session Activation

6.4.1.2.1 Description

A trace session starts on a provider configured to support a TraceJob via management or signaling-based activation. Management-based trace session activation is initiated from the Provisioning Management Service Consumer to activate a TraceJob which has been configured on the provider. See clause 6.4.5 of the present document. With signaling-based trace session activation, the provider receives a signaling message that contains trace consumer ID address (IP address for file-based or URI for streaming) along with trace control parameters. Each Trace session has a unique trace session identifier that is associated with all of the trace data collected for this session.

If the trace session is configured to be file-based, the provider collects the data and stores the data in a file. The provider optionally sends the file directly to the consumer or sends the location of the file to the consumer. File transport approach is not standardized.

ETSI TS 128 532 [3] supports the streaming of trace data from the provider to the consumer. Trace data for a trace session is collected and transmitted to the provider across a secure WebSocket connection in data bursts which are emitted frequently enough to ensure the relevance of the data while conserving transport resources. See clause 6.4.6 and Annex C of the present document for details on the streaming service.

6.4.1.2.2 Requirements

Requirements for Trace Session Activation for file-based and streaming trace specified in 3GPP TS 32.421 [11], clause 5.3.1 shall apply.

6.4.1.2.3 Procedures

Procedures for activating a Trace Session via management-based control are found in 3GPP TS 32.422 [12], clause 4.1.1.1 for general procedures and 3GPP TS 32.422 [12], clause 4.1.1.9 for NGRAN specific procedures. Procedures for activating a Trace Session via signaling are found in 3GPP TS 32.422 [12], clauses 4.1.2.1 and 4.1.2.16.

6.4.1.3 Trace Session Deactivation

6.4.1.3.1 Description

A Trace Session is terminated/deactivated when any of the defined stop triggering events occur as specified in 3GPP TS 32.421 [11], such as a timer expiring, or the TraceJob Session is deactivated via management control.

6.4.1.3.2 Requirements

Requirements for Trace Session Deactivation specified in 3GPP TS 32.421 [11], clause 5.4.1 shall apply.

6.4.1.3.3 Procedures

Procedures for Trace Session Deactivation are found in 3GPP TS 32.422 [12], clause 4.1.3.10 for management-based trace deactivation and clause 4.1.4.1.2 for signalling-based trace deactivation.

6.4.1.4 Trace Recording Session Activation

6.4.1.4.1 Description

A trace recording session is a specific instance of the data specified to be collected for a particular trace session, for example, a specific call. For management-based activation, the trace recording session starts on a provider configured with an active trace session when a triggering event occurs, such as a new call starting. Each Trace recording session within a trace session has a unique trace recording session reference. This recording session reference and the session reference are included with each trace record, uniquely identifying the trace record as belonging to a particular trace recording session. For signaling-based activation, the Trace Recording Session starts when the NF receives trace control and configuration parameters via a control signalling message. 3GPP TS 32.422 [12], clause 4.3.2.12 outlines the procedures the node is to follow when determining when to begin a new trace recording session and when to continue with an existing session.

6.4.1.4.2 Requirements

Requirements for Trace Recording Session Activation specified in 3GPP TS 32.421 [11], clause 5.3.2 shall apply.

6.4.1.4.3 Procedures

Procedures for starting a Trace Recording Session are found in 3GPP TS 32.422 [12], clause 4.2.1 for general requirements. 3GPP TS 32.422 [12], clause 4.2.2.10 has requirements for management-based trace session activation and clause 4.2.3.12 has requirements when the trace session was activated via signaling.

6.4.1.5 Trace Recording Session Termination

6.4.1.5.1 Description

A Trace Recording Session is terminated when any of the defined stop triggering events occur or the Trace Session is deactivated.

6.4.1.5.2 Requirements

Requirements for Trace Recording Session Termination specified in 3GPP TS 32.421 [11], clause 5.4.2 shall apply.

6.4.1.5.3 Procedures

Procedures for Trace Recording Session Termination are found in 3GPP TS 32.422 [12], clauses 4.2.4.10 and 4.2.5.13.

6.4.2 Minimization of Drive Testing (MDT)

6.4.2.1 Description

ETSI TS 137 320 [i.9] provides an overall description for MDT. An O-RAN network function may support Immediate and Logged MDT as described in ETSI TS 137 320 [i.9]. Logged MDT is always file-based. Immediate MDT may be configured to be file-based or streaming. MDT measurements are described in ETSI TS 137 320 [i.9]. 3GPP TS 32.421 [11], 3GPP TS 32.422 [12] and 3GPP TS 32.423 [13] describe the management of MDT and have been updated to support 5G.

6.4.2.2 Requirements

Requirements for managing MDT specified in 3GPP TS 32.421 [11], clause 6 shall apply.

6.4.2.3 Procedures

Procedures for Trace Session Activation are the same for MDT as for Call Trace and are found in 3GPP TS 32.422 [12], clause 4.1. Procedures for specifying MDT Trace selection conditions are found in 3GPP TS 32.422 [12], clause 4.1.5.

Procedures for Trace Recording Sessions start and stop for MDT are found in 3GPP TS 32.422 [12], clause 4.2.

Procedures for handling MDT sessions at handover for Immediate MDT are found in 3GPP TS 32.422 [12], clause 4.4 and Logged MDT in 3GPP TS 32.422 [12], clause 4.5.

Procedures for user consent handling in MDT are specified in 3GPP TS 32.422 [12], clause 4.6.

Procedures for MDT reporting are specified in 3GPP TS 32.422 [12], clause 6.

MDT Trace Record Contents are specified in 3GPP TS 32.423 [13], clause 4.

Trace file format for MDT Trace is specified in 3GPP TS 32.423 [13], clause A.2.1. Example XML files are provided in 3GPP TS 32.423 [13], clause D.1.4.

6.4.3 Radio Link Failure (RLF)

6.4.3.1 Description

Radio Link Failure (RLF) reporting is a special Trace Session which provides the detailed information when a UE experiences an RLF event, and the reestablishment is successful to the source gNB. 3GPP TS 32.421 [11], 3GPP TS 32.422 [12] and 3GPP TS 32.423 [13] describe the management of RLF.

6.4.3.2 Requirements

Requirements for RLF specified in 3GPP TS 32.421 [11], clause 7 shall apply.

6.4.3.3 Procedures

Procedures for Trace session activation and deactivation for RLF reporting are found in 3GPP TS 32.422 [12], clauses 4.3.1 and 4.3.2.

Procedures for specifying the RLF reporting job type when configuring the RLF reporting session are found in 3GPP TS 32.422 [12], clause 5.9a.

Procedures for RLF reporting follow standard trace reporting procedures documented in 3GPP TS 32.422 [12], clause 7.

6.4.4 RRC Connection Establishment Failure (RCEF)

6.4.4.1 Description

Radio Resource Control (RRC) Connection Establishment Failure (RCEF) is activated on the gNB as a special Trace Session where the job type indicates RCEF reporting only. The records are produced when a UE experiences an RCEF event and the RRC establishment is successful to the same gNB.

6.4.4.2 Requirements

Requirements for RCEF specified in 3GPP TS 32.421 [11], clause 7 shall apply.

6.4.4.3 Procedures

Procedures for trace session activation of RCEF are found in 3GPP TS 32.422 [12], clause 4.8.1.

Procedures for trace session deactivation for RCEF reporting are found in 3GPP TS 32.422 [12], clause 4.8.2.

Procedures for specifying the job type for RCEF are found in 3GPP TS 32.422 [12], clause 5.9a.

Procedures for RCEF Reporting are specified in 3GPP TS 32.422 [12], clause 7.

6.4.5 Trace Control

6.4.5.1 Description

Starting with 3GPP Release 16, Management-based Trace Control is supported with IOCs with attributes that can be read and/or set using generic provisioning mechanisms in the Trace Control Service. For Trace Control, this includes operations such as Create TraceJob, Activate TraceJob, Deactivate TraceJob, and Query TraceJobs. TraceJobs can be created, activated, deactivated, and queried by setting and/or getting attributes in the TraceJob IOC. The TraceJob IOC supports Management-based activation for Call Trace, MDT, RLF and RCEF.

Trace sessions can also be activated and deactivated via Signaling-based configuration initiated from another NF to propagate a configured trace, such as a UE trace when the UE moves from one NF to another.

6.4.5.2 Requirements

Management-based activation and deactivation shall be done via the TraceJob IOC defined in ETSI TS 128 622 [7] clause 4.30. Requirements for TraceJob Activation specified in 3GPP TS 32.421 [11], clause 5.3.1 and requirements for TraceJob deactivation specified in 3GPP TS 32.421 [11], clause 5.4.1 shall apply for both Management and Signaling activation.

6.4.5.3 Procedures

Management-based activation and deactivation accomplished using CRUD operations specified in clause 6.1 of the present document. The attributes of the TraceJob are specified in ETSI TS 128 622 [7], clause 4.3.30.2. Constraints on these attributes are specified in ETSI TS 128 622 [7], clause 4.3.30.3. Trace Control IOC mapping for management-based control is specified in ETSI TS 128 623 [23]. The YANG model for the Trace Control IOC is specified in ETSI TS 128 623 [23], clause D.2.10.

Procedures for Signaling-based Trace Session Activation are found in 3GPP TS 32.422 [12], clause 4.1.2.

Procedures for Trace Session Deactivation are found in 3GPP TS 32.422 [12], clause 4.1.4.

6.4.6 Streaming Trace

6.4.6.0 Overview

A NF can be configured to deliver trace data via a file or via a streaming interface. The streaming capability was introduced in 3GPP Release 16. The additional requirements and procedures supported for streaming trace are provided in this clause. An example of the configuration, activation, recording and termination of a streaming trace connection are shown in Informative Annex C.

6.4.6.1 Streaming Trace Requirements and Procedures

As noted above, trace session and recording activation and deactivation, as well as the content of the trace record, are the same for file-based and streaming trace. The requirements for streaming trace delivery specified in 3GPP TS 32.421 [11], clause 5.5 shall apply. Operations for establishing the streaming connection, adding, and deleting streams from the connection and reporting streaming trace data shall be as specified in ETSI TS 128 532 [3], clause 11.5. O-RAN NFs supporting streaming trace shall support the establishStreamingConnection, reportStreamData and terminateStreamingConnection operations. O-RAN NFs that support the multiplexing of trace streams across a single connection shall support the addStream and deleteStream operations. Optionally, the NF may also support the getConnectionInfo and getStreamInfo operations which allow the provider to query for information on the connection and streams on the connection. No notifications have been defined for streaming trace.

Stage 3 information on the streaming operations is provided in ETSI TS 128 532 [3], clause 12.5 with Open API YAML definition provided in clause A.6.1.2.

The procedure for establishStreamingConnection is an HTTP POST operation to provide the information on the stream to the consumer and to receive the Connection ID as a response. The HTTP POST is followed by an HTTP GET to upgrade the connection to a WebSocket connection. This operation is used when no connection is established between the provider and the consumer. The WebSocket connection can contain one or more streams of data from streaming trace or streaming PM. See ETSI TS 128 532 [3], clause 12.5.1.1.2.

The terminateStreamingConnection is a WebSocket close frame operation. This operation is used when all streams on a connection have terminated. See ETSI TS 128 532 [3], clause 12.5.1.1.3.

The addStream Operation is an HTTP POST to indicate that additional streams are being added to the connection. A stream corresponds to a trace job or a streaming PM job. See ETSI TS 128 532 [3], clause 12.5.1.1.5.

The deleteStream Operation is an HTTP DELETE to indicate that a stream has been terminated from the connection. See ETSI TS 128 532 [3], clause 12.5.1.1.6.

The reportStreamData is a WebSocket data frame sent across the connection containing the streaming trace or streaming PM data or an optional alive message indicating that the stream is active, but no data is available. See ETSI TS 128 532 [3], clause 12.5.1.1.4.

The getConnectionInfo Operation is an HTTP GET from the provider to the consumer to obtain information about the connection, such as which streams are supported. See ETSI TS 128 532 [3], clause 12.5.1.1.7.

The getStreamInfo Operation is an HTTP GET from the provider to the consumer to obtain information on the stream. See ETSI TS 128 532 [3], clause 12.5.1.1.8.

Annex C in the present document provides a streaming trace activation example for management-based activation control.

6.4.7 UE Identifiers for Trace Records

6.4.7.1 Description

The contents of the Trace Records are specified in 3GPP TS 32.423 [13], clause 4 and Trace Record Header in 3GPP TS 32.423 [13], clause 5.2.2. The Trace Record containing protocol related messages may contain 3GPP defined UE identifiers corresponding to the protocol. These UE identifiers are a part of protocol messages sent as Trace Records. The Trace Header also contains RAN UE ID as an optional information element. However, for correlation of Trace Records from different O-RAN entities, the UE identifiers embedded in the protocol messages and the RAN UE ID in Trace Header may not be sufficient and may need to be complemented by other information. Hence a set of UE Identifiers and Node Identifiers are defined in O-RAN-Architecture-Description document [15], clause 5.5 for O-RAN ecosystem.

To enable correlation of Trace Records between O-RAN entities, Trace MnS provider includes the optional RAN UE ID in the Trace Header when available and other applicable 3GPP UE identifiers defined in O-RAN-Architecture-Description document [15], clause 5.5 in the optional *vendorExtension* IE defined in 3GPP TS 32.423 [13], clause 5.2.2. in the Trace Header.

Refer to Annex D for the recommendation for UE Identifier format for *vendorExtension* IE in the Trace Header.

6.5 File Management Services

6.5.0 Overview

File management services allow a File Management MnS Consumer to get notification of new available files; query available files and request the transfer of files between the File Management MnS Provider and the File Management MnS Consumer.

Relevant 3GPP specifications for file transfer are ETSI TS 128 537 [4], ETSI TS 132 341 [8], ETSI TS 132 342 [9] and ETSI TS 132 346 [i.8].

6.5.1 File Ready Notification

6.5.1.1 Description

The File Ready Notification notifies a File Management MnS Consumer that a file is available for retrieval from the File Management MnS Provider. In general, File Management MnS Provider sends a notifyFileReady notification for files that the File Management MnS Consumer has configured the File Management MnS Provider to collect on a periodic basis, such as file-based Trace Data or PM Measurement Reports.

6.5.1.2 Requirements

The notifyFileReady notification shall be as specified in ETSI TS 128 532 [3], clause 11.6.1.1.

6.5.1.3 Procedures

File Management MnS Consumer configures a File Management MnS Provider to collect data files with specific characteristics that the File Management MnS Consumer desires, such as file-based Trace Data or PM Measurement Reports described in the Performance Assurance clause of the present document. After configuration, the File Management MnS Consumer terminates the configuration session and waits for the File Management MnS Provider to report that the file is ready for collection.

When a file is available, the File Management MnS Provider sends a notifyFileReady notification to the File Management MnS Consumer using REST/HTTPS.

```
@startuml
skin rose
Title notifyFileReady Notification
Autonumber
participant "File Management MnS Consumer" as consumer
participant "File Management MnS Provider" as provider
Note over provider : New file is available
provider ->> consumer : <<HTTP/TLS>> notifyFileReady Notification
@enduml
```

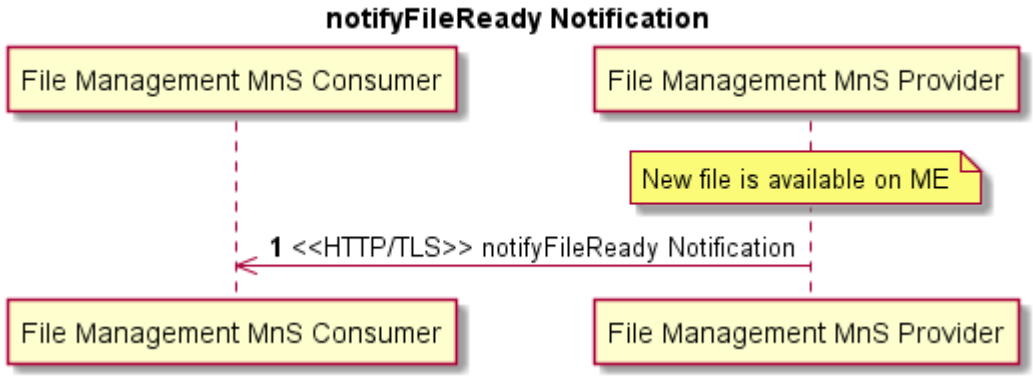

Figure 6.5.1.3-1: File Available for Transfer to Consumer

Pre-condition:

- A new file is available on the File Management MnS Provider.

Procedure:

1) File Management MnS Provider sends notifyFileReady notification to File Management MnS Consumer over HTTP/TLS. Mutual certificate authentication is performed.

6.5.1.4 Operations and Notifications

A File Ready notification shall be in one of the following formats:

- SDO O1 format:
  - An O1-supported 3GPP-specified File Ready notification, as specified in ETSI TS 128 532 [3].
- VES O1 format:
  - A Harmonized VES event, as specified in the VES Event Listener Specification [18], containing stndDefinedFields with a "data" element that contains an O1-supported 3GPP-specified File Ready notification, as specified in ETSI TS 128 532 [3].

The O1-supported 3GPP-specified File Ready notification is:

- notifyFileReady

6.5.1.5 File Types Supported

File Type requirements are documented in ETSI TS 132 341 [8], clause 5.2.

6.5.1.6 File Naming Requirements

Unless explicitly stated in the present document for particular File Types, the File Naming Convention specified in ETSI TS 132 342 [9] Annex A shall apply.

6.5.2 List Available Files

6.5.2.1 Description

File Management MnS Consumer queries the File Management MnS Provider to identify files that are available on the File Management MnS Provider. Upon receipt of the available files and their locations, the File Management MnS Consumer can determine the next appropriate action.

6.5.2.2 Requirements

Requirements on the types of files specified in clause 5.2 of ETSI TS 132 341 [8] shall apply.

6.5.2.3 Procedures

List Available Files Use Case allows the File Management MnS Consumer to obtain a list of available files and their locations by reading the AvailableFileList IOC as specified in ETSI TS 132 342 [9]. A File Management MnS Consumer may use this management service in scenarios where the File Management MnS Provider is collecting information, such as logs, on a standard basis in support of debugging activities. Under normal operations, the File Management MnS Provider does not send this data to the File Management MnS Consumer as the File Management MnS Consumer does not need it. The File Management MnS Provider retains the data with the oldest data being over-written when space is exhausted. In some scenarios, the File Management MnS Consumer may want to retrieve some, or all, of the available log files to resolve an issue. In this case, File Management MnS Consumer sends a NETCONF <get> command to the File Management MnS Provider to obtain the list of available files. File Management MnS Provider responds with AvailableFileList which contains a list of available files and their locations and file types. File Management MnS Consumer may use this information to transfer the desired files. See Transfer File Service clause 6.5.3.

The File Management MnS Consumer does not have to initiate a file retrieval as a result of the obtaining the list of available files. There are use cases where the File Management MnS Consumer may want to verify that files are being collected or verify that all files of a particular type (PM for example) have been retrieved.

```
@startuml
Title List Available Files
autonumber "[0]"
participant "File Management MnS Consumer" as NMS
participant "File Management MnS Provider" as ME
NMS <-> ME : Establish NETCONF Session
NMS -> ME: NETCONF <get> <filter>
ME --> NMS: NETCONF <rpc-reply> <data>
NMS <-> ME : Terminate NETCONF Session
@enduml
```

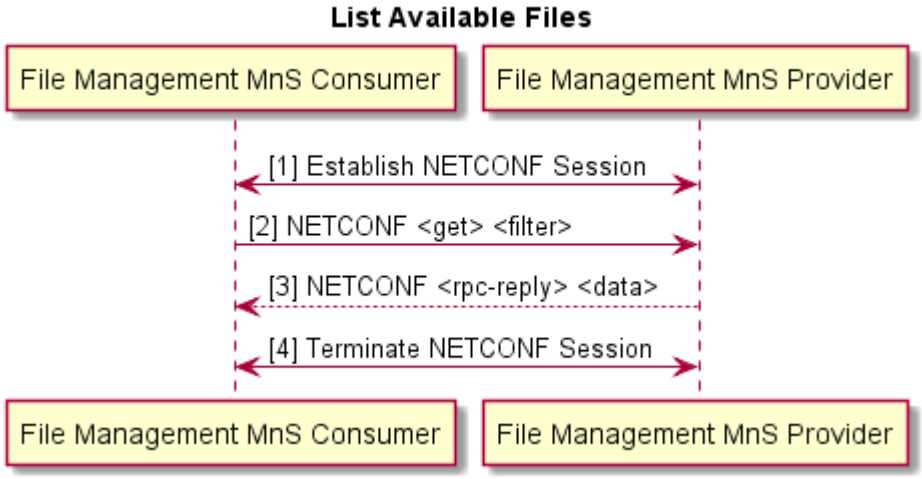

Figure 6.5.2.3-1: List Available Files

1) File Management MnS Consumer establishes NETCONF session with File Management MnS Provider.

2) File Management MnS Consumer sends NETCONF <get> <filter> to the File Management MnS Provider to retrieve the contents of the AvailableFileList.

3) File Management MnS Provider sends NETCONF <rpc-reply> <data>to the File Management MnS Consumer with list of available files on the File Management MnS Provider.

4) File Management MnS Consumer terminates NETCONF session with File Management MnS Provider.

6.5.3 File Transfer to and from File Management MnS Provider

6.5.3.1 Description

The File Transfer by File Management MnS Consumer Use Case provides the capability for a File Management MnS Consumer to transfer files from or to the File Management MnS Provider. In this use case, File Management MnS Consumer is the client and File Management MnS Provider is the file server.

The File Management MnS Consumer can perform this action as a result of:

1) notifyFileReady notification from the File Management MnS Provider informing the File Management MnS Consumer that a file(s)is available.

2) Querying the File Management MnS Provider for the list of available files (see clause 6.5.2).

3) A need to transfer a file from a known location on the File Management MnS Provider.

4) A need to transfer a file to a known location on the File Management MnS Provider. Some examples of files that could be transferred to the FileManagement MnS Provider are:

   - Beamforming configuration file (Opaque Vendor specific data).

- Machine Learning.
- Certificates.

File Transfer is performed using a secure file transfer protocol (SFTP, FTPeS or HTTPS) from or to the File Management MnS Provider.

6.5.3.2 Requirements

File Transfer Requirements specified in clause 7.1.3 of ETSI TS 128 537 [4] shall apply.

6.5.3.3 Procedures

Case 1: File Management MnS Consumer determines that a file needs to be transferred from the the location provided by the File Management MnS Provider as a result of receiving a notifyFileReady notification from the File Management MnS Provider (described in clause 6.5.1).

Case 2: File Management MnS Consumer determines that a file needs to be transferred from the File Management MnS Provider as a result of receiving a list available files from the File Management MnS Provider (described in clause 6.5.2).

Case 3: File Management MnS Consumer determines that a file needs to be transferred from the File Management MnS Provider from a known location on the File Management MnS Provider.

Case 4: File Management MnS Consumer determines that a file needs to be transferred to the File Management MnS Provider to a known location on the File Management MnS Provider.

File Management MnS Consumer initiates a secure file transfer using FTPeS, SFTP or HTTPS to transfer a file from or to the File Management MnS Provider.

```
@startuml
skin rose
Title File Transfer by File Management MnS Consumer.
Autonumber
participant "File Management MnS Consumer" as NMS
participant " File Management MnS Provider" as ME
NMS -> ME : <<FTPeS, SFTP or HTTPS>> Transfer File
@enduml
```

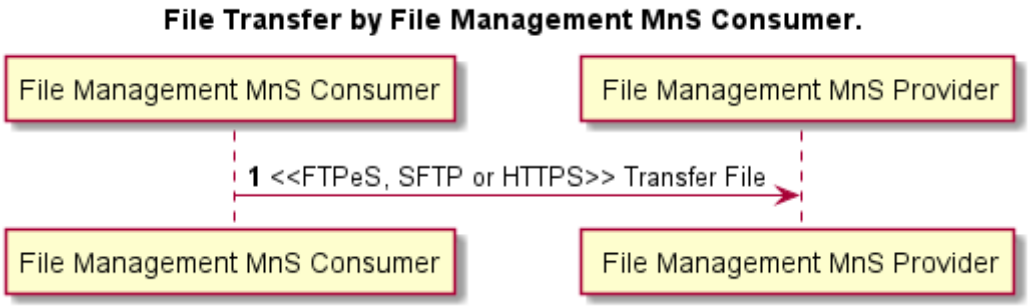

Figure 6.5.3.3-1: File Transfer by File Management MnS Consumer

6.5.4 Download File from remote file server

6.5.4.1 Description

The File Management MnS Consumer has a file that needs to be downloaded to the File Management MnS Provider such as:

- Software file to upgrade software version executed on the File Management MnS Provider
- Beamforming configuration file (Opaque Vendor specific data)

- Machine Learning
- Certificates

The File Management MnS Consumer triggers the file download. The File Management MnS Provider uses a secure file transfer protocol to download the file from the location specified by the File Management MnS Consumer and then notifies the File Management MnS Consumer of the result of the download. In this use case, the File Management MnS Provider is the client. The file could be located on any File Server reachable by the File Management MnS Provider.

6.5.4.2 Requirements

General File Download requirements specified in clause 7.4.3 of ETSI TS 128 537 [4] shall apply.

6.5.4.3 Procedures

```
@startuml
skin rose
Title File Download
autonumber "[0]"
participant "File Management MnS Consumer" as NMS
participant "File Management MnS Provider" as ME
Participant "File Server" as FS
NMS <-> ME : Establish Netconf Session
NMS -> ME: NETCONF <rpc><file-download><remote-file-path>
ME --> NMS: NETCONF <rpc-reply><file-download><status>
NMS <-> ME : Terminate Netconf Session
ME <-> FS : <<FTPeS, SFTP or HTTPS>> file download
Opt Download Progress Notifications
ME ->> NMS : <<HTTP/TLS>> downloadFile Event
End
|||
ME ->> NMS : <<HTTP/TLS>> downloadFile Event
@enduml
```

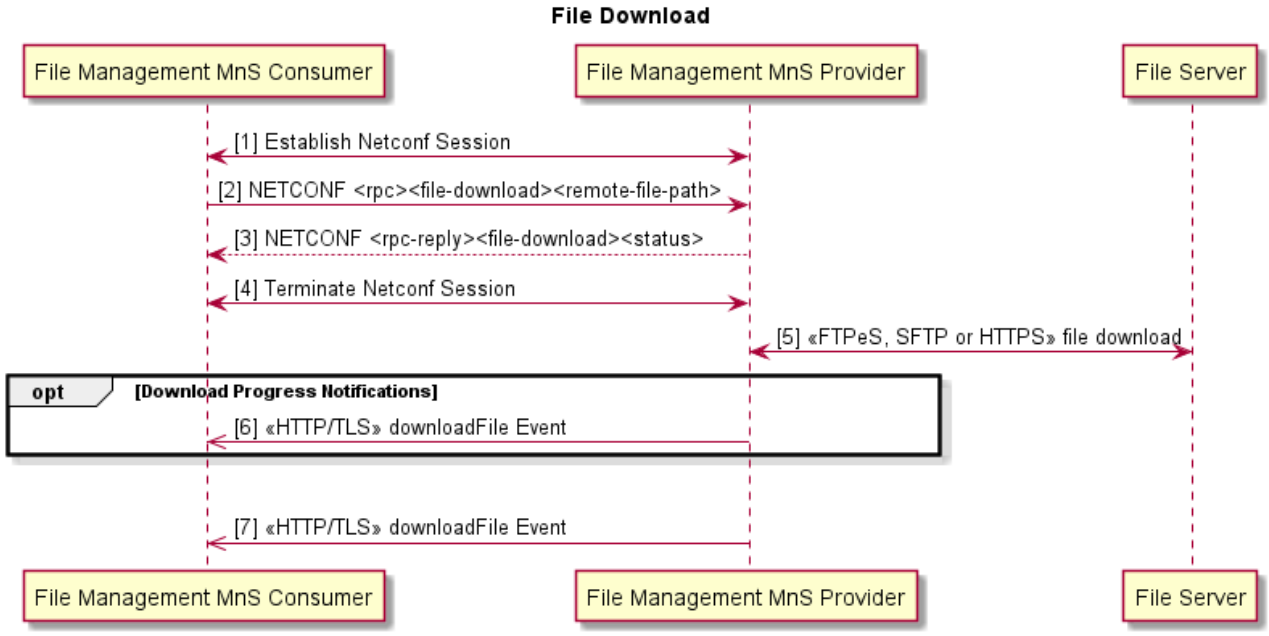

Figure 6.5.4.3-1: File Download

Procedure:

1) File Management MnS Consumer establishes NETCONF session with File Management MnS Provider.
2) File Management MnS Consumer sends NETCONF RPC file-download request, including the location of the file to download, to the File Management MnS Provider to trigger a file download.
3) File Management MnS Provider replies with its ability to begin the download.

4) File Management MnS Consumer terminates NETCONF session with File Management MnS Provider.

5) File Management MnS Provider sets up a secure connection and downloads the file via FTPeS, SFTP or HTTPS. SFTP is authenticated with username/password, SSH keys or X.509 certificates. FTPES is authenticated with X.509 certificates. HTTPS is mutually authenticated with X.509 certificates.

6) (Optional) If the download takes a long time, File Management MnS Provider sends periodic downloadFile notifications to the File Management MnS Consumer with the current status of the download (download in progress).

7) When download completes, File Management MnS Provider sends a downloadFile notification to the File Management MnS Consumer with the final status of the download (success, file missing, failure).

6.5.4.4 Operations and Notifications

A File Download notification shall be in one of the following formats:

- SDO O1 format:
  - Either a 3GPP-specified notifyFileDownload or an O-RAN-specified o1NotifyFileDownload notification should be defined.
- VES O1 format:
  - A Harmonized VES event, as specified in the VES Event Listener Specification [18], containing stndDefinedFields with a "data" element that contains either a 3GPP-specified notifyFileDownload or an O-RAN-specified o1NotifyFileDownload notification.

6.5.5 File push from a MnS producer to a MnS consumer

6.5.5.1 Description

Refer to ETSI TS 128 537 [4] clause 7.3.1.

6.5.5.2 Requirements

Requirements specified in ETSI TS 128 537 [4] clause 7.3.3 shall apply.

6.5.5.3 Procedures

```
@startuml
skin rose
participant "File Management MnS Consumer" as consumer
participant "File Management MnS Producer" as producer
participant "file server" as fs
autonumber 1
consumer <--> producer: Establish NETCONF session
consumer --> producer: NETCONF <rpc><file-push><remote-file-path>
consumer <-- producer: NETCONF <rpc-reply><file-push><status>
consumer <--> producer: Terminate NETCONF session
producer --> fs: <<FTPeS, SFTP, HTTPS>> file push
opt progress notification desired
  loop for each progress update in file transfer
    producer -->consumer: <<HTTPS>> pushFile Event (progress)
  end
end
producer -->consumer: <<HTTPS>> pushFile Event (completion)
@enduml
```

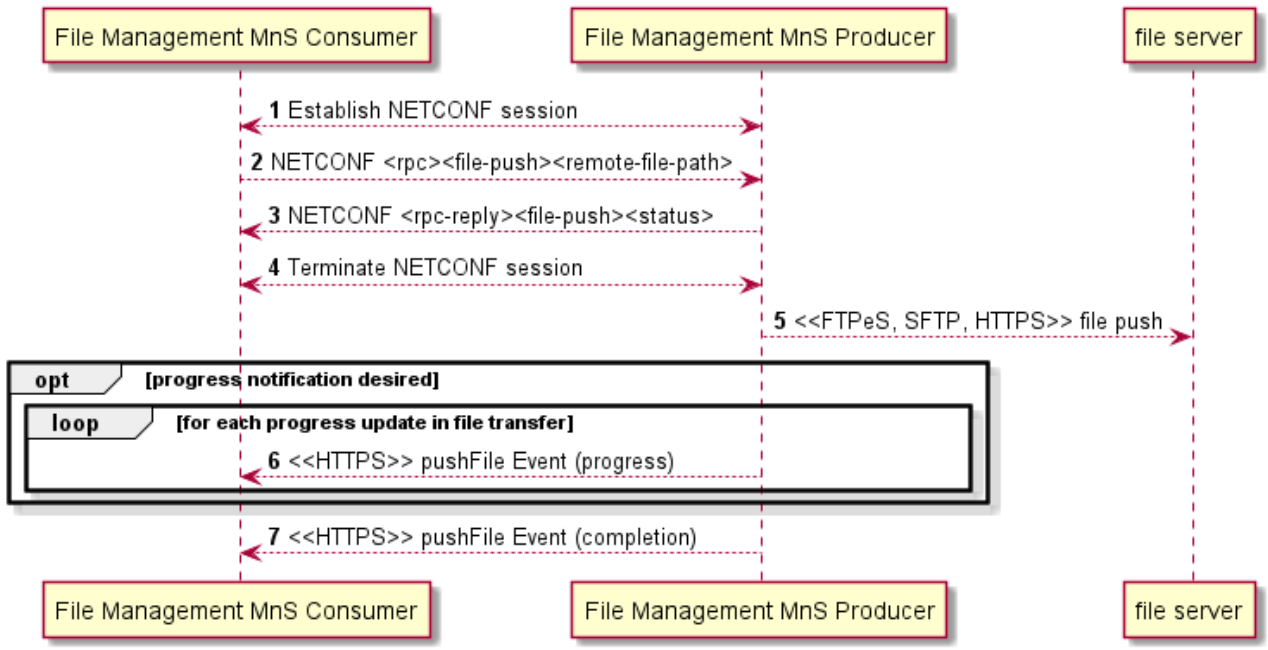

Figure 6.5.5.3-1: File Push

Procedure:

1) File Management MnS Consumer establishes NETCONF session with File Management MnS Provider.

2) File Management MnS Consumer sends NETCONF RPC file-push request, including the location of the file to download, to the File Management MnS Provider to trigger a file push.

3) File Management MnS Provider replies with its ability to begin the push.

4) File Management MnS Consumer terminates NETCONF session with File Management MnS Provider.

5) File Management MnS Provider sets up a secure connection and pushes the file via FTPeS, SFTP or HTTPS. SFTP is authenticated with username/password, SSH keys or X.509 certificates. FTPES is authenticated with X.509 certificates. HTTPS is mutually authenticated with X.509 certificates.

6) (Optional) File Management MnS Provider sends periodic pushFile notifications to the File Management MnS Consumer with the current status of the push (push in progress).

7) When push completes, File Management MnS Provider sends a pushFile notification to the File Management MnS Consumer with the final status of the push (success, file missing, failure).

6.5.5.4 Operations and Notifications

A File Pushed notification shall be in one of the following formats:

- SDO O1 format:
  - Either a 3GPP-specified notifyPush or an O-RAN-specified o1NotifyFilePush notification should be defined.
- VES O1 format:
  - A Harmonized VES event, as specified in the VES Event Listener Specification [18], containing stndDefinedFields with a "data" element that contains either a 3GPP-specified notifyFilePush or an O-RAN-specified o1NotifyFilePush notification.

6.6 Heartbeat Management Services

6.6.0 Overview

Heartbeat MnS allow a Heartbeat MnS Provider to send heartbeats to the Heartbeat MnS Consumer and allow the Heartbeat MnS Consumer to configure the heartbeat services on the Heartbeat MnS Provider.

Stage 1 Heartbeat MnS is specified in ETSI TS 128 537 [4]. This 3GPP specification is aligned with the Services Based Management Architecture (SBMA) approach defined in ETSI TS 128 533 [i.4], clause 4 and contains Use Cases, Requirements and Procedures for configuring the heartbeat period, reading the heartbeat period, triggering an immediate heartbeat notification and emitting a periodic heartbeat notification.

Stage 2 notifyHeartbeat notification is specified in ETSI TS 128 532 [3].

Stage 2 HeartbeatControl IOC is specified in ETSI TS 128 622 [7].

Stage 3 Solution Sets for XML, JSON and YANG are specified in ETSI TS 128 623 [23].

6.6.1 Heartbeat Notification

6.6.1.1 Description

Heartbeat MnS Provider sends asynchronous heartbeat notifications to Heartbeat MnS Consumer at a configurable frequency to allow Heartbeat MnS Consumer to supervise the connectivity to the Heartbeat MnS Provider.

6.6.1.2 Requirements

Requirements for heartbeat notifications specified in ETSI TS 128 537 [4], clause 4.2.2.2 shall apply.

6.6.1.3 Procedures

Procedures for heartbeat notifications are specified in ETSI TS 128 537 [4], clauses 4.3.2 and 4.3.3.

6.6.1.4 Operations and Notifications

A Heartbeat notification shall be in one of the following formats:

- SDO O1 format:
  - An O1-supported 3GPP-specified notifyHeartbeat notification, as specified in ETSI TS 128 532 [3].
- VES O1 format:
  - A Harmonized VES event, as specified in the VES Event Listener Specification [18], containing stndDefinedFields with a "data" element that contains an O1-supported 3GPP-specified notifyHeartbeat notification, as specified in ETSI TS 128 532 [3].

6.6.2 Heartbeat Control

6.6.2.1 Description

Starting with 3GPP Release 16, dedicated operations for Management Services Use Cases are supported by IOCs with attributes that can be read and/or set using generic provisioning mechanisms. For Heartbeat MnS, a Heartbeat Control IOC is specified in ETSI TS 128 622 [7] that includes attributes to Get/Set Heartbeat Period, (heartbeatNtfPeriod) and Trigger Immediate Heartbeat (triggerHeartbeatNtf).

6.6.2.2 Requirements

Requirements for heartbeat control specified in ETSI TS 128 537 [4], clause 4.2.2.1 shall apply.

HeartbeatControl IOC definition shall be as specified in ETSI TS 128 622 [7], clause 4.3.

YANG solution set for HeartbeatControl IOC shall be as in ETSI TS 128 623 [23], clause D.2.6a.

6.6.2.3 Procedures

Procedures for heartbeat control are specified in ETSI TS 128 537 [4], clauses 4.3.1 and 4.3.2.

NETCONF protocol and YANG data models are used to read and configure the heartbeatNtfPeriod and triggerHeartbeatNtf in the HeartbeatControl IOC. Refer to the Provisioning management services clause for procedures to read MOI attributes and modify MOI attributes using NETCONF.

6.6.2.4 Void

6.7 PNF Startup and Registration Management Services

6.7.0 Overview

PNF Startup and Registration management services allow a physical PNF Startup and Registration MnS Provider to acquire its network layer parameters either via static procedures (pre-configured in the element) or via dynamic procedures (Plug-n-Connect) during startup. During this process, the PNF Startup and Registration MnS Provider also acquires the IP address of the PNF Startup and Registration MnS Consumer for PNF Startup and Registration MnS Provider registration. Once the PNF Startup and Registration MnS Provider registers, the PNF Startup and Registration MnS Consumer can then bring the PNF Startup and Registration MnS Provider to an operational state.

Relevant 3GPP specifications for PNF Plug-n-Connect (PnC) are ETSI TS 128 314 (V17.0.0) [1], ETSI TS 128 315 [2] and ETSI TS 128 316 [i.2].

6.7.1 PNF Plug-n-Connect

6.7.1.1 Description

PNF Plug-n-Connect (PnC) scenario enables a PNF Startup and Registration MnS Provider to obtain the necessary start-up configuration to allow it to register with a PNF Startup and Registration MnS Consumer for subsequent management.

6.7.1.2 Requirements

Specification requirement for Plug and Connect specified in ETSI TS 128 314 [1], clause 6.2.1 shall apply.

6.7.1.3 Procedures

Functional elements involved in Plug and Connect Mns Service, for example, IP Autoconfiguration services, DNS server, Certification Authority server, Security gateway and Software and Configuration Server (SCS) are described in ETSI TS 128 315 [2], clause 4.2.

Plug-and-Connect and related procedures are specified in ETSI TS 128 315 [2], clause 5.

6.7.2 PNF Registration

6.7.2.1 Description

PNF Startup and Registration MnS Provider sends an asynchronous pnfRegistration or o1NotifyPNFRegistration event to a PNF Startup and Registration MnS Consumer after PnC to notify PNF Startup and Registration MnS Consumer of new PNF Startup and Registration MnS Provider to be managed.

6.7.2.2 Requirements

REQ-PNFR-FUN-1: The PNF Startup and Registration MnS Provider shall support sending the PNF Registration Notifications (see clause 6.7.2.4) upon PNF reset and/or registration events resulting in O1 connection re-establishment.

6.7.2.3 Procedures

PNF Registration procedures are illustrated by Figure 6.7.2.3-1.

```
@startuml
skin rose
Title PNF Registration Notification
Autonumber
participant "PNF Startup and Registration MnS Consumer" as NMS
participant " PNF Startup and Registration MnS Provider" as ME
Note over ME : PnC completes
ME ->> NMS : <<HTTP/TLS>> pnfRegistration or o1NotifyPNFRegistration Event
Note over NMS : Register PNF
@enduml
```

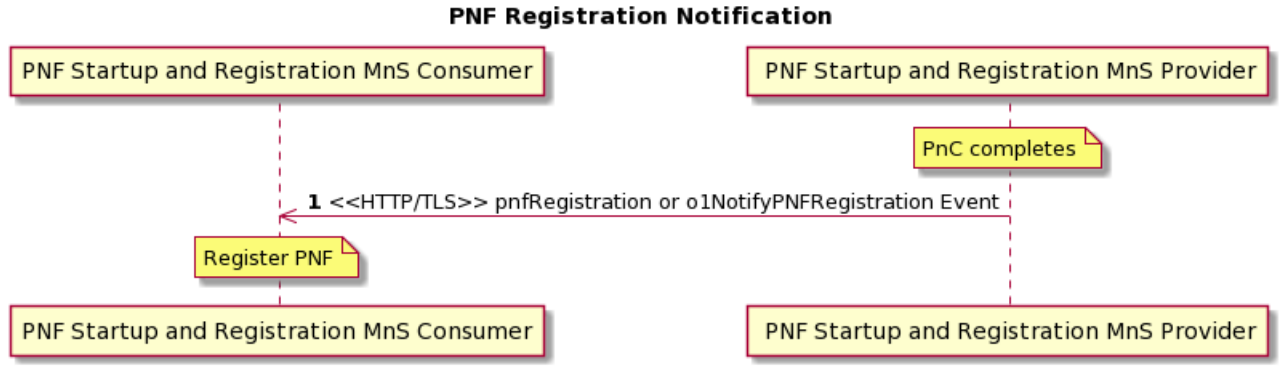

Figure 6.7.2.3-1: PNF Registration Notification

Pre-condition:

- PNF completes Plug-n-Connect.

Procedure:

1) PNF Startup and Registration MnS Provider sends pnfRegistration or o1NotifyPNFRegistration notification event to PNF Startup and Registration MnS Consumer over HTTP/TLS. Mutual certificate authentication is performed.

Post-condition:

- PNF Startup and Registration MnS Consumer registers the PNF Startup and Registration MnS Provider so that it can be managed.

6.7.2.4 Operations and Notifications

A PNF Registration notification can be either an o1NotifyPNFRegistration or a pnfRegistration event. They shall be in one of the following formats:

o1NotifyPNFRegistration:

- SDO O1 format:
  - The O-RAN-specified o1NotifyPnfRegistration notification defined in Table 6.7.2.4-1.

Table 6.7.2.4-1

Parameter Name	S	Information Type	Comment
objectClass	M	ManagedEntity.objectClass	Class of the managed object, registering for service.
objectInstance	M	ManagedEntity.objectInstance	Instance of the managed object, registering for service.
notificationId	M	NotificationId	Notification identifier as defined in Recommendation ITU-T X.733 [i.18]
notificationType	M	"o1notifyPnfRegistration"	
eventTime	M	DateTime	Time when the NF is sending the registration.
systemDN	M	SystemDN	DN of the MnS provider of the notification
o1SpecVersion	M	number	Version of the O1 Specification defining the format of this PNF registration notification
serialNumber	M	string	ETSI TS 128 632 [i.7] serialNumber = serial number of the unit
vendorName	M	string	ETSI TS 128 632 [i.7] vendorName = name of the NF vendor.
oamV4IpAddress	CM	string	IPv4 m-plane IP address to be used by the manager to contact the NF.
oamV6IpAddress	CM	string	IPv6 m-plane IP address to be used by the manager to contact the NF.
macAddress	O	string	MAC address of the OAM of the unit
unitFamily	O	string	ETSI TS 128 632 [i.7] vendorUnitFamilyType = general type of HW unit
unitType	O	string	ETSI TS 128 632 [i.7] vendorUnitTypeNumber = vendor name for the unit
modelNumber	O	string	ETSI TS 128 632 [i.7] versionNumber = version of the unit from the vendor
softwareVersion	O	string	ETSI TS 128 632 [i.7] swName = software release name. This is the software provided by the vendor at onboarding to be run on this version of the NF and can contain multiple underlying software images.
restartReason	O	string	Reason the NF restarted, if known
manufactureDate	O	string	ETSI TS 128 632 [i.7] dateOfManufacture = manufacture date of the unit; e.g. 2016-04-23
lastServiceDate	O	string	ETSI TS 128 632 [i.7] dateOfLastService = date of last service; e.g. 2017-02-15
additionalFields	O	hashMap	Additional registration fields if needed, provided as key-value pairs.
CM: Either oamV4IpAddress or oamV6IpAddress shall be provided depending upon what the network function supports.			

NOTE: Table 6.7.2.4-1 describes the content of o1NotifyPnfRegistration may be revised when the IM/DM work (capturing the notification details) is complete.

- VES O1 format:
  - A Harmonized VES event, as specified in the VES Event Listener Specification [18], containing stndDefinedFields with a "data" element that contains an O-RAN-specified o1NotifyPnfRegistration notification.

pnfRegistration:

- VES O1 format:
  - A legacy pnfRegistration VES event, as specified in the VES Event Listener Specification [18].

6.8 PNF Software Management Services

6.8.0 Overview

Software management services allow a PNF Software MnS Consumer to request a physical PNF Software MnS Provider to download, install, validate and activate a new software package and allow a physical PNF Software MnS Provider to report its software versions.

6.8.1 Software Package Naming and Content

PNF Software Package naming, content and format are vendor specific and do not require standardization in O-RAN. A PNF Software Package contains one or more files. Some of the files in the Software Package are optional for the PNF (example: a file that has not changed version). The PNF is aware of the content and format of its available Software Packages and can determine which files it needs to download.

The softwarePackage Managed Object Class (MOC) contains attributes about a software package such as:

- software package name, version;
- fileList;
- integrityStatus (valid, invalid, empty);
- runningState (active, passive);
- vendor;
- productName;
- softwareType (operational, factory);
- etc.

This MOC is applicable to VNFs and PNFs and is a generic term that O-RAN will use to refer to the software available on the PNF rather than the legacy term of software slot.

The PNF creates one instance of softwarePackage for each software package supported concurrently on the PNF. Typically, a PNF will have two softwarePackage MOIs for operational software; one with runningState = active and one with runningState = passive. Some PNFs also have a softwarePackage MOI for the factory software which would be read only. O-RAN can have PNFs that support more than one passive slot. In this case the inventory query result would show multiple MOIs with runningState=passive.

6.8.2 Software Inventory

6.8.2.1 Description

The PNF Startup and Registration MnS Consumer sends a Software Inventory Request and retrieves information about the software packages on the PNF Software MnS Provider.

6.8.2.2 Requirements

REQ-SWI-FUN-1: The PNF software management service provider shall have the capability to provide its authorized consumer information about the software packages on the PNF software management service provider.

6.8.2.3 Procedures

```
@startuml
Title Software Inventory
autonumber "[0]"
participant "PNF Software MnS Consumer" as NMS
participant "PNF Software MnS Provider" as ME
NMS <-> ME : Establish NETCONF Session
NMS -> ME: NETCONF <rpc> <get><filter>
Note over ME : Retrieve Software Inventory Information
ME --> NMS: NETCONF <rpc-reply> <data>
NMS <-> ME : Terminate NETCONF Session
@enduml
```

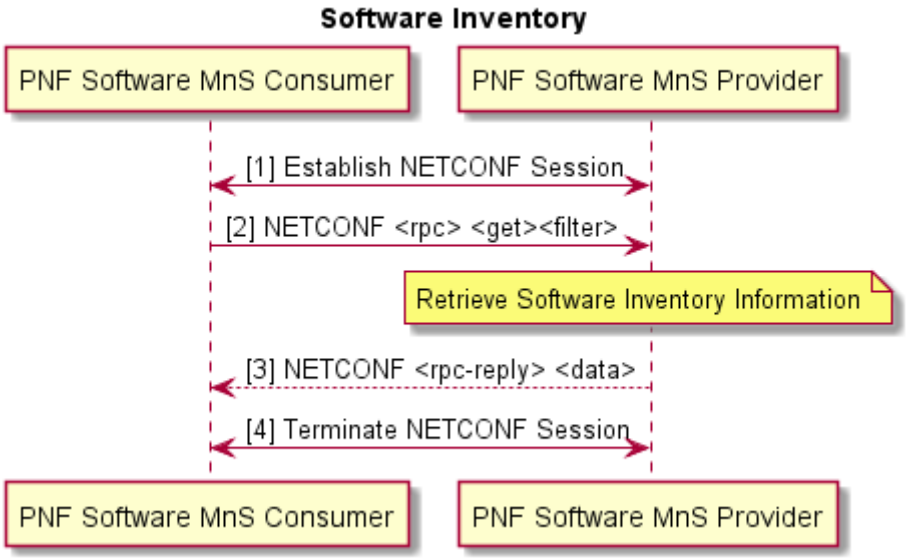

Figure 6.8.2.3-1: Software Inventory

Procedure:

1) PNF Software MnS Consumer establishes NETCONF session with PNF Software MnS Provider. The NETCONF session has authorized read privileges into the identified section of the data store.

2) PNF Software MnS Consumer sends NETCONF <rpc> <get><filter> to retrieve an optionally filtered subset configuration from the running configuration datastore. <filter> can be used to identify the software package MOIs. GET retrieves configuration and operational state of softwarePackage MOIs:

   a) PNF Software MnS Provider retrieves software inventory information.

3) PNF Software MnS Provider returns requested data in NETCONF <rpc-reply> response.

4) PNF Software MnS Consumer terminates NETCONF session with PNF Software MnS Provider.

6.8.3 Software Download

6.8.3.1 Description

Software Download triggers the download of a specific software package to the PNF Software MnS Provider. This download service includes integrity checks on the downloaded software and the installation of the software into the software slot corresponding to the softwarePackage MOI.

6.8.3.2 Requirements

REQ-SWD-FUN-1: The PNF software management service provider shall have the capability to allow its authorized consumer to specify the location of software that is to be downloaded and to specify into which softwarePackage the software is to be stored.

REQ-SWD-FUN-2: The PNF software management service provider shall have the capability to verify if a software download is in progress and the ability to reject subsequent download commands until the one in progress completes.

REQ-SWD-FUN-3: The PNF software management service provider shall have the capability to deny download of software if the download request is not valid for the PNF software management service provider.

REQ-SWD-FUN-4: The PNF software management service provider shall have the capability to download needed files from a software server at a specified location.

REQ-SWD-FUN-5: The PNF software management service provider shall have the capability to perform integrity checks on downloaded software.

REQ-SWD-FUN-6: The PNF software management service provider shall have the capability to notify the PNF software management consumer with the software download result.

6.8.3.3 Procedures

```
@startuml
skin rose
Title Software Download
autonumber "[0]"
participant "PNF Software MnS Consumer" as NMS
participant "PNF Software MnS Provider" as ME
participant "Software Server" as SWS
NMS <-> ME : Establish NETCONF Session
NMS -> ME: NETCONF <rpc><software-download><remote-file-path><softwarePackage>
Note over ME : Validate Request
ME --> NMS: NETCONF <rpc-reply><software-download-status>
NMS <-> ME : Terminate NETCONF Session
ME -> SWS : <<FTPeS, SFTP or HTTPS>> file download
Note over ME : Integrity check SW
Note over ME : Store SW in a persistent location
Note over ME : Update softwarePackage
Opt Download Progress Notifications
ME ->> NMS : <<HTTP/TLS>> downloadFile Event
End
|||
ME ->> NMS : <<HTTP/TLS>> downloadFile Event
@enduml
```

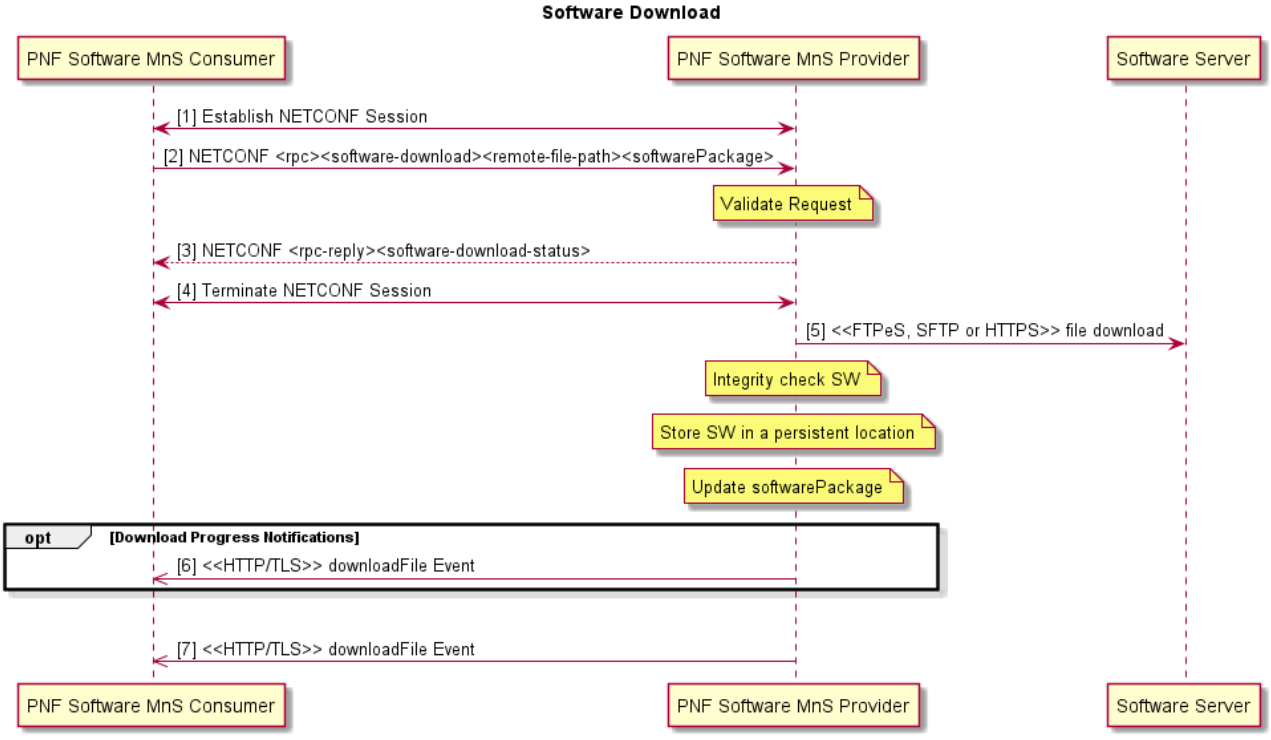

Figure 6.8.3.3-1: Software Download

Procedure:

1) PNF Software MnS Consumer establishes NETCONF session with PNF Software MnS Provider. The NETCONF session has authorized execution privileges for retrieve file list and file-download rpcs.

2) PNF Software MnS Consumer sends NETCONF <rpc><software-download><remote-file-path><softwarePackage> to trigger a download of the software located at remoteFilePath and save its information in softwarePackage:

   a) PNF Software MnS Provider validates the request. Validation includes determining if the operation can be performed. This is PNF Software MnS Provider specific but could include things like: checking that there is not a software download already in progress, softwarePackage is runningState = passive and softwareType = operational, etc.

3) PNF Software MnS Provider returns NETCONF <rpc-reply><software-download-status>.

4) PNF Software MnS Consumer terminates NETCONF session with PNF Software MnS Provider.

5) PNF Software MnS Provider initiates SFTP, FTPES or HTTPS connection and downloads the software package from remoteFilePath. SFTP is authenticated with username/password, SSH keys or X.509 certificates. FTPES is authenticated with X.509 certificates. HTTPS is mutually authenticated with X.509 certificates. PNF Software MnS Provider understands the software package format and downloads all the files it needs from the package. PNF Software MnS Provider decides where to store the software internally. This is PNF Software MnS Provider specific but could be a temporary location like /tmp:

   a) PNF Software MnS Provider integrity checks the downloaded software. This is PNF Software MnS Provider specific but could include checking-checksum, correct software for the hardware, etc.

   b) PNF Software MnS Provider stores the software in a persistent location.

   c) PNF Software MnS Provider updates softwarePackage attributes for the downloaded software.

6) (Optional) If the download takes a long time, PNF Software MnS Provider may send periodic downloadFile notifications to the PNF Software MnS Consumer with the current status of the download (download in progress, integrity checks passed, install complete).

7) When download operation completes, PNF Software MnS Provider sends downloadFile event notification to PNF Software MnS Consumer with the final status of the download (success or the reason for failure).

6.8.3.4 Operations and Notifications

A File Download notification shall be in one of the following formats:

- SDO O1 format:
  - Either a 3GPP-specified notifyFileDownload or a O-RAN-specified o1NotifyFileDownload notification should be defined.
- VES O1 format:
  - A Harmonized VES event, as specified in the VES Event Listener Specification [18], containing stndDefinedFields with a "data" element that contains either a 3GPP-specified notifyFileDownload or a O-RAN-specified o1NotifyFileDownload notification.

6.8.4 Software Activation Pre-Check

6.8.4.1 Description

Activation Pre-check is an optional Use Case that the Service Provider can choose to utilize prior to software activation to confirm that the PNF Software MnS Provider is in a good state to activate the new software and provide information needed for planning the timing of the software replacement--such as whether a reset or a data migration is required.

6.8.4.2 Requirements

REQ-SPC-FUN-1: The PNF software management service provider shall have the capability to confirm that the software in the passive slot targeted for activation is good.

REQ-SPC-FUN-2: The PNF software management service provider shall have the capability to determine whether the activation of the targeted software requires a reset and/or data migration.

6.8.4.3 Procedures

```
@startuml
Title Activation Pre-Check
autonumber "[0]"
participant "PNF Software MnS Consumer" as NMS
participant "PNF Software MnS Provider" as ME
NMS <-> ME : Establish NETCONF Session
NMS -> ME: NETCONF <rpc><activation-pre-check><softwarePackage>
Note over ME : Perform Pre-Check
ME --> NMS: NETCONF <rpc-reply> <data>
NMS <-> ME : Terminate NETCONF Session
@enduml
```

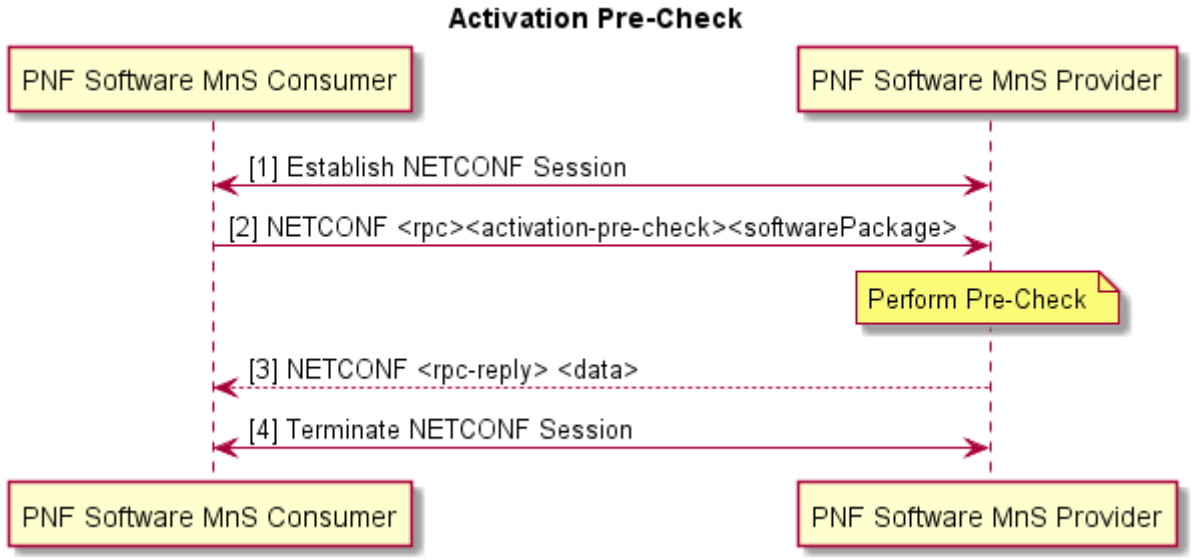

Figure 6.8.4.3-1: Software Activation Pre-Check

Procedure:

1) PNF Software MnS Consumer establishes NETCONF session with PNF Software MnS Provider.

2) PNF Software MnS Consumer sends NETCONF <rpc><activation-pre-check><softwarePackage> to trigger a pre-check of the software stored in softwarePackage and to return the results of the pre-check:

   a) PNF Software MnS Provider performs the activation pre-check which includes validating that the software in softwarePackage is good, whether the activation of the software in softwarePackage will result in a reset and whether data migration is needed, etc.

3) PNF Software MnS Provider returns NETCONF <rpc-reply> to the PNF Software MnS Consumer with the results of the pre-check.

4) PNF Software MnS Consumer terminates NETCONF session with PNF Software MnS Provider.

6.8.5 Software Activate

6.8.5.1 Description

PNF Software MnS Consumer triggers the activation of a software package on the PNF Software MnS Provider including data migration and reset if needed.

6.8.5.2 Requirements

REQ-SWA-FUN-1: The PNF software management service provider shall have the capability to allow its authorized consumer to activate valid software in a specific softwarePackage.

REQ-SWA-FUN-2: The PNF software management service provider shall have the capability to verify whether a software activation is in progress and deny a concurrent activation of software.

REQ-SWA-FUN-3: The PNF software management service provider shall have the capability to deny activation of software if the activation request is not valid for the PNF software management service provider.

REQ-SWA-FUN-4: The PNF software management service provider shall have the capability to activate the softwarePackage.

REQ-SWA-FUN-5: The PNF software management service provider shall have the capability to reset the PNF software management service provider if the software activation requires it.

REQ-SWA-FUN-6: The PNF software management service provider shall provide the capability for the PNF software management service provider to send a re-set reason notification to its authorized consumer if the activation results in a reset.

REQ-SWA-FUN-7: The PNF software management service provider shall have the capability to perform data migration on the PNF software management service provider if the software activation requires it.

REQ-SWA-FUN-8: The PNF software management service provider shall have the capability to fallback to the previously active software if the new software cannot be activated.

REQ-SWA-FUN-9: The PNF software management service provider shall have the capability to fallback to the factory software if the new and the previously active software can not be activated.

6.8.5.3 Procedures

```
@startuml
Title Software Activate
autonumber "[0]"
participant "PNF Software MnS Consumer" as NMS
participant "PNF Software MnS Provider" as ME
NMS <-> ME : Establish NETCONF Session
NMS -> ME: NETCONF <rpc><software-activate><softwarePackage>
Note over ME : Validate request
ME --> NMS: NETCONF <rpc-reply> <status>
NMS <-> ME : Terminate NETCONF Session
Note over ME : Activate Software
Alt if Data Migration or Reset are needed then
Alt if Data Migration Needed then
Note over ME : Migrate Data if needed
|||
End
Alt if Reset Needed then
Note over ME : Reset
ME ->> NMS : <<HTTP/TLS>> resetReason Event
|||
End
|||
End
Alt if Activation fails then
Note over ME : Fallback if failure
|||
End
Opt Activation Progress Notifications
ME ->> NMS : <<HTTP/TLS>> softwareActivate Event
End
|||
ME ->> NMS : <<HTTP/TLS>> softwareActivate Event
Note over ME : Config change occurs
ME ->> NMS : <<HTTP/TLS>> notifyMOIAttributeValueChange Event
Note over NMS : Reconcile Database
@enduml
```

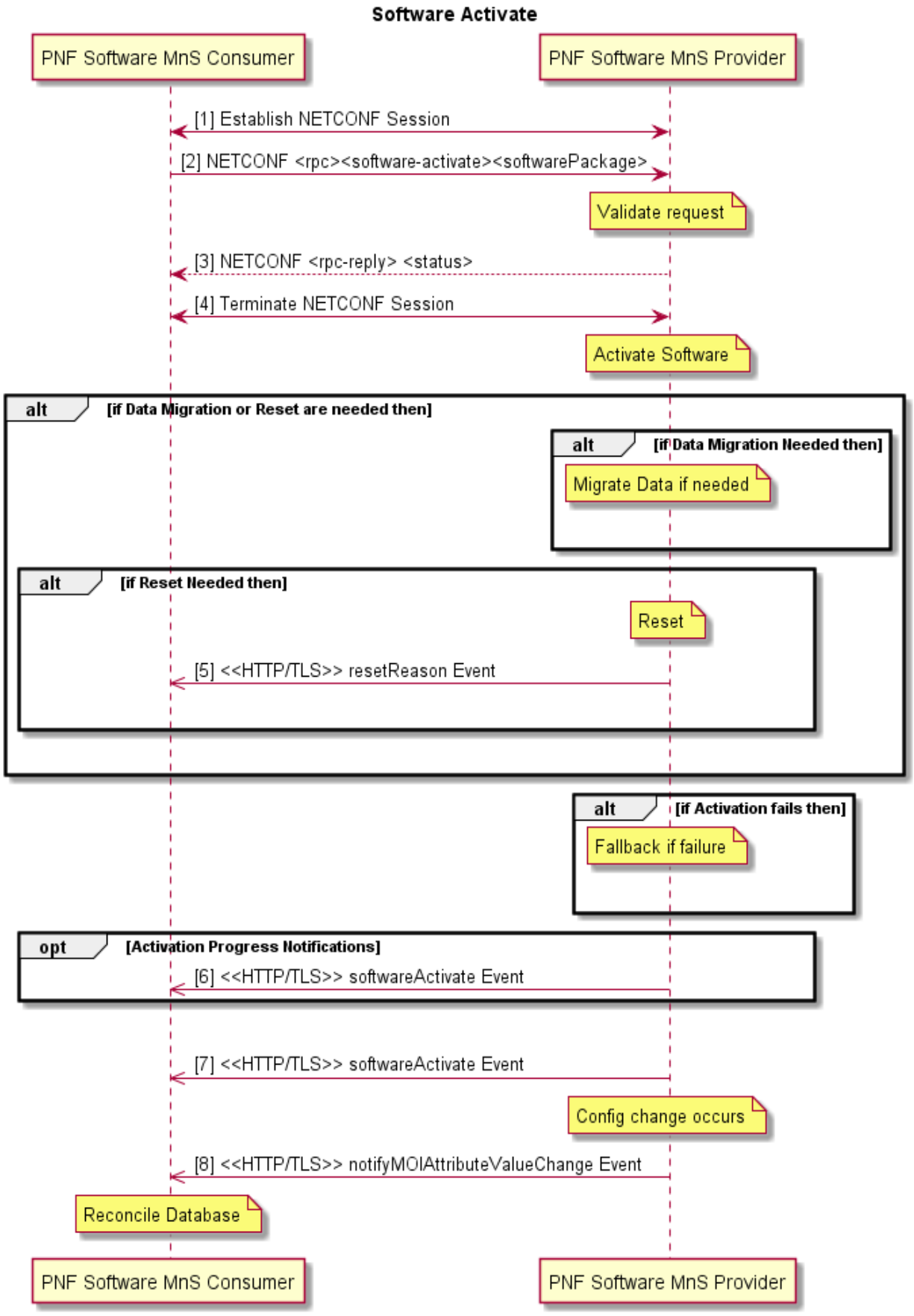

Figure 6.8.5.3-1: Activate Software

Procedure:

1) PNF Software MnS Consumer establishes NETCONF session with PNF Software MnS Provider.

2) PNF Software MnS Consumer sends NETCONF <rpc><software-activate><softwarePackage> to trigger an activation of the software in softwarePackage:

   a) PNF Software MnS Provider validates the request. This is PNF Software MnS Provider specific but could include things like checking that there is not a software activation already in progress, softwarePackage is runningState = passive and integrityStatus = valid, etc.

3) PNF Software MnS Provider returns status to the PNF Software MnS Consumer in the NETCONF <rpc-reply> response:

   a) PNF Software MnS Provider performs the steps needed to make the softwarePackage the active one. This is PNF Software MnS Provider specific but includes things like updating the runningState of the about-to-be-active and previously-active software packages.

4) PNF Software MnS Consumer terminates NETCONF session with PNF Software MnS Provider.

   (Optional) PNF Software MnS Provider performs data migration if necessary. PNF Software MnS Provider knows whether this is necessary.

5) (Optional) PNF Software MnS Provider performs reset if necessary. PNF Software MnS Provider knows whether reset is necessary. If a reset occurs, PNF Software MnS Provider sends a resetReason notification to the PNF Software MnS Consumer with the reason for the reset; in this case software activation.

   (Optional) If the PNF Software MnS Provider can not activate the software, PNF Software MnS Provider has recovery logic to fallback to the previously active software and potentially fallback to the factory software in a worst-case scenario.

6) (Optional) If the activation takes a long time, PNF Software MnS Provider sends periodic softwareActivate notifications to PNF Software MnS Consumer with the current status of the activation (e.g. activation in progress, data migration successful).

7) After activation operation completes, PNF Software MnS Provider sends a softwareActivate notification to PNF Software MnS Consumer with the final status of the activation.

8) PNF Software MnS Provider sends notifyMOIAttributeValueChange to the PNF MnS Consumer updating the active software running on the PNF.

6.8.5.4 Operations and Notifications

A Software Activate notification shall be in one of the following formats:

- SDO O1 format:
  - Either a 3GPP-specified notifySoftwareActivate or an O-RAN-specified o1NotifySoftwareActivate notification should be defined.
- VES O1 format:
  - A Harmonized VES event, as specified in the VES Event Listener Specification [18], containing stndDefinedFields with a "data" element that contains either a 3GPP-specified notifySoftwareActivate or an O-RAN-specified o1NotifySoftwareActivate notification.

6.9 PNF Reset Management Services

6.9.0 Overview

PNF Reset Management Services allow a PNF Reset MnS Consumer to trigger a reset of a HW unit of a PNF Reset MnS Provider on command.

6.9.1 PNF Reset Command

6.9.1.1 Description

The PNF Reset Command procedure allows a PNF Reset MnS Consumer to trigger a reset of a HW unit of a PNF Reset MnS Provider on command. Any HW unit that is resettable via a reset command is represented by a Managed Object Instance (MOI) and is able to be identified by a Distinguished Name (DN). The NETCONF RPC <reset> command identifies the unit to reset by the DN. The unit to reset can be the entire PNF or a resettable HW subcomponent of the PNF. A resettable HW subcomponent of a PNF is a subcomponent of a PNF that is able to be independently reset and whose PNF Reset MnS Provider supports a reset command for the subcomponent. It is vendor and PNF-specific whether a PNF has resettable HW subcomponents. The reset command also has an attribute to identify the type of reset requested. The types of reset commands that a PNF supports are vendor and PNF specific. O-RAN O1 Interface Specification specifies two mandatory reset command types that every PNF supports: conditional and forced. A conditional reset command can be rejected by the PNF Reset MnS Provider depending on the conditions on the PNF, for example if the unit to reset is not in a proper state to reset, such as, if there is an emergency call in progress on the unit. A valid forced reset command cannot be rejected. Valid means that the unit to reset supports a reset command. Invalid forced resets will be rejected, for example, if the unit to reset is not a resettable HW unit, such as a cell. Vendors are allowed to extend the O1 specified reset command types to add vendor and PNF specific reset command types.

6.9.1.2 Requirements

REQ-RM-FUN-1: The PNF Reset MnS Provider shall support the capability for a PNF Reset MnS Consumer to trigger a reset of a HW unit of the PNF Reset MnS Provider on command.

REQ-RM-FUN-2: The PNF Reset MnS Provider shall support reset command types conditional and forced.

REQ-RM-FUN-3: The PNF Reset MnS Provider shall be allowed to reject a conditional reset command type.

NOTE 1: The validations performed and the reasons for a conditional reset rejection, if any, are vendor and PNF specific.

REQ-RM-FUN-4: The PNF Reset MnS Provider shall not be allowed to reject a valid forced command reset type.

NOTE 2: Valid means that the unit to reset supports a reset command. Invalid forced resets will be rejected, for example, if the unit to reset is not a resettable HW unit, such as a cell.

6.9.1.3 Procedures

This procedure shows how a PNF Reset MnS Consumer triggers a reset of a HW unit of a PNF Reset MnS Provider on command. The HW unit to reset is identified by the <unitToReset> input attribute. The type of reset command is identified by the <resetCommandType> input attribute. The <status> output attribute returned in the NETCONF response indicates whether the reset command has been accepted. The unit is reset after the NETCONF response is returned. The reason for the reset (e.g. conditional reset command or forced reset command) is persistently stored by PNF Reset MnS Provider before executing the reset.

```
@startuml
Title PNF Reset Command
participant "PNF Reset MnS Consumer" as NMS
participant " PNF Reset MnS Provider" as ME
NMS -> ME: 1 NETCONF <rpc><reset><unitToReset><resetCommandType>
Note over ME : 2 Validate command \n   Save reset reason
ME --> NMS: 3 NETCONF <rpc-reply><reset><status>
Note over ME : 4 Reset unit
@enduml
```

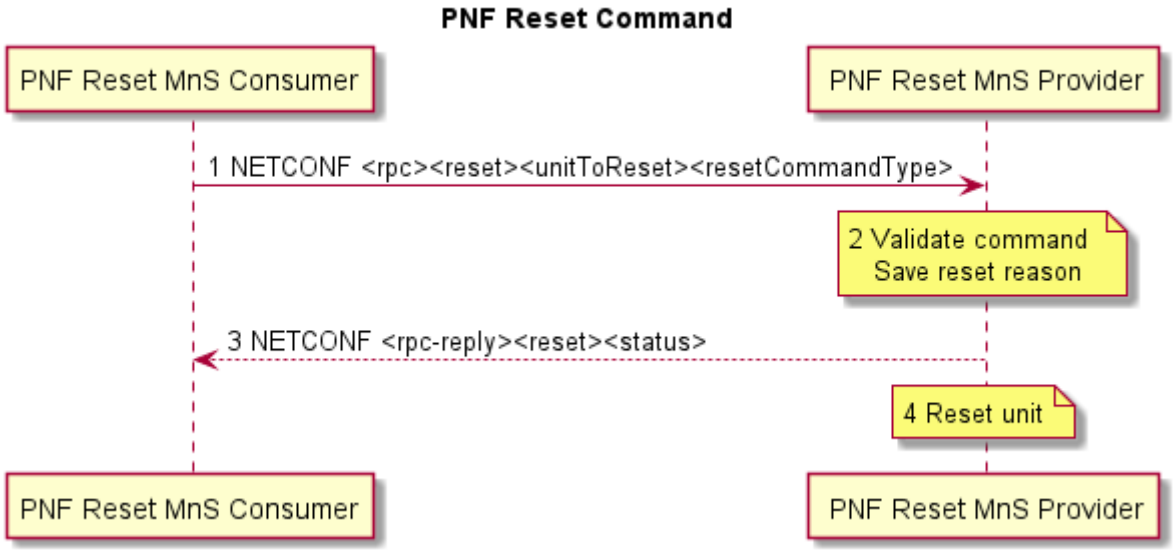

Figure 6.9.1.3-1: PNF Reset Command

Pre-conditions:

- PNF Reset MnS Consumer has established a NETCONF session to the PNF Reset MnS Provider as specified in Provisioning Management Services, clause 6.1.8. The NETCONF session has authorized execution privileges for <reset> RPC.
- (Optionally) PNF Reset MnS Consumer has locked the appropriate DS of the PNF Reset MnS Provider as specified in Provisioning Management Services, clause 6.1.10.

Procedure:

1) PNF Reset MnS Consumer sends NETCONF <rpc> <reset> <unitToReset><resetCommandType> to PNF Reset MnS Provider, indicating the unit to reset and the type of reset command.
2) PNF Reset MnS Provider validates the command. Validation is vendor and PNF specific but typically includes verifying that the <unitToReset> is resettable and can be reset at this time. A conditional reset command type allows the PNF Reset MnS Provider to reject the reset command, depending on the conditions on the PNF, for example if an emergency call is in progress. The conditions are vendor and PNF specific. A valid forced reset command type cannot be rejected. Valid means that the unit to reset supports a reset command. Invalid forced resets will be rejected, for example if the unit to reset is not a resettable HW unit, such as a cell. If the reset command is accepted, the reset reason (e.g. conditional reset command or forced reset command) is stored persistently on the PNF Reset MnS Provider.
3) PNF Reset MnS Provider responds, indicating in the <status> attribute whether the command is accepted. If the command is rejected, the <rpc-reply> contains an <rpc-error> element with the reason for the rejection.
4) Unit is reset.

Post-conditions:

- (Optionally) PNF Reset MnS Consumer unlocks the DS of the PNF Reset MnS Provider after sending the reset command, as specified in Provisioning Management Services, clause 6.1.11.
- (Optionally) PNF Reset MnS Consumer terminates the NETCONF session to the PNF Reset MnS Provider after sending the reset command, as specified in Provisioning Management Services, clause 6.1.9.

6.9.1.4 Operations

Information Model and YANG solution set for the NETCONF RPC <reset> command and its attributes will be specified in the O-RAN Information Model and Data Models Specification [i.14].

6.9.2 Notifications

REQ-RN-FUN-1: A PNF MnS Provider shall support the capability to inform a PNF MnS Consumer that a reset has occurred and the reason that a HW unit has reset.

REQ-RN-FUN-2: A PNF MnS Provider shall save the reason for a reset persistently before resetting.

NOTE 1: This requirement applies to resets that occur under the control of the PNF.

REQ-RN-FUN-3: If a reset reason has not been saved persistently, the PNF MnS Provider shall set the reset reason to unknown in the notification.

NOTE 2: This requirement applies to resets that occur unexpectedly before the reset reason could be stored.

6.10 Cloudified NF Registration Management Service

6.10.0 Overview

The Cloudified NF Registration Management Service supports the registration of a Cloudified NF Registration Management Service Provider to the Cloudified NF Registration Management Service Consumer after the Cloudified NF instantiation via the O2 has completed and the NF application has initialized and is ready for final configuration and management (e.g. ready to be put in service). Application initialization includes things like setting up the NETCONF server, creating MOIs for the NF, and perhaps some vendor specific steps which can take place after the Cloudified NF instantiation completes. The Cloudified NF Registration MnS is applicable to VNFs and CNFs and supports the NF informing the SMO when it has completed its initialization steps and is ready to be managed. Without this service, the SMO would have to poll the NF until the NF responded that it had completed its application initialization and was ready for final configuration (if needed) and management. Registration is accomplished by sending a Cloudified NF Registration notification.

6.10.1 Cloudified NF Registration Notification

6.10.1.1 Description

To register, the Cloudified NF Registration MnS Provider sends an asynchronous o1NotifyCloudNFRegistration event to a Cloudified NF Registration MnS Consumer to notify the Cloudified NF Registration MnS Consumer of a new Cloudified NF Registration MnS Provider to be managed. The Cloudified NF Registration Provider will periodically send the o1NotifyCloudNFRegistration event (at vendor specified intervals) until a NETCONF session is established. This indicates that the Cloudified NF Registration MnS Provider has registered, and the Cloudified NF Registration MnS Consumer can begin managing the Cloudified NF Registration MnS Provider and bring the Cloudified NF Registration MnS Provider to an operational state.

NOTE: The o1NotifyCloudNFRegistration notification does not require a subscription. It is sent after the application comes up if a Cloudified NF Registration MnS Consumer address (e.g. IP@ or FQDN) is obtained during instantiation or is pre-provisioned. The o1NotifyCloudNFRegistration notification is also sent after a restart for the VNF/CNF.

6.10.1.2 Requirements

REQ-CNFR-FUN-1: The Cloudified NF Registration MnS Provider shall support the capability to send a o1NotifyCloudNFRegistration notification to the Cloudified NF Registration MnS Consumer when it has completed instantiation and application initialization and is ready for final configuration and to be managed by the Cloudified NF Registration MnS Consumer.

REQ-CNFR-FUN-2: The Cloudified NF Registration MnS Provider shall support the capability to send a o1NotifyCloudNFRegistration notification to the Cloudified NF Registration MnS Consumer when it completes a restart.

6.10.1.3 Procedures

The Cloudified NF Registration MnS Provider sends an asynchronous HTTP/TLS o1NotifyCloudNFRegistration notification to the Cloudified NF Registration MnS Consumer after it has been instantiated via the O2 interface, completed application initialization and is ready for final configuration and to be managed (put into service).

```
@startuml
Title Cloudified NF Registration
participant "Cloudified NF Registration MnS Consumer" as NMS
participant "Cloudified NF Registration MnS Provider" as ME
Note over ME : NF has completed instantiation and application initialization and is ready to be
managed
ME ->> NMS : 1 <<HTTP/TLS>> o1NotifyCloudNFRegistration Notification
@enduml
```

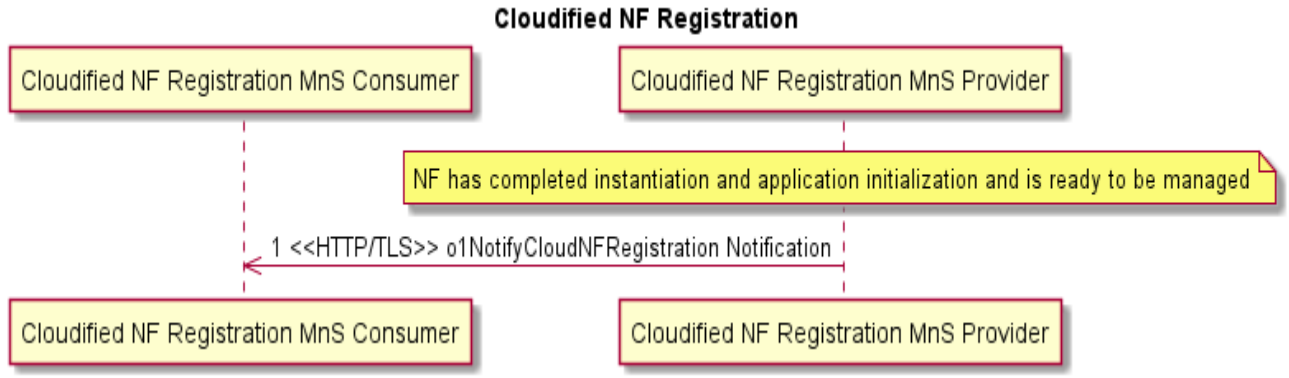

Figure 6.10.1.3-1: Cloudified NF Registration Procedure

Pre-condition:

- NF has been instantiated via the O2.
- Cloudified NF Registration MnS Consumer address is obtained during instantiation or is pre-provisioned.
- Cloudified NF Registration MnS Provider has completed application initialization and is ready to be managed.

Procedure:

1) Cloudified NF Registration MnS Provider sends o1NotifyCloudNFRegistration notification to Cloudified NF Registration MnS Consumer over HTTP/TLS. Mutual certificate authentication is performed.

6.10.1.4 Operations and Notifications

A Cloudified NF Registration notification shall be in one of the following formats:

- SDO O1 format:
  - An O-RAN-specified o1NotifyCloudNFRegistration notification as will be specified in the O-RAN Information Model and Data Models Specification [i.14].
- VES O1 format:
  - A Harmonized VES event, as specified in the VES Event Listener Specification [18], containing stndDefinedFields with a "data" element that contains an O-RAN-specified o1NotifyCloudNFRegistration notification.

Annex A (informative): O-RAN Performance Measurement Definition Example

A.1 ETSI TS 132 404 PM Template Usage in O-RAN

A.1.0 Overview

Examples are presented below to illustrate how to use the ETSI TS 132 404 [10], clause 3.3 template or template required information to specify O-RAN defined O1 compliant performance measurements. The O-RAN defined O1 compliant performance measurement will be defined using this template and documented in the appropriate O1 Interface Specification, e.g. O1 Interface Specification for Near-RT RIC [i.10], O1 Interface Specification for O-CU-UP and O-CU-CP [i.11] and O1 Interface Specification for O-DU [i.12].

NOTE: This PM template applies to O1 complaint nodes, specifically Near-RT RIC, O-CU-CP, O-CU-UP and O-DU.

The MF-specific O1 Interface Specifications will contain a template similar to clause A.1.1.1 for each counter defined and that these tables will be part of the official documentation.

There are three scenarios when O-RAN defines its own measurement or extends other SDO, for example, 3GPP specified measurement:

1) O-RAN defines a new measurement:

   a) Measurement Name follows the guidance of ETSI TS 132 404 [10], clause 3.3, is descriptive and begins with "OR". For example, "OR O-DU counter UL…".

   b) Measurement Type follows the guidance of ETSI TS 132 404 [10], clause 3.3 and in addition has "OR." prefix. For example, in format of OR.RLC.xxxx.

2) O-RAN extends the definition of an existing 3GPP measurement which does not have subcounter defined:

   a) A new O-RAN measurement needs to be defined.

   b) For example, A.1.3 Example 3 O-RAN extends 3GPP measurement "UL Total PRB Usage" is given.

3) O-RAN defines new subcounters to an existing 3GPP measurement which has subcounters defined:

   a) A new O-RAN measurement needs to be defined.

   b) Existing filters (or called additional items in ETSI TS 132 404 [10], clause 3.3) for a 3GPP measurement that the new O-RAN measurement is based on, can be re-defined in the new O-RAN measurement's Measurement Type. This enables supporting of combination of existing filters and the new filter.

A.1.1 Example 1 O-DU counter UL PDCP PDUs transmitted via F1-U UL GTP-U tunnel

A.1.1.1 PM Template

Measurement Name	OR UL PDCP PDUs transmitted via F1-U
Description	This counter provides the number of the UL PDCP PDUs transmitted via F1-U UL GTP-U tunnel It is optional counter for O-DU
Collection Method	CC (Cumulative Counter)
Condition	Measurement subcounter is incremented by 1 whenever the UL PDCP PDU is transmitted via F1 U UL GTP-u tunnel when the QCI of the UL PDCP PDU is group of subcounter.*Pmgroup*
Measurement Result	Integer number (U32)
Measurement Type	OR.F1.UlPdcpPduTxF1UUl.*Pmgroup* where *PmGroup* is PmCountGroup number: 0: #0 1: #1 … 19: #19
Measurement Object Class	gNBDUFunction
Switching Technology	Packet Switched
Generation	5GS
Purpose	Network Operator's Traffic Engineering Community

A.1.2 Example 2 O-DU counter Received UL RLC PDU volume

A.1.2.1 PM Template

Measurement Name	OR received UL RLC PDU Vol
Description	This counter provides the received UL RLC PDU volume It is recommended to support for O-DU
Collection Method	SI (Status Inspection)
Condition	Measurement subcounter is incremented by the volume of the UL RLC PDU whenever the UL RLC PDU is received when the QCI of the UL RLC PDU is group of subcounter.*Pmgroup*
Measurement Result	kilobyte (U32)
Measurement Type	OR.RLC.RxUlRlcPduVol.*Pmgroup* where *Pmgroup* is PmCountGroup number: 0: #0 1: #1 … 19: #19
Measurement Object Class	gNBDUFuncton
Switching Technology	Packet Switched
Generation	5GS
Purpose	Network Operator's Traffic Engineering Community

A.1.3 Example 3 O-RAN extends 3GPP measurement "UL Total PRB Usage"

A.1.3.1 PM Template alternative 1

Measurement Name	OR UL Total PRB Usage
Description (a)	Refer to 3GPP TS 28.552 [i.5] clause 5.1.1.2.a
Collection Method (b)	Refer to 3GPP TS 28.552 [i.5] clause 5.1.1.2.b
Condition (c)	Refer to 3GPP TS 28.552 [i.5] clause 5.1.1.2.c
Measurement Result (d)	Refer to 3GPP TS 28.552 [i.5] clause 5.1.1.2.d Additionally, the measurement is performed per PLMN ID
Measurement Type (e)	The short form measurement name has the form OR.RRU.PrbTotUl _Filter, Where filter is PLMN ID
Measurement Object Class (f)	Refer to 3GPP TS 28.552 [i.5] clause 5.1.1.2.f
Switching Technology (g)	Refer to 3GPP TS 28.552 [i.5] clause 5.1.1.2.g
Generation (h)	Refer to 3GPP TS 28.552 [i.5] clause 5.1.1.2.h
Purpose (i)	Refer to 3GPP TS 28.552 [i.5] clause 5.1.1.2.i. Additional for each PLMN ID

A.1.3.2 PM Template alternative 2

x.y.z OR UL Total PRB Usage

a) Refer to 3GPP TS 28.552 [i.5] clause 5.1.1.2.a

b) Refer to 3GPP TS 28.552 [i.5] clause 5.1.1.2.b

c) Refer to 3GPP TS 28.552 [i.5] clause 5.1.1.2.c

d) Refer to 3GPP TS 28.552 [i.5] clause 5.1.1.2.d

   Additionally, the measurement is performed per PLMN ID

e) The short form measurement name has the form OR.RRU.PrbTotUl _filter

   Where filter is PLMN ID

f) Refer to 3GPP TS 28.552 [i.5] clause 5.1.1.2.f

g) Refer to 3GPP TS 28.552 [i.5] clause 5.1.1.2.g

h) Refer to 3GPP TS 28.552 [i.5] clause 5.1.1.2.h

i) Refer to 3GPP TS 28.552 [i.5] clause 5.1.1.2.i. Additionally for each PLMN ID

Annex B (informative): Guidelines and Example for stndDefined VES Events

B.1 Guidelines for use of stndDefined VES for sending 3GPP-specified or O-RAN-specified O1 notifications

A stndDefined VES event, as specified in VES Event Listener Specification [18], allows a VES event to carry, as its payload, a notification specified by an SDO. In the case of O-RAN O1 Interface Specification, a harmonized stndDefined VES event carries either a 3GPP-specified O1 notification or an O-RAN-specified O1 notification as its payload.

3GPP has published an informative Annex B in ETSI TS 128 532 [3] providing guidelines for the integration of 3GPP-specified notifications with VES. This annex expands on the information provided by 3GPP, including information on how to include O-RAN-specified O1 notifications in a VES stndDefined event.

When an O-RAN and 3GPP compliant ME supports VES stndDefined events for sending asynchronous notifications, a3GPP-specified O1 notification, as defined by 3GPP, or an O-RAN-specified O1 notification, as defined by O-RAN, is included in the event.

A VES common event header, as defined by VES Event Listener Specification [18], is added to the notification.

In VES, the domain field in the common event header is used to route the event to the proper consumers and to map to a schema for the event payload. VES Event Listener Specification [18] added a new domain field enumeration value called stndDefined that indicates that the event is complying with a schema defined by a standards body.

An additional field was added to the VES common event header called stndDefinedNamespace, which contains a valid namespace as defined by the standards body. This field is only populated when the domain is stndDefined. 3GPP has defined four namespaces in ETSI TS 128 532 [3] Annex B; namely 3GPP-Provisioning, 3GPP-Heartbeat, 3GPP-FaultSupervision and 3GPP-PerformanceAssurance. O-RAN has defined a namespace for the notifications it defines. Refer to clause 5.2.2 for details. A VES collector uses the stndDefinedNamespace, along with the stndDefined domain, to route the event to the correct consumer.

A stndDefined VES event has a field structure called stndDefinedFields, specified in VES Event Listener Specification [18]. This structure contains three properties:

- schemaReference (type = string, format = uri)
- data (JSON object which is identical to the 3GPP or O-RAN notification)
- stndDefinedFieldsVersion (type = string, format = enum)

The schemaReference, if present, is used to verify that the notification content is correct. 3GPP is publishing the notification schemas defined using OpenAPI, to a public repository, (https://forge.3gpp.org/rep/sa5) so that schema references can be included in the event. Likewise, O-RAN will define its notification schemas using OpenAPI and publish them in a public repository. This repository is still to be created.

The data element contains either a 3GPP-specified O1 notification, in JSON format, as specified in ETSI TS 128 532 [3] or an O-RAN-specified O1 notification, in JSON format, as specified in O-RAN Information Model and Data Models Specification [i.14].

The stndDefinedFieldsVersion provides the version of the stndDefinedFields structure, as defined by VES Event Listener Specification [18].

Clause B.2 provides an example of a stndDefined VES event for a new alarm notification.

B.2 Example stndDefined VES event for a new alarm notification

The following example illustrates the population of a new alarm notification using a stndDefined VES event.

The VES Common Header is shown from line 44 through line 58. It contains:

- the domain set to stndDefined;
- the stndDefinedNamespace set to 3GPP-FaultSupervision.

The stndDefinedFields structure begins on line 59. It contains:

- the 3GPP schema reference for the 3GPP fault notification type
- the data element which contains the full 3GPP notifyNewAlarm fault notification
- the version of the stndDefinedFields

```
{
    "event": {
        "commonEventHeader": {
            "domain": "stndDefined",
            "eventId": "stndDefined-gNB-Nokia-000001",
            "eventName": "stndDefined-gNB-Nokia",
            "lastEpochMicrosec": 1594909352208000,
            "priority": "Normal",
            "reportingEntityName": "NOKb5309",
            "sequence": 0,
            "sourceName": "NOKb5309",
            "startEpochMicrosec": 1594909352208000,
            "stndDefinedNamespace": "3GPP-FaultSupervision",
            "version": "4.1",
            "timeZoneOffset": "UTC-05.00",
            "vesEventListenerVersion": "7.2"
        },
        "stndDefinedFields": {
            "schemaReference":https://forge.3gpp.org/rep/sa5/5G_APIs/blob/REL-
17/(…)/faultNotifications.json#definitions/notifyNewAlarm-NotifType,
            "data": {
                "href": 1,
                "uri": "xyz",
                "notificationId": "123",
                "notificationType": "notifyNewAlarm",
                "eventTime": "xyz",
                "systemDN": "xyz"
                "probableCause": "High Temperature",
                "perceivedSeverity": "Major",
                "rootCauseIndicator": false,
                "specificProblem": "7052",
                "backedUpStatus": true,
                "backUpObject": "xyz",
                "trendIndication": "No change",
                "thresholdInfo": {},
                "stateChangeDefinition": {},
                "monitoredAttributes": [],
                "proposedRepairActions": "xyz",
                "additionalText": "xyz",
                "additionalInformation": [],
                "alarmId": "15",
                "alarmType": "Environmental Alarm"
            }
        },
        "stndDefinedFieldsVersion": "1.0"
    }
}
```

Annex C (informative): Streaming Trace Management Activation Example

Example with Management-based Trace Activation, Data Reporting and Deactivation for Streaming Trace follows. The sequence below is based on 3GPP specifications which are referred in clause 6.4 of the present document.

```
@startuml
skin rose
Title Streaming Trace Connection Establishment, Data Reporting and Deactivation
autonumber "[0]"
participant "Provisioning MnS Consumer" as NMS
participant "Trace MnS Provider" as ME
participant "Trace MnS Consumer" as TMC
NMS --> ME : Trace Job Configuration create traceJob MOI
ME --> NMS : notifyMOIChanges
Opt (No connection to the Trace Mns Consumer exists)
ME -> TMC : establishStreamingConnection (HTTP POST request (SourceID, Trace Session Information))
TMC -> ME : HTTP: response (Connection ID)
ME -> TMC : HTTP GET request(Connection ID, Upgrade Header)
TMC -> ME : HTTP: response (Sec-WebSocket-Accept)
End

Opt
ME -> TMC: AddStream Operation (HTTP ADD)
End

|||
ME -> ME: Start Trace Session
ME -> TMC: Trace Session Start administrative message
loop (while trace session is active)
Opt (trace stream heartbeat)
ME -> ME: Hearbeat sending criteria are met
Note right
The criteria for sending
heartbeat administrative messages
are implementation specific
End note

ME -> TMC: Trace Stream Heartbeat administrative message
End

loop (Trace recording session handling)
ME -> ME: "start" triggering event detected

ME -> ME: Start Trace Recording Session and allocate new TRS (embedded in a reportStreamData
Operation)
ME -> TMC : Trace Recording Session Start administrative message
loop (until "stop" triggering event is detected)


loop (until reporting condition is satisfied)

ME -> ME: Capture trace record

End

ME -> TMC: "reportStreamData(traceRecords)"


End
ME -> ME: Recording session complete/stop criteria are met
ME -> ME: Stop trace recording session
ME -> TMC: Trace Recording Session Stop administrative message

End

End
NMS --> ME: Trace Session Deactivation/Configuration
ME -> ME: Stop Trace Session
loop (for each on-going Trace Recording Session)
ME -> ME : Stop Trace Recording Session
Opt (there are outstanding trace records)
ME -> TMC: "reportStreamData(traceRecords)"
End
ME -> TMC: Trace Recording Session Stop administrative message
```

```
End
ME -> TMC: Trace Session Stop administrative message
Opt (multiple streams exist)
ME -> TMC: deleteStream Operation (HTTP DELETE)
End
Opt
ME -> TMC: terminateStreamingConnection(WebSocket Close Frame)
ME <<->> TMC: Terminate Connection
End
@enduml
```

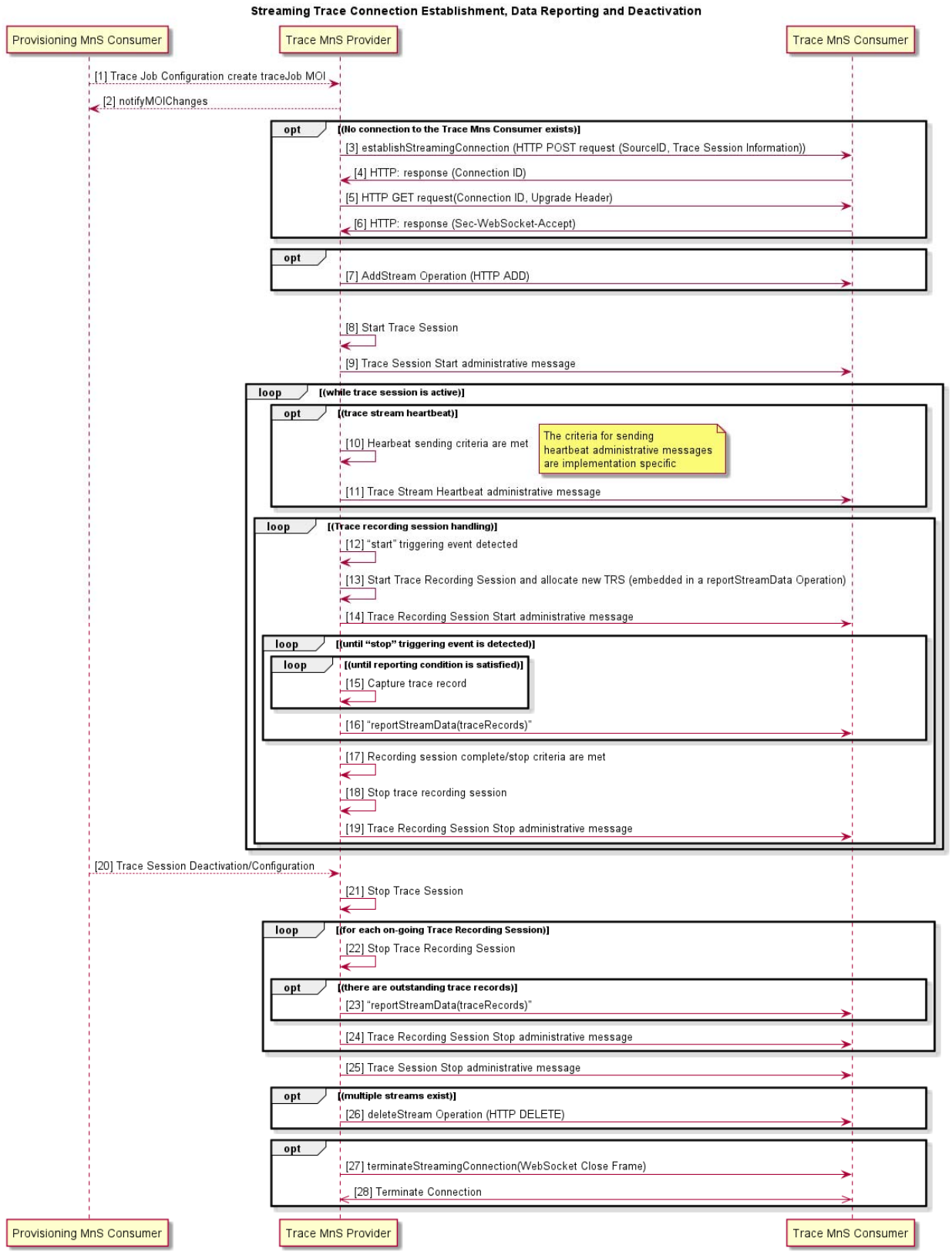

Figure C-1: Streaming Trace Connection Establishment, Data Reporting and Deactivation Example

Scenario:

- Provisioning Management Service Consumer activates/configures Trace Session on Trace Provider. This will be accomplished using Provisioning Management services described in clause 6.1 of the present document.

- Trace Provider sends a notifyMOIChanges to indicate the new MOI is created.
  Steps 3-6 are optional when no connection to trace MnS consumer exist.

- Trace Provider needs to establish a connection to the Trace Consumer to set up a streaming connection (streams are active at this time between the Provider and Consumer). This is done using the establishStreamingConnection Operation via an HTTP POST request containing MetaData associated with this Trace Session.

- Trace Consumer responds with an acknowledgement that contains the ConnectionID needed by the Provider when requesting that the connection be upgraded to a WebSocket to support streaming of the trace data.

- Trace Provider requests the upgrade of the connection to a WebSocket using the ConnectionID and an HTTP GET operation.

- Trace Consumer accepts the upgrade and WebSocket is established. WebSocket will remain connected until the last streaming trace session active on the Trace Provider is ended.

NOTE: In this example, only one streaming trace session is active.

- Optionally addStream operation is used to add a stream to the trace connection.

- Trace Provider starts trace session, waiting for triggering event to occur.

- Trace Provider sends trace session start administrative message to Trace MnS Consumer.

- Heartbeat sending criteria are met. The criteria about when to send Trace stream heartbeat administrative message are implementation specific.

- Trace stream heartbeat administrative message is sent to Trace consumer repeatedly. Trace stream heartbeat administrative message is used for monitoring whether the trace session connection is alive and can be executed parallel to other loops.

- "start" triggering event detected.

- A new trace recording session is started on the Trace Provider. Each trace recording session has a unique Trace Recording Session (TRS) Reference associated with it.

- Trace recording session start administrative message is sent from Trace MnS Provider to Trace MnS Consumer.

- While this trace record is active, and the reporting criteria are not fulfilled, the Trace MnS Provider collects trace data.

- When the reporting criteria are fulfilled, either timer expires or the buffer fills, or the buffer has data and the "stop" triggering event is detected, the Trace Provider sends a trace data report to the Trace Consumer containing trace record data for active recording sessions in a trace session. These records are the payload of the reportStreamData operation.

- The criteria for the trace recording session completion or stop occurs (call ends, etc.).

- The Trace Provider stops collecting data for this trace recording session.

- Trace Provider sends trace recording session stop administrative message to Trace MnS Consumer.

- Provisioning Management Service Consumer deactivates the trace via procedures defined in clause 6.1 of the present document. Deactivation means that the trace data collection ceases, and the Trace Provider stops all active trace recording sessions and sends data that it has collected up to this point, if any, for each active trace recording to the Trace Consumer.

- Trace Provider initiates the termination of the trace session.

- For each active trace recording session, Trace Provider initiates a Stop Trace Recording Session.

- Optionally if there are outstanding record(s) for this trace recording session that have not been streamed to the Trace Consumer, Trace Provider sends them as the payload of the reportStreamData operation.

- Trace Provider informs the Trace Consumer that this Trace Recording Session has ended by sending the trace record termination administrative message. The producer repeats this until all trace recording sessions for this trace session have been terminated.
- Trace MnS Provider sends the trace session stop administrative message to Trace MnS Consumer.
- Optionally the Trace Provider sends the Trace Consumer the deleteStream operation indicating that the stream has been removed in case the connection is used for multiple streams.
- Optionally when all active Trace Sessions between Trace Provider and Trace Consumer have ended, the WebSocket connection is to be torn down. Trace MnS Provider sends the Trace MnS Consumer the terminateSignalingConnection Operation which is a WebSocket close frame.
- Terminate connection.

Annex D (normative): Recommendation for UE Identifier Format in Trace Header

Specification 3GPP TS 32.423 [13], clause 5.2.2 defines *vendorExtension* IE in Trace Header as an Arraylist of String. The Trace Record Header should be encoded using GPB in Annex G of 3GPP TS 32.423 [13]. Based on Annex G, Trace Record Header in GPB is defined as:

```
message TraceRecordHeader {
  int64                time_stamp = 1;
  string               nf_instance_id = 2;
  string               nf_type = 3;
  bytes                trace_reference = 4;
  bytes                trace_recording_session_ref = 5;
  TraceRecordType      trace_rec_type_id = 6;
  bytes                ran_ue_id = 7;
  string               payload_schema_uri = 8;
  GlobalGnbId          global_gnb_id = 9;
  map<string, string>  vendor_extension = 10;
}
```

Several UE identifiers and node identifiers are identified as necessary for trace record correlation. Refer to O-RAN architecture description [15], clause 5.5 for detailed information.

To enable trace record correlation, a new map entry is defined for vendor_extension to be used to send O-RAN UE/Node identifiers.

Defined TraceRecordHeader field vendor-extension is in following format:

```
map<string, string> vendor_extension = 10;
```

The map entry should be added for UE identifier and node identifiers is as below:

First string in the map entry: `value = "oranUENodeIdentifiers"`

Second string in the map entry: value = result of "print string" of message OranUEAndNodeIdentifiers

NOTE: The O-RAN defined map entry for O-RAN UE/Node identifiers `"oranUENodeIdentifiers"` can co-exist with other vendor defined vendor-extension map entries. O-RAN defined map entry `"oranUENodeIdentifiers"` can be add in any position in the `vendor_extension` map.

```
message OranUEAndNodeIdentifiers {
  optional OranConnectedEntity  connected_entity_id =1;
  optional OranUEId             originator_ue_id = 2;
  optional OranUEId             connected_entity_ue_id =3;
}

Message OranUEId{
  optional int64  amf_ue_ngap-id = 1;
  optional int64  ran_ue_ngap_id =2;
  optional int64  mme_ue_s1ap_id = 3;
  optional int64  gnb_cu_ue_f1ap_id = 4;
  optional int64  gnb_cu_cp_ue_e1ap_id = 5;
  optional int64  gnb_cu_up_ue_e1ap_id= 6;
  optional int64  traced_ng_ran_node_ue_xnap_id = 7;
  optional int64  connected_ng_ran_node_ue_xnap_id = 8;
  optional int64  m_enb_ue_x2ap_id = 9;
  optional int64  c_rnti = 10;
}

Message OranConnectedEntity {
  oneof connected_entity_id {
    bytes            ng_connected_guami = 1;            // AMF ID of the connected AMF
    Guami            ng_connected_guami_decoded = 2;    // AMF ID of the connected AMF
    GlobalGnbId      xn_connected_global_gnb_id  = 3;   // ID of neighbouring gNB-CU-CP
    OranGlobalEnbId  xn_connected_global_enb_id = 4;    // ID of neighbouring ng-eNB node
    OranGlobalEnbId  x2_connected_global_enb_id  = 5;   // ID of connected NSA eNB node
    bytes            s1_connected_mme= 6;               // ID of connected MME
    Gummei           s1_connected_mme_decoded= 7;       // ID of connected MME
    int64            f1_connected_du_id = 8;            // ID of connected gNB-DU
    int64            e1_connected_cuup_id = 9;         // ID of connected gNB-CU-UP
  }
```

```
}

message GlobalEnbId {
  bytes  plmn_identity = 1;
  int64  enb_id = 2;
}

Message Guami {
  bytes    plmn_identity =1;
  string   amf_region_id=2;
  string   amf_set_id=3;
  string   amf_pointer=4;
}

Message Gummei {
  bytes    plmn_identity =1;
  string   mme_grp_id=2;
  string   mme_code=3;
}
```

Based on the value nf_type (for example, gNB-CU-CP, gNB-CU-UP, gNB-DU) in the TraceRecordHeader, different types of UE identifiers and node identifier can be reported. For detail, refer to O-RAN architecture description [15], clause 5.5.

Annex E (informative): Change history

Date	Revision	Description
2019.03.18	0.01.00.00	First draft of O-RAN OAM Interface Specification.
2019.03.28	0.01.01.00	Updates from review remarks received.
2019.05.21	0.01.01.01	Fault Supervision, Performance Assurance and File Management updates.
2019.05.28	0.01.01.02	References, Abbreviations, Definitions, Provisioning, Communication Surveillance, PNF Start Up and Registration updates.
2019.06.13	0.01.01.03	Diagrams for File Management converted to UML, Performance Assurance UML, PNF Software Management Updates.
2019.06.17	0.01.01.04	Provisioning Updates.
2019.07.01	01.00	Review Comments Addressed TSC approved copy.
2019.09.27	02.00	Updates for late review comments, additional CM notifications, NETCONF requirements and updated references to 3GPP SA5 Rel-16.
2020.03.03	03.00	Update Heartbeat Management Service. New clauses for Subscription Control, Streaming PM, O-RAN Defined PM Measurements and an Annex showing examples for using the specified template for O-RAN defined PM Measurements.
2020.08.18	04.00	Update Introductory Material, Provisioning, Fault Supervision, Performance Assurance, Trace Management, and Heartbeat Management to incorporate 3GPP Rel 16 CRs. Add Annex B for stndDefined event example and Annex C for Streaming Trace example.
2020.08.31	04.00	Update document with comments from WG1 review.
2021.03.11	04.01	Incorporate approved CRs to prepare for v05.00. Update Provisioning with approved CR 10. Update Fault Supervision with approved CR 11.
2021.04.27	04.02	Update Software Download with approved CR 13.
2021.05.24	04.03	Incorporate approved Updates and Corrections CR 14. Updates to References, Security Protocols and Trace.
2021.06.21	04.04	Incorporate approved YANG Module Discovery CR 15.
2021.06.22	05.00	O1v5 incorporating CRs from 04.01.00 through 04.04.00.
2021.10.25	06.00	Incorporate approved CRs: PNF Reset CR 16, Performance Management CR 17, Cloudified NF Registration CR 18, Notify Alarm List Rebuilt CR 19, O1 Notifications CR 20 and References Updates CR 21.
2022.03.15	07.00	Incorporate approved CRs: PM Streaming Format Correction CR 22, 3GPP specified Notification VES format support CR 23, Annex C Streaming Trace Management CR 24, PNF Registration Notification CR 25, Rearrange PNF Reset Notification Requirements CR 26, Clarify counter naming requirement CR 27 and Notification capability CR 28.
2022.07.18	08.00	Incorporate approved CRs: O-RAN counter name clarification CR 29, File management update CR 30, O1 Notification CR 31, Plug and Connect uplift CR 32, UE Identifiers for Trace header CR 33 and CM Notifications uplift CR 34. Editorial changes related to the copyright clarification.
2022.08.31	08.00.01	Incorporate approved CR 36 resolving outdated 3GPP references.
2022.11.01	09.00.00	Incorporate approved CRs: Alignment with 3GPP and editorial modifications CR37, PM file format for NR measurements CR38. Editorial changes related to the new document naming format. Editorial changes related to application of embedded O-RAN styles template.
2022.11.21	09.00.01	Editorial CR39 introduced changes for alignment with ODR, O-RAN TS Template and ETSI PAS - re-arranged and re-numbered clauses. Removal of author information from the history table.
2023.01.31	09.00.02	Incorporate approved CRs: UE Identifier schema CR40, Measurement job control clarification CR41 and File management correction CR42.
2023.03.06	10.00	Incorporate approved CRs: Clean-up of 3GPP TS 28.532 reference CR43, Correction of 3GPP TS 28.533 reference CR44, O-RU change in O1 introduction CR45, Split of normative and informative references CR46, Clean-up references CR47, Clean-up of introduction CR48, Remove out of scope Fault Notification requirements CR49 and Clean-up Fault Supervision Control Requirements CR50.
2023.07.11	11.00	Incorporate approved CRs: Reference update to O-RAN internal specifications CR33, Normative language clean-up CR52.
2024.06	11.0.0	First published ETSI/O-RAN version.

History

Document history		
V11.0.0	June 2024	Publication