O-RAN.WG4.MP.0-v05.00 Technical Specification
O-RAN Alliance Working Group 4
Management Plane Specification

April 15, 2021

Neo SASTECH Co., LTD.

panjongp@gmail.com

Neo SASTECH

Bug fixes and correction to v04.00:

- Clarify operation of default acccount for certificate access
- Clarify operation of supervision in lock state
- Clarify PRACH patterns
- Fixing copy/paste errors in the S-plane PTP status definitions
- Corrected omissions from optional feature table - Clarify center bandwidth parameter
- Replace previous NMS terms with SMO - Corrections to C/U plane monitoring for FHM

Addition of new functionality, including:

- New NACM permissions for SMO and hybrid ODU
- New optional feature for performing pnfRegistration
- New optional feature for configured YANG subscriptions sent over JSON/REST
- Updating mandatory cipher to AES128-CTR
- Bandwidth management to avoid over-subscription of O-RU resources
- Shared cell with selective Tx/Rx using Beam ID
- Cascaded FHM Operation
- New capability to support co-ordinated (self) antenna calibration

Contents

Neo SASTECH

1.3.2 Abbreviations

ALD Antenna Line Device

DHCP Dynamic Host Configuration Protocol

NETCONF Network Configuration Protocol

PNF Physical Network Function

sFTP Secure File Transfer Protocol or SSH File Transfer Protocol

SSH Secure Shell

T-TSC Telecom Time Subordinate Clock

YANG Yet Another Next Generation

1.4 Conventions

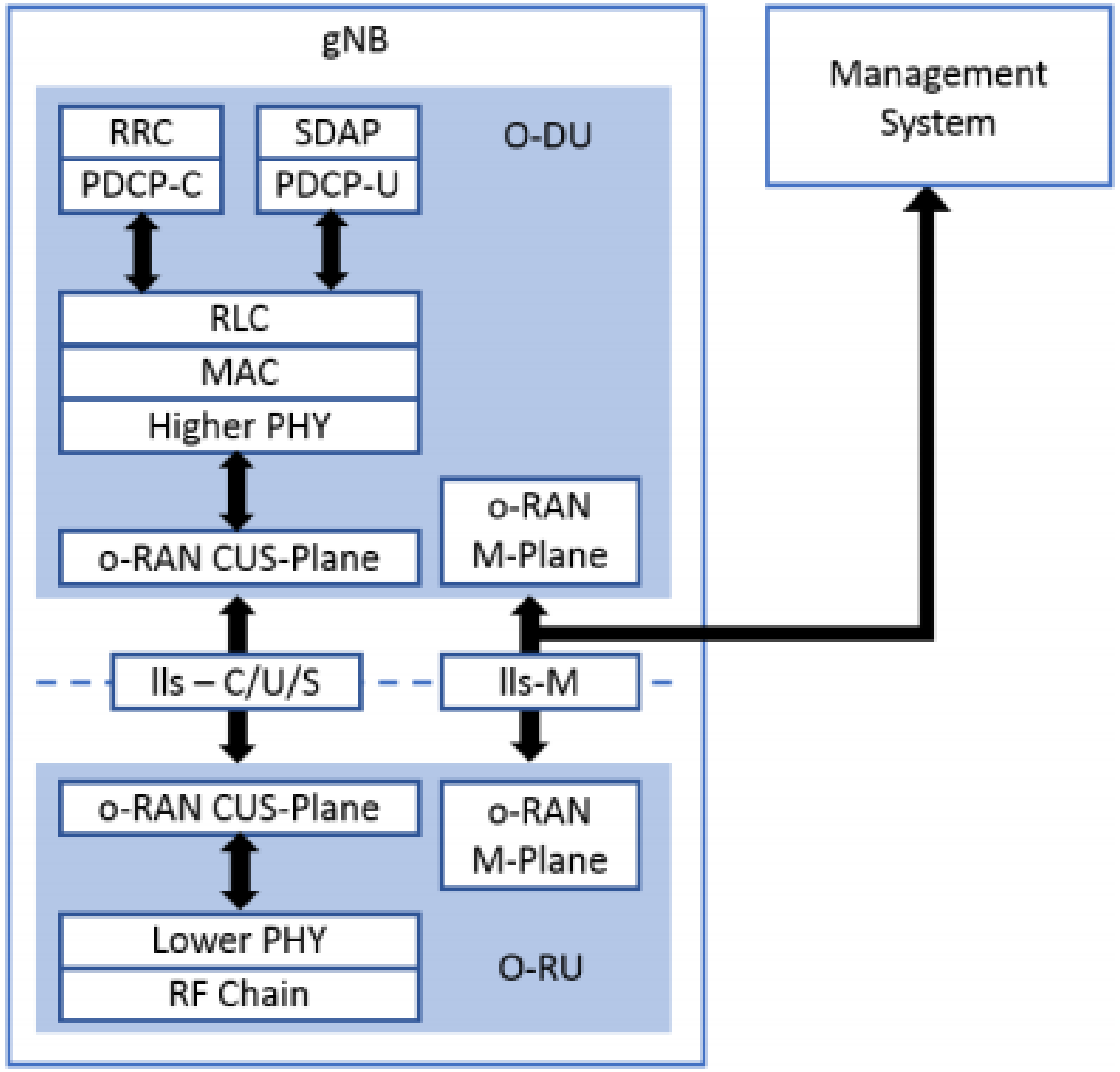
If there is any conflict between the YANG models and the accompanying text description in this specification, **the definition of the YANG models shall take precedence.**

1.5 Topics for Future Specification Versions

1. Beam Id field interpretation for various types of beamforming
2. Redundancy and failover scenario
3. Shared cell support for IP-defined flows
4. Enhancements to better align with O-RAN Alliance O1 specification

Neo SASTECH

2.1.1 Architecture for O-RAN WG4 Fronthaul functional split



2.1.2 M-Plane architecture model

Hierarchical model.

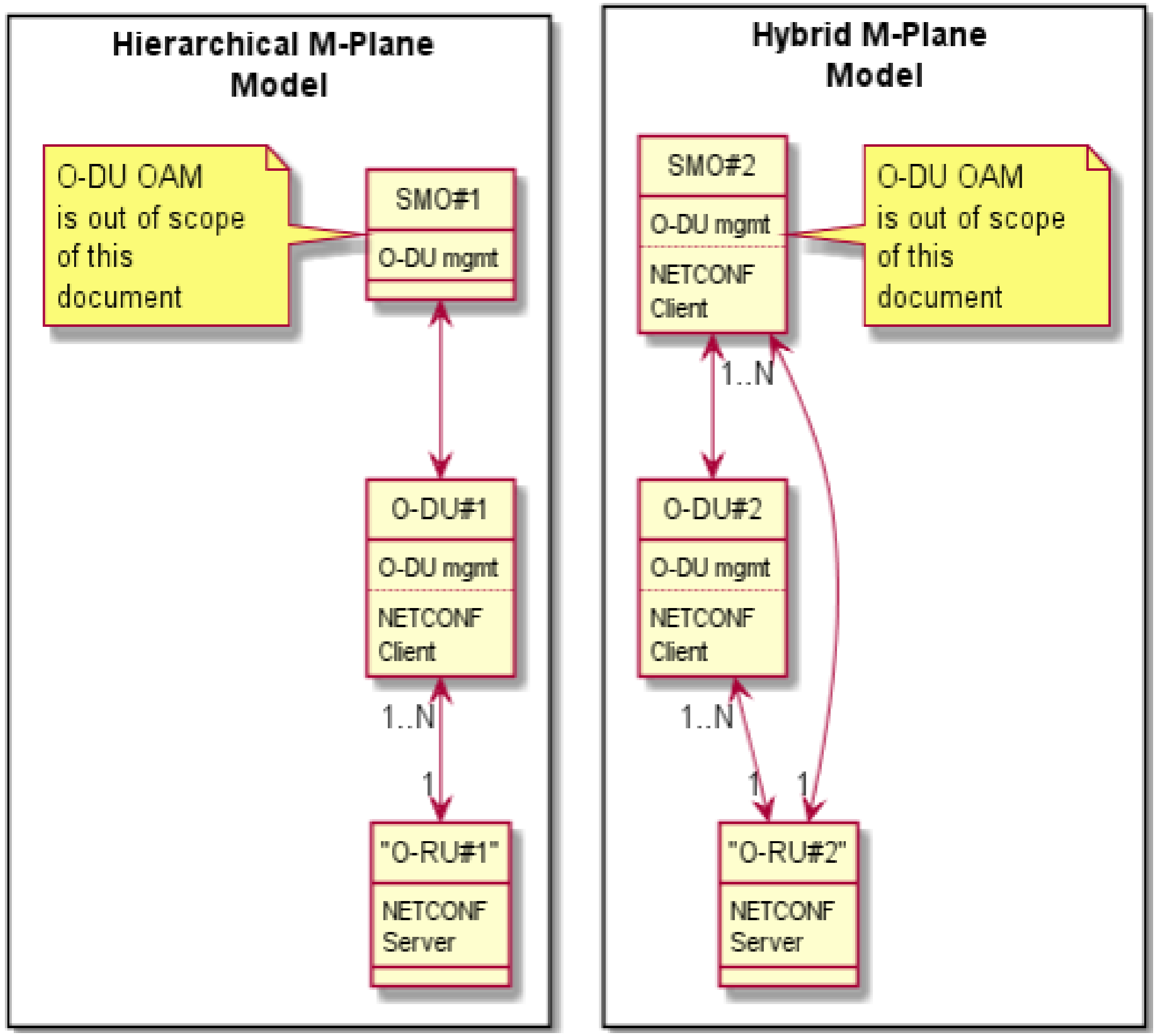
As shown on the left side Figure 1, the O-RU is managed entirely by one or more O-DU(s) using a NETCONF based M-Plane interface. When the O-RU is managed by multiple O-DUs, it is typically for enabling O-DU and/or transport connectivity redundancy capabilities. Refer to Chapter 3 for more details.

Hybrid model.

As shown on the right side of Figure 1, the hybrid architecture enables one or more direct logical interface(s) between management system(s) and O-RU in addition to a logical interface between O-DU and the O-RU. It should be noted that the NETCONF clients connecting to the O-RU may be of different classes (e.g. O-DU and SMO). For example, functions like O-RU software management, performance management, configuration management and fault management can be managed directly by the management system(s).

Neo SASTECH

M-Plane Architecture



NETCONF/YANG is used as the network element management protocol [3] and data modeling language [4].
Use of such a standardized framework and common modeling language simplifies integration between O-DU and O-RU as well as operator network integration (in terms of running service) in case of elements sharing a common set of capabilities. The framework supports integration of products with differing capabilities enabled by well-defined published data models. NETCONF also natively supports a hybrid architecture which enables multiple clients to subscribe and receive information originating at the NETCONF server in the O-RU.

Neo SASTECH

2.1.3 Transport Network

2.1.4 M-Plane functional description

“Start up” installation --- Ch.3

- During startup, the O-RU acquires its network layer parameters either via static (pre-configured in the O-RU) or dynamically via DHCP or DHCPv6
- O-RU establishes the NETCONF connectivity using the “call home” feature
- pnfRegistration procedure

SW management --- Ch.5

- software download, installation, validation and activation

Configuration management --- Ch. 6

- Retrieve Resource State, Modify Resource State, Modify Parameters and Retrieve Parameters
- NETCONF get-config and edit-config RPCs

Performance management --- Ch. 7

- YANG Notification: **get** rpc and/or notification
- File Upload

Fault Management --- Ch. 8

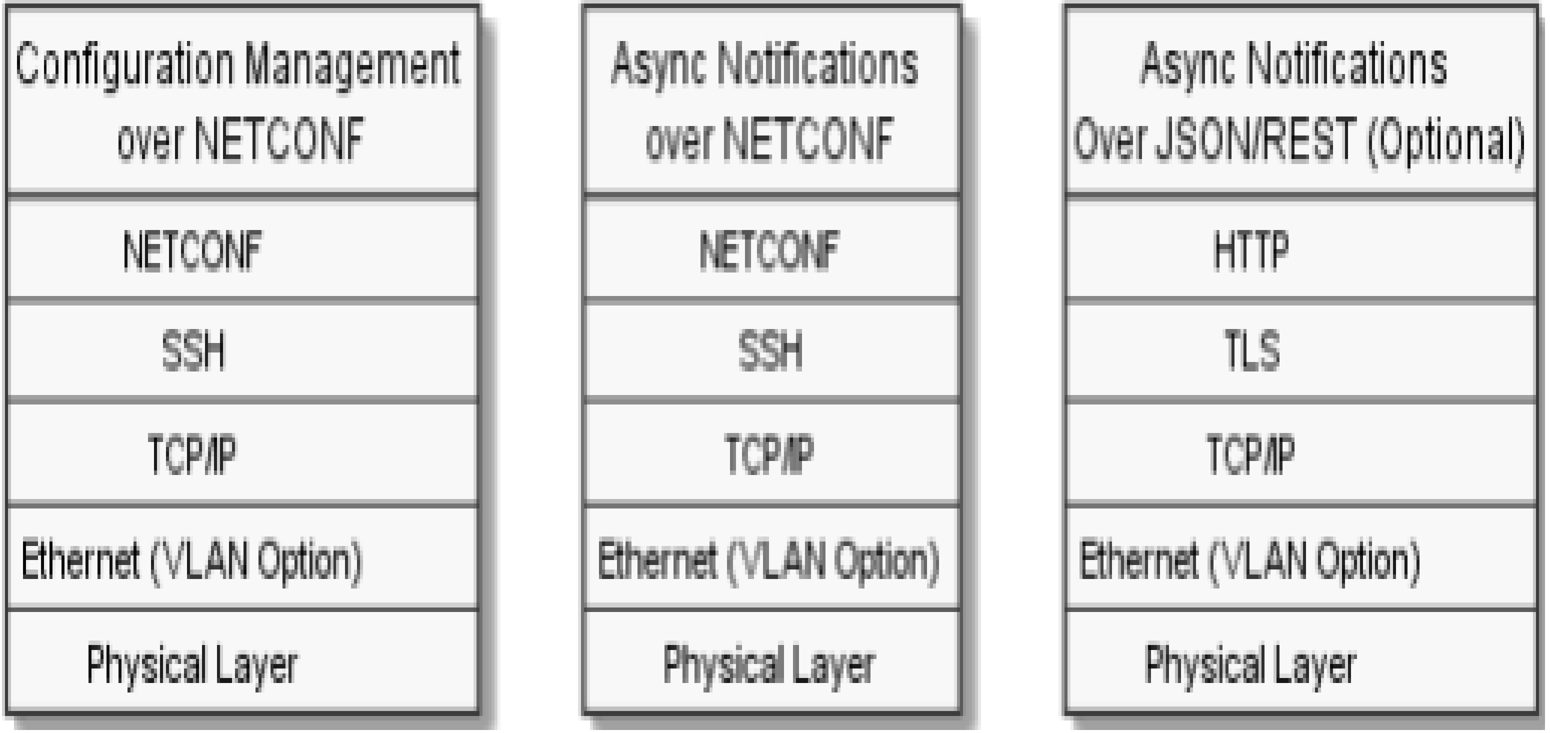
- alarm notifications

File Management --- Ch. 9

- sFTP connection between O-RU to O-DU/SMO.

2.2 Interfaces

M-plane protocol stack



Neo SASTECH

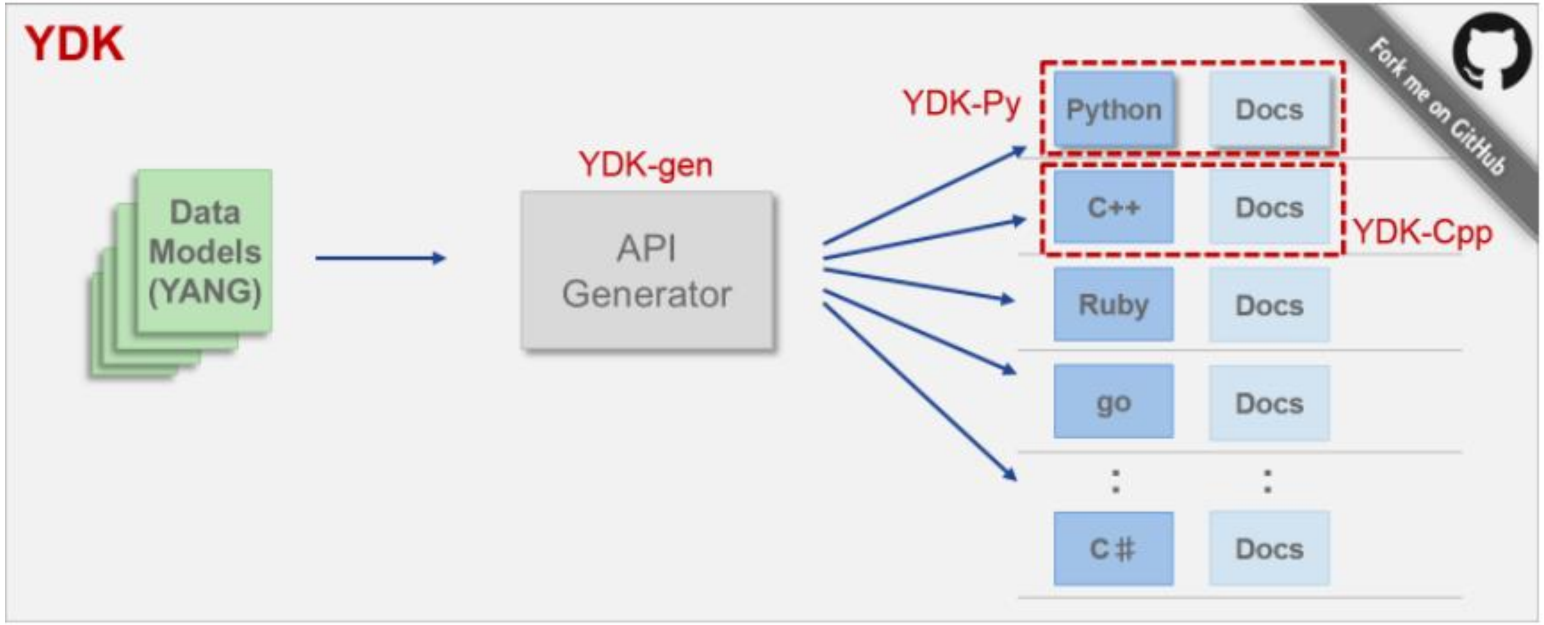
2.3 YANG Module Introduction

http://ydk.cisco.com/py/docs/getting_started.html#overview

Table of Contents

What is YDK?

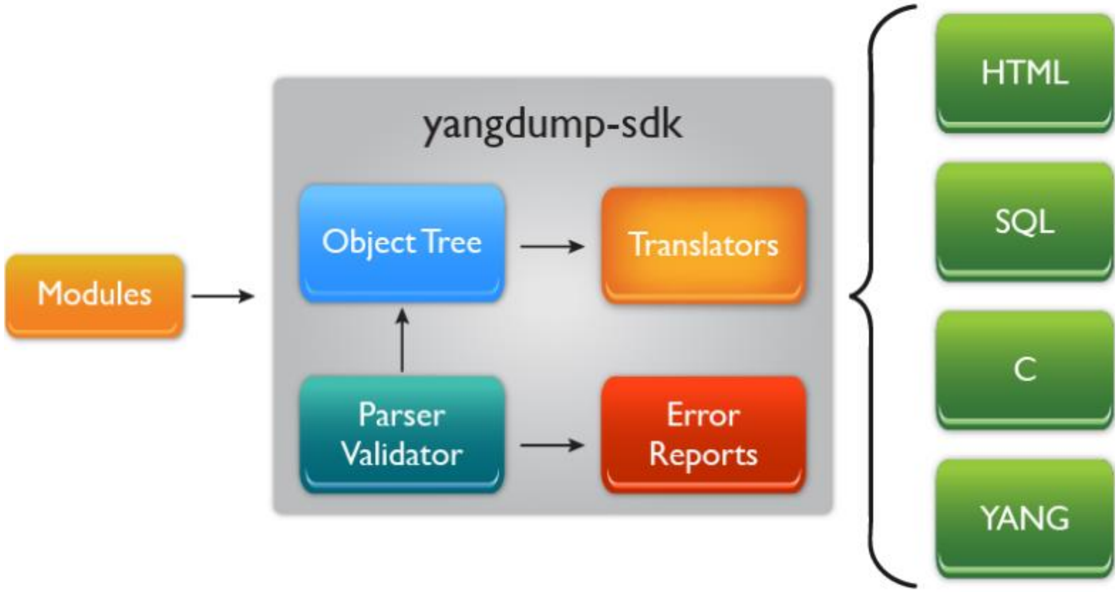
We have created the YANG Development Kit (YDK) to facilitate network programmability using data models. YDK can generate APIs in a variety of programming languages using YANG models. These APIs can then be used to simplify the implementation of applications for network automation. YDK has two main components: an API generator (YDK-gen) and a set of generated APIs. Today, YDK-gen takes YANG models as input and produces Python APIs (YDK-Py) that mirror the structure of the models.



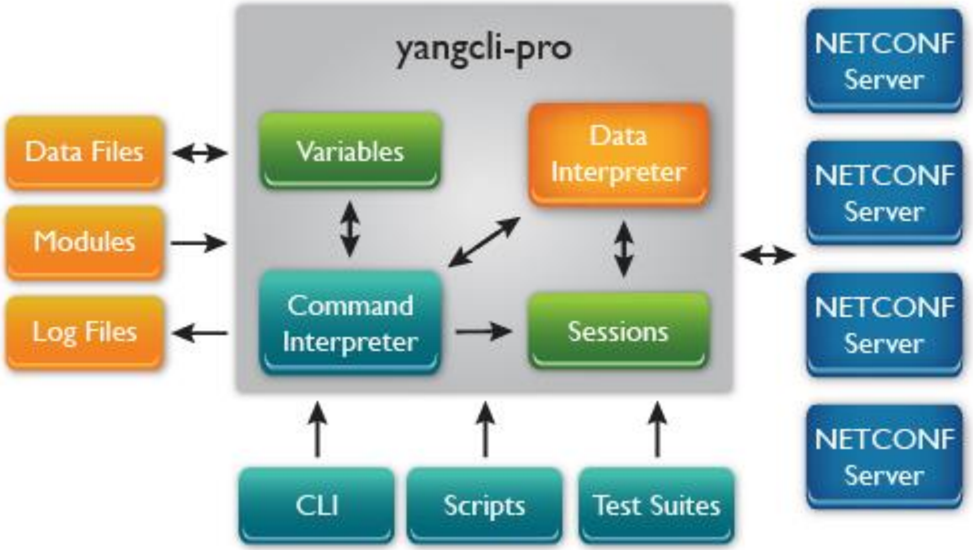
Neo SASTECH

2.3 YANG Module Introduction

https://www.yumaworks.com/tools/yang-compiler/



YANG-Based NETCONF Client and Test Platform



https://www.yumaworks.com/products/
- YumaPro Client
- YumaPro SDK Basic
- YumaPro SDK Binary
- YumaPro SSDK Source

https://github.com/OnVelocity/yang-compiler
https://github.com/openconfig/goyang
https://tools.ietf.org/id/draft-ietf-netmod-rfc6087bis-13.html
Guidelines for Authors and Reviewers of YANG Data Model Documents
draft-ietf-netmod-rfc6087bis-13
https://yangcatalog.org/

Neo SASTECH

Common Models

+Interfaces
- +o-ran-ald-port.yang : 14.5.1
- +o-ran-dhcp.yang : 3.1
- +o-ran-ethernet-forwarding.yang: 14.5.2
- +o-ran-externalio.yang
- +o-ran-interface.yang : 3.1, 4.1, 4.3, 4.4, 4.5, 4.11, 12.2.3, 14.5.1
- +o-ran-mplane-int.yang: 6.3
- +o-ran-transceiver.yang: 4.2, 4.11, 14.5.1

+Operations
- +o-ran-ald.yang: 14.5.1
- +o-ran-file-management.yang: 15.4, 15.5
- +o-ran-operations.yang: 3.4, 3.8.2, 12.1, 15.5, 15.6.1
- +o-ran-software-management.yang: 5.1
- +o-ran-trace.yang
- +o-ran-troubleshooting.yang

+Sync
- +o-ran-sync.yang: 10.4, 10.6, 12.1

+System
- +o-ran-fan.yang
- +o-ran-fm.yang
- +o-ran-hardware.yang: 3.8.2, 6.1, 12.1
- +o-ran-supervision.yang: 3.5, 4.10, 15.6.2
- +o-ran-usermgmt.yang
- +o-ran-ves-subscribed-notification.yang: 15.5
- +o-ran-wg4-features.yang

Imported Models

- +iana-hardware.yang: 3.4
- +iana-if-type.yang
- +ietf-crypto-types.yang
- +ietf-datastores.yang: 3.4
- +ietf-dhcpv6-types.yang
- +ietf-hardware.yang
- +ietf-inet-types.yang
- +ietf-interfaces.yang: 3.4
- +ietf-ip.yang: 3.4
- +ietf-netconf-acm.yang: 3.4
- +ietf-netconf-monitoring.yang
- +ietf-network-instance.yang
- +ietf-subscribed-notifications.yang: 15.1
- +ietf-yang-library.yang: 6.2, 13.1
- +ietf-yang-types.yang

RU Specific Models

+interface
- +o-ran-processing-element.yang: 4.5,12.2.3, 14.5.3, Annex B

+operations
- +o-ran-ecpri-delay.yang
- +o-ran-lbm.yang: 4.6.1.3
- +o-ran-performance-management.yang: 7.1, 7.2.2
- +o-ran-udp-echo.yang
- +o-ran-uplane-conf.yang: 12.2.3, 12.4.1, 12.4.4, 12.6.1.2, 12.6.2, 13.1, 13.2.2, 14.2, 14.5.1, 14.5.4, 14.6.1, Annex A
- +o-ran-antenna-calibration.yang: 12.5, 12.5.1
- +o-ran-beamforming.yang: 12.2.3, 12.4.1, 12.4.2, 12.4.3, 12.4.4, 14.5.1
- +o-ran-compression-factors.yang
- +o-ran-delay-management.yang
- +o-ran-laa.yang: 13.1, 13.2.2, 13.3.1, 14.5.1
- +o-ran-module-cap.yang: 12.6.1, 12.6.2, 12.7, 13.1, 13.2, 15.5.1
- +o-ran-shared-cell.yang: 14.2, 14.4, 14.5.1

Neo SASTECH

```
module o-ran-delay-management {
  yang-version 1.1;
  namespace "urn:o-ran:delay:1.0";
  prefix "o-ran-delay";

  organization "O-RAN Alliance";

  contact
    "www.o-ran.org";

  description
    "This module covers off aspects of O-DU to O-RU delay management,
    including config data related to O-RU transmission and reception
    windows.

    Copyright 2020 the O-RAN Alliance.

    THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS 'AS IS'
    AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
    IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
    ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE
    LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
    CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
    SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
    INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
    CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
    ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE
    POSSIBILITY OF SUCH DAMAGE.

    Redistribution and use in source and binary forms, with or without
    modification, are permitted provided that the following conditions are met:

    * Redistributions of source code must retain the above copyright notice,
    this list of conditions and the above disclaimer.
    * Redistributions in binary form must reproduce the above copyright notice,
    this list of conditions and the above disclaimer in the documentation
    and/or other materials provided with the distribution.
    * Neither the Members of the O-RAN Alliance nor the names of its
    contributors may be used to endorse or promote products derived from
    this software without specific prior written permission.";

  revision "2020-08-10" {
    description
      "version 4.0.0

      1) introduction of new t1a-max-cp-dl leaf to enable decoupled timing between C- and U-Plane";

    reference "ORAN-WG4.M.0-v04.00";
  }

  revision "2019-07-03" {
    description
      "version 1.1.0

      1) fixing descriptions of ta3-min and ta3-max.
      2) introducing grouping/uses to enable model re-use by WG5";

    reference "ORAN-WG4.M.0-v01.00";
  }

  revision "2019-02-04" {
    description
      "version 1.0.0

      1) imported model from xRAN
      2) changed namespace and reference from xran to o-ran";

    reference "ORAN-WG4.M.0-v01.00";
  }


  feature ADAPTIVE-RU-PROFILE {
    description
```

2.4 Security

SSHv2

per aes128-ctr and hmac-sha2-256 are mandatory.

Plane	Integrity (protection from modifications)	Confidentiality (encryption protection)	Authentication (validity of the originator)	Remarks
M-Plane/ NETCONF	Yes	Yes	Yes	Using the SSHv2 layer used for NETCONF transport
Optional support of JSON/REST	Yes	Yes	Yes	HTTPS used for JSON/REST transport

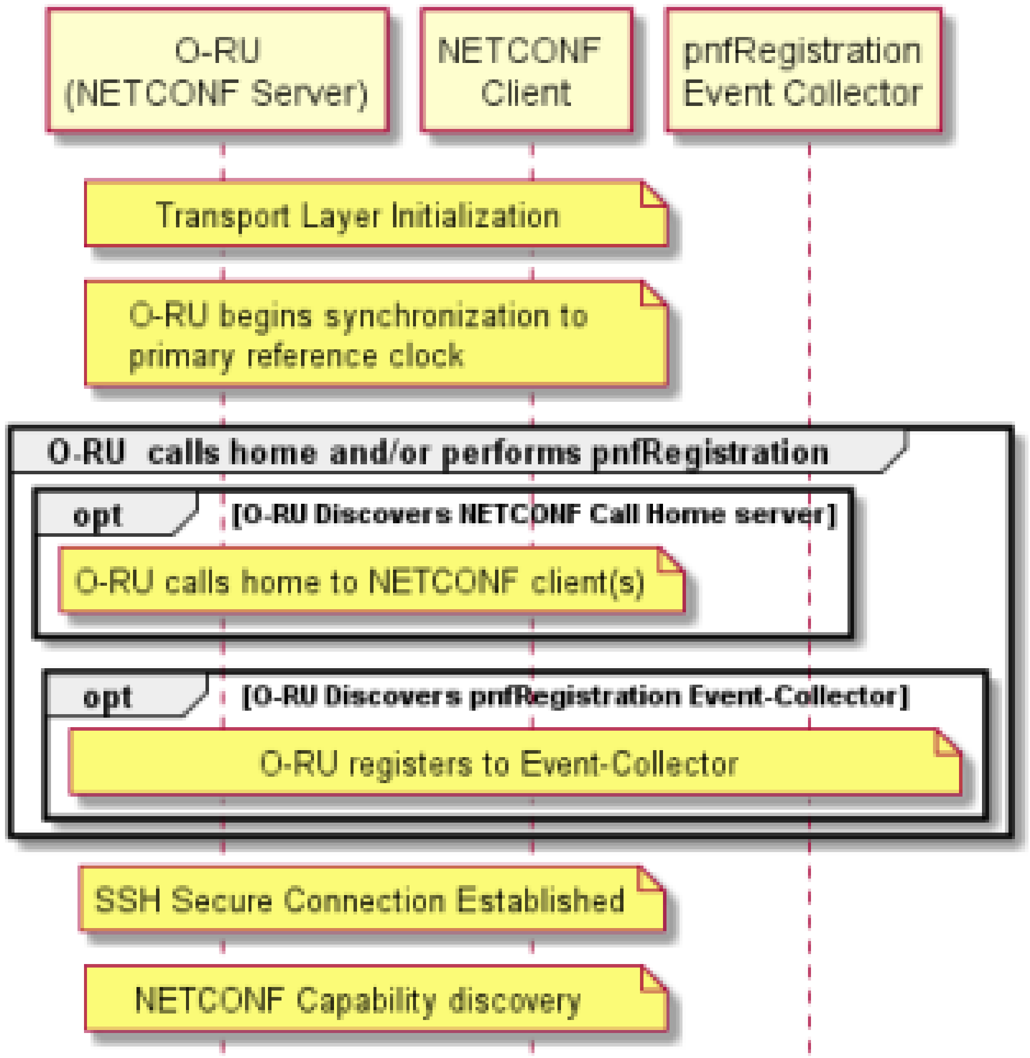
Pre-condition:

- Power-ON for O-RU/NETCONF Server or O-RU restart operation.
- Power-ON for O-RU controller/NETCONF Client(s) and/or pnfRegistration event-collector.
- Physical interface(s) is(are) connected.

Post-condition:

- O-RU is ready for the radio transmission to the air on at least one carrier if packet transmission received from O-DU
- O-RU is ready for the packet transmission to the O-DU if radio reception received at the air on at least one carrier.
- At least one O-RU Controller/NETCONF client with either “super-user” or “hybrid-odu” access privileges can control the carrier configuration of the O-RU/NETCONF server in O-RU.

Neo SASTECH



transport layer resolution (DHCP, MAC, VLAN, IP, etc.)
and recovers IP address(es) of O-RU controller(s)
and/or pnfRegistration event-collector

synchronization of the O-RU against a Primary Reference Clock

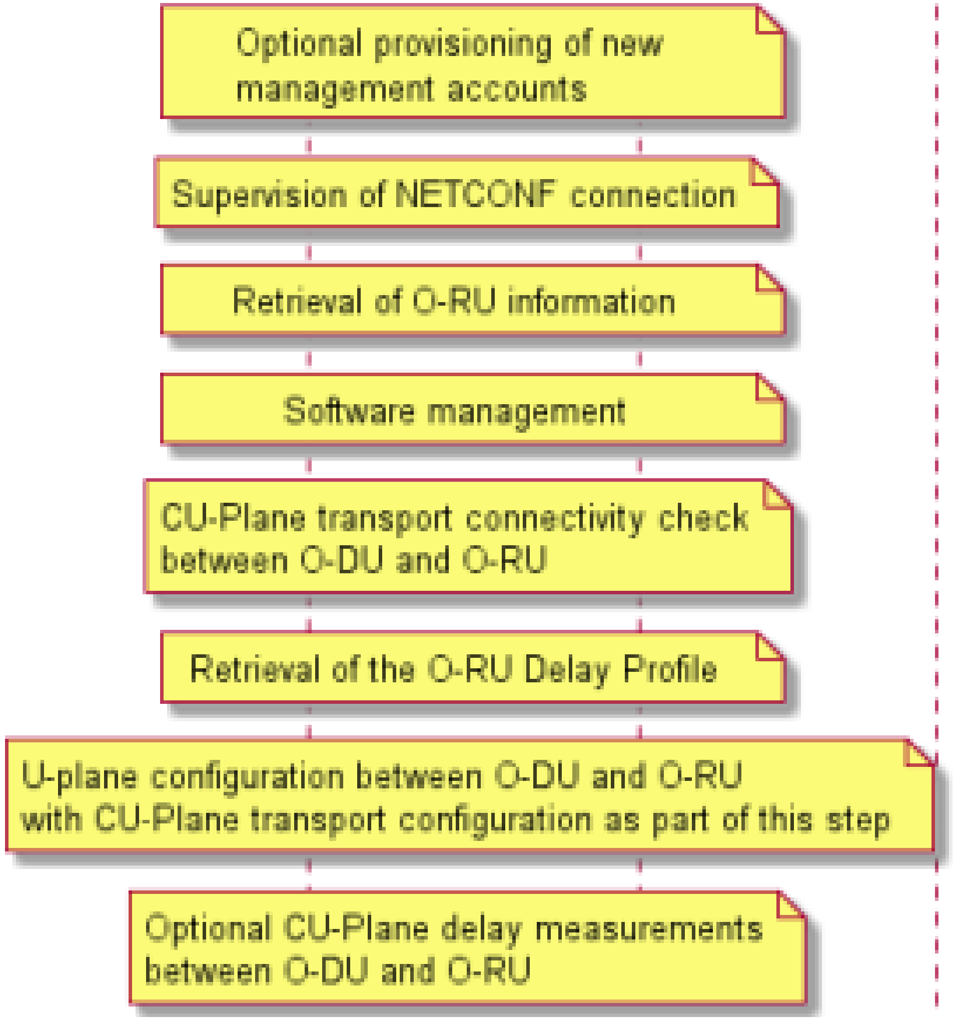
NETCONF Call Home

pnfRegistration

SSH connection establishment

NETCONF capability discovery

Chapter 3 “Start up” installation



optional provisioning of new management accounts

supervision of NETCONF connection

retrieval of O-RU information

SW management

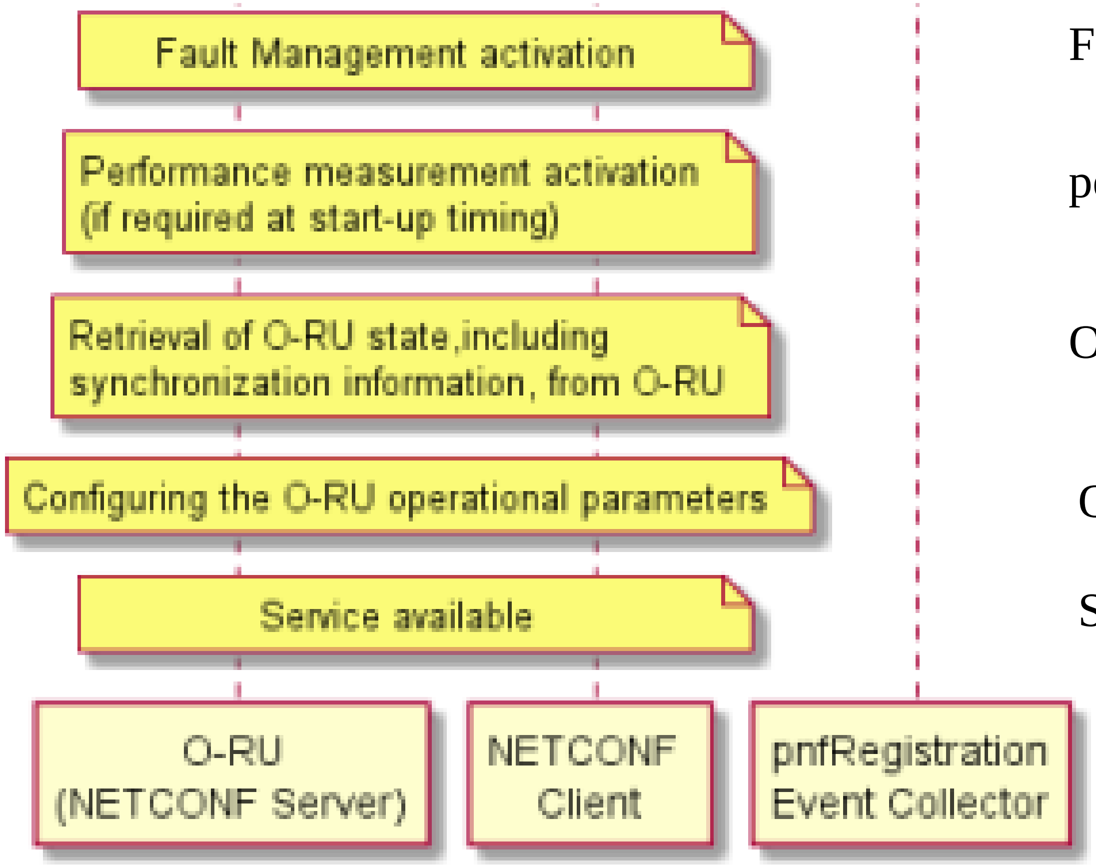
connectivity checking on the O-RU, enabling the O-DU

O-RU delay profile from the O-RU

U-Plane configuration between O-DU and O-RU

O-RU delay profile from the O-RU
U-Plane configuration between O-DU and O-RU
C/U-Plane delay measurements between O-DU and O-RU

Neo SASTECH



Fault Management activation

performance measurement

O-RU state

O-RU operational parameters

Service available

Neo SASTECH

3.1 Management Plane Transport aspects

Pre-condition:

- Physical interface is connected.
- When operating in an environment using call-home, the NETCONF server and NETCONF Client(s) have an identical NETCONF call home port configured, to ensure the NETCONF client listens on the same port used by the NETCONF Server.

Post-condition:

- Transport Layer address(es) for M-plane are known to O-RU and O-RU controllers.
- O-RU is aware of the physical port(s) for M-plane, e.g., if there are multiple ports in the O-RU.
- O-RU is aware of the VLAN(s) to be used for M-Plane, e.g., if VLANs are used in the transport network.
- Then O-RU is ready to establish TCP connection for NETCONF call home and/or for PNF registration.

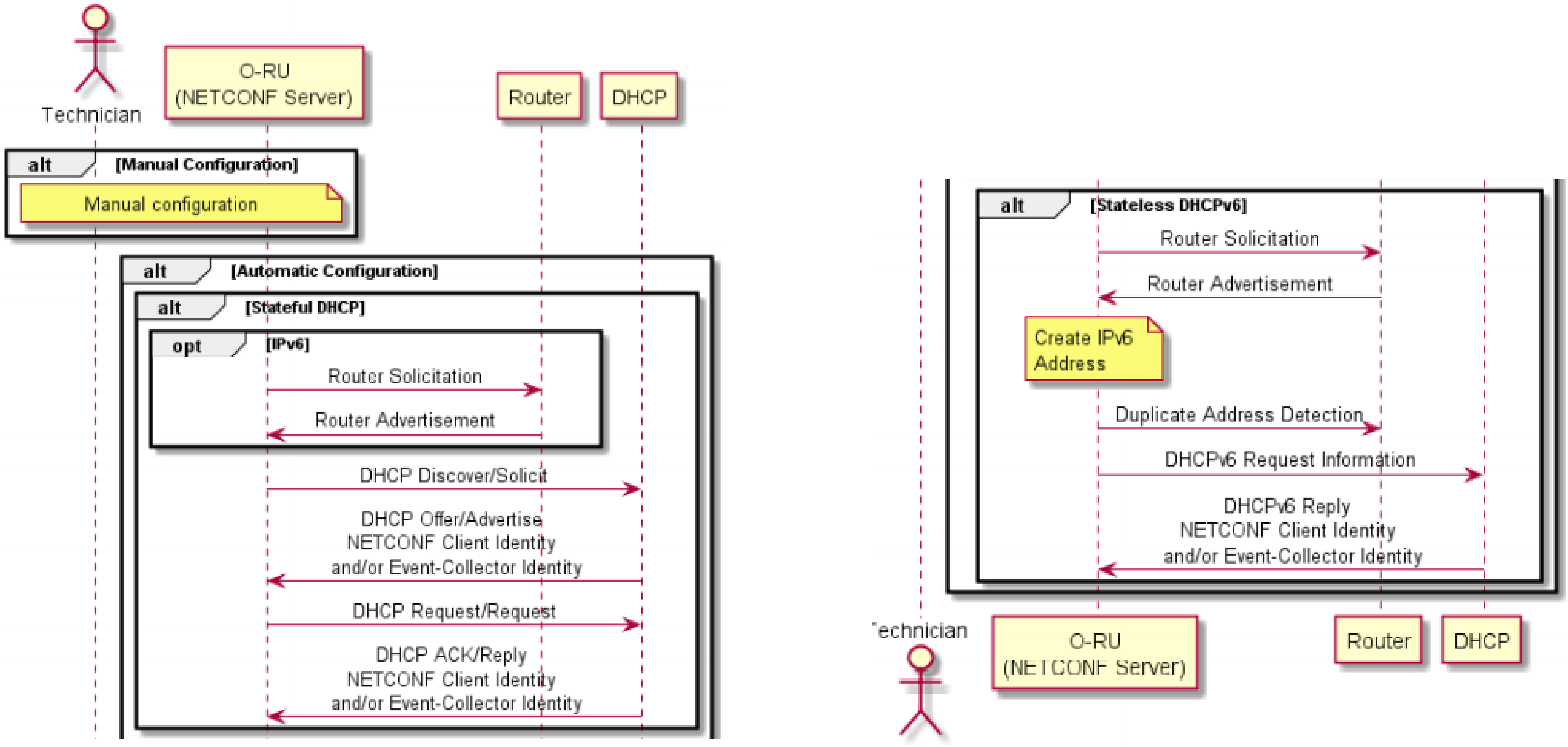
For the transport establishment,

a. Manual transport layer address configuration in O-RU
b. DHCP server provides O-RU’s transport layer address information together with the identity of the NETCONF client and/or the identity of the event-collector.
c. If IPv6 is supported, Stateless Address Auto-Configuration (SLAAC) is used to configure the O-RU’s transport address with the DHCP server providing the identity of the NETCONF client and/or event-collector.

Neo SASTECH

The O-RU uses the o-ran-dhcp.yang model to be able to expose information signaled by the DHCP server.

Transport Layer Establishment for M-plane



Neo SASTECH

3.1.1 O-RU identification in DHCP : o-ran-dhcp YANG model.

DHCPv4 Vendor Class Option:

- Option: 60
- Vendor Class Identifier Option 60: string

The format of the vendor class string shall be configured to one of the following three options:

1. ““o-ran-ru2/<vendor>, e.g., “o-ran-ru2/vendor
2. “o-ran-ru2/<vendor>/<product-code>”, e.g., “o-ran-ru2/vendorA/ORUAA100”
3. “o-ran-ru2/<vendor>/<product-code>/<serial-number>”,e.g. , “**o-ran-ru2/vendorA/ORUAA100/FR1918010111**”

DHCPv4 Vendor-Identifying Vendor Class Option:

Option: 124

Enterprise number: O-RAN-alliance 53148

Vendor-Class-Data: the format of the string shall follow the rules defined for the DHCPv4 Vendor Class Option

DHCPv6 Vendor Class Option:

Option: 16

Enterprise number: O-RAN-alliance 53148

Vendor-Class-Data: the format of the string shall follow the rules defined for the DHCPv4 Vendor Class Option

3.1.2 Management Plane VLAN Discovery Aspects

At start up, the O-RU will typically not be able to immediately determine whether its ports are attached to remote transport equipment configured for access or trunk mode operation.

Once an O-RU completes its boot-up sequence and Ethernet connectivity is detected on at least one of its Ethernet interfaces, the O-RU starts management plane connection establishment.

The O-RU needs to determine whether it is connected to an access port or a trunk port.

An O-RU **may have been previously** configured with management plane VLAN information, for example storing the last VLAN(s) used for management plane connectivity, and/or being previously configured with a range of management plane VLANs by a NETCONF client that has been stored in reset-persistent memory. The O-RU may use this information to optimize its discovery of the VLAN ID(s) used for management plane connectivity.

If the O-RU **does not have previously** configured management plane VLAN information, the O-RU shall attempt to discover DHCP servers on all of its Ethernet ports using untagged Ethernet frames.

If the O-RU does not receive a DHCP OFFER from a DHCP server using untagged frames, or previously configured VLANs, the O-RU should attempt to contact a DHCP server using individual VLANs on all of its Ethernet ports.

3.1.3 O-RU Management Plane IP Address Assignment

1. IPv4 configuration using DHCPv4, RFC2131 [10] enables DHCP servers to configure IPv4 network address(es) on the O-RU.
2. IPv6 Stateless Address Auto-Configuration (SLAAC), RFC4862 [11] enables the O-RU to generate link-local and global addresses
3. IPv6 State-full address configuration uses DHCPv6, RFC3315 [12] and enables DHCP servers to configure IPv6 network address(es) on the O-RU.

3.1.4 O-RU Controller Discovery

O-RUs that have obtained their IPv6 addresses by stateless address auto-configuration, shall use stateless DHCPv6, RFC3736 [13], to obtain management plane configuration information.

Other O-RUs operating using stateful IPv4 or IPv6 address allocations shall obtain management plane configuration information **during IP address allocation**.

The O-RU as NETCONF Server shall be able to recover NETCONF Client information using the following DHCP Options, RFC8572 [14]:

- DHCPv4 OPTION V4_SZTP_REDIRECT [143]
- DHCPv6 OPTION_V6_SZTP_REDIRECT [136]

The definition of the types used within the DHCPv4 option 43/DHCPv6 Option 17 depends on the vendor-class option reported by the O-RU in its DHCP messages.

Neo SASTECH

When a legacy O-RU reports its vendor-class using the “**o-ran-ru**” prefix, the following types are defined:

Type: 0x01 – O-RU Controller IP Address

Type: 0x02 – O-RU Controller Fully Qualified Domain Name

When the O-RU reports its vendor-class using the “**o-ran-ru2**” prefix, the following types are defined:

Type: 0x81 – O-RU Controller IP Address

Type: 0x82 – O-RU Controller Fully Qualified Domain Name

When Type corresponds to an O-RU Controller IP Address, the value encodes IPv4 address(es) in hexadecimal format.

For example, a single server with IPv4 address 198.185.159.144 will be encoded in an option 43 TLV as

Type 0x81 (or x01 for legacy)

Length: 0x04

Value: C6 B9 9F 90 (198.185.159.144)

When Type corresponds to an O-RU Controller Fully Qualified Domain Name, this encodes the string representation of domain name, using ACSII encoding (i.e., following for encoding used for the domain name in the Host Name DHCP Option 12).

For example, a server with FQDN “controller.operator.com” will be encoded in an option 43 TLV as

Type 0x82 (or x02 for legacy)

Length: 0x17

Value: 63 6F 6E 74 72 6F 6C 6C 65 72 2E 6F 70 65 72 61 74 6F 72 2E 63 6F 6D

(Controller.operator.com)

3.1.5 Multi-Vendor Plug-and-Play

O-RU may optionally support certificate enrollment using CMPv2. 3GPP 32.509 specifies how the O-RU can discover the IP address or FQDN of one or more Certification Authority (CA/RA) servers using DHCP Option 43.

An O-RU shall report any discovered multi-vendor plug-and-play servers using the o-ran-dhcp YANG model.

3.1.6 Event-Collector Discovery

The support by an O-RU of PNF Registration to a discovered Event-Collector is optional and hence this section only applies to those O-RUs that support this optional capability.

O-RUs that have obtained their IPv6 addresses by stateless address auto-configuration, shall use stateless DHCPv6, RFC3736 [13], to obtain Event-Collector information. Other O-RUs operating using stateful IPv4 or IPv6 address allocations shall obtain Event-Collector information during IP address allocation. Other O-RUs which have had their IP address(es) manually configured, shall also have their Event-Collector(s) and Event-Collector Notification Format manually configured.

The O-RU shall be able to recover **Event-Collector information** using O-RAN defined vendor specific option to signal Event-Collector information to the O-RU using option 43 for DHCPv4 and option 17 for DHCPv6.

The definition of the types used within the DHCPv4 option 43/DHCPv6 Option 17 are as follows:

Type: 0x83 – Event-Collector IP Address

Type: 0x84 – Event-Collector Fully Qualified Domain Name

Type: 0x85 – Event-Collector Notification Format

For example, an Event-Collector with IPv4 address 198.185.159.144 will be encoded in an option 43 TLV as
Type 0x83 Length: 0x04 Value: C6 B9 9F 90 38
When Type corresponds to an **Event-Collector Notification Format**, the value encodes in what format the Event-Collector expects to receive asynchronous notifications. In this version of the specification, only a single format is defined:
For example, an Event-Collector expecting the pnfRegistration notification to be signaled using the ONAP defined format will encode the option 43 TLV as Type 0x85 Length: 0x01 Value: 00

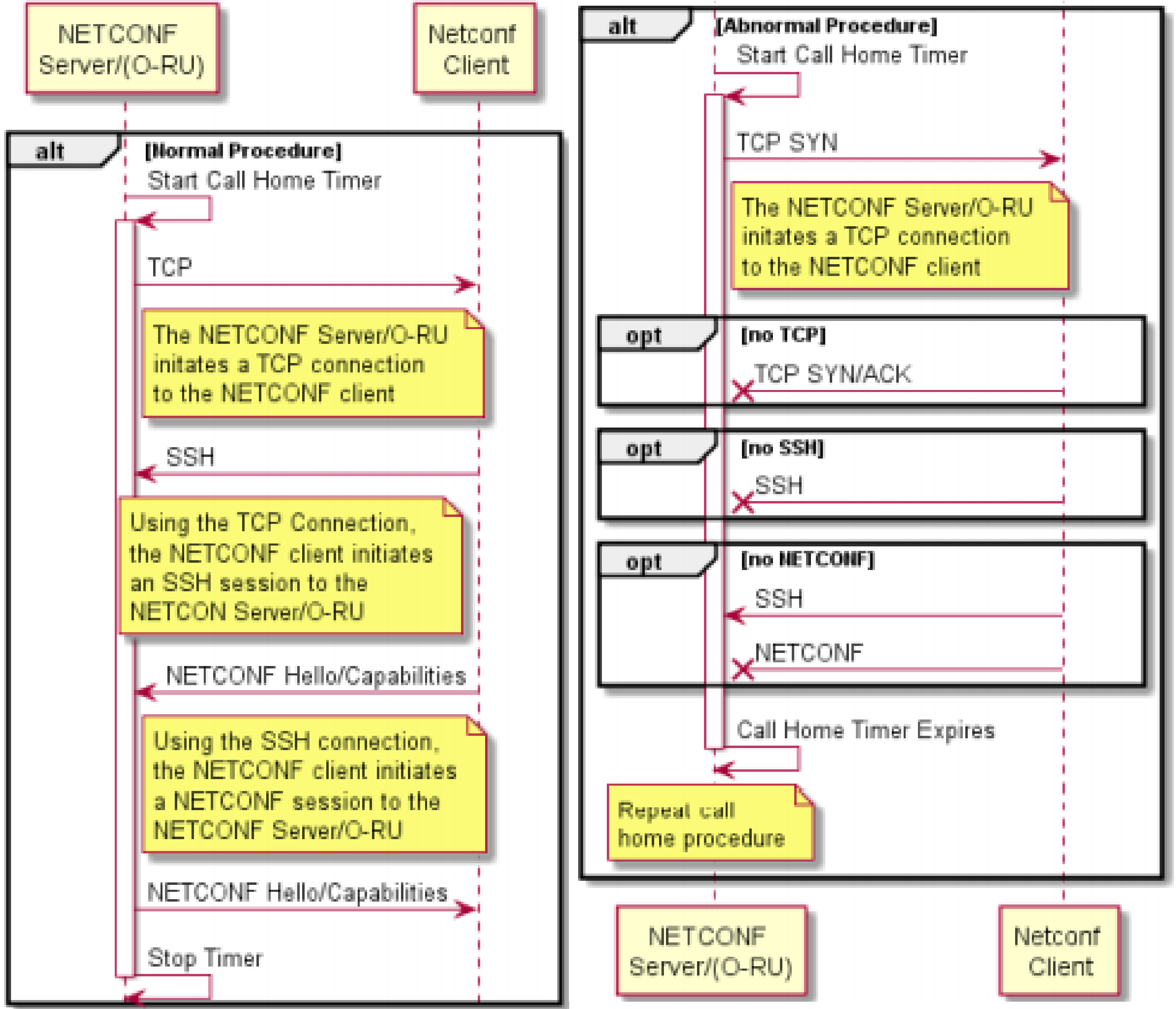
Neo SASTECH

3.2 NETCONF Call Home to O-RU Controller(s)

In order to support NETCONF clients corresponding to known O-RU Controllers that either do not attempt to initiate a NETCONF session with the O-RU, or are prohibited from doing so, e.g., because of Network Address Translation limitations, the O-RU shall **call home** to all known O-RU Controllers with which it does not already have an active NETCONF session.

If the O-RU is unable to establish a NETCONF session with any of the O-RU Controller(s), the O-RU shall use the “**re-call-home-no-ssh-timer**” to repeatedly re-perform the call home procedure to all with which is does not have an established NETCONF session.

Outline of NETCONF call home procedure



3.3 SSH Connection Establishment

The identity of the SSH server (O-RU) shall be verified and authenticated by the SSH client (NETCONF client) according to local policy before password-based authentication data or any configuration or state data is sent to or received from the SSH server.

Public key-based host authentication shall be used for authenticating the server (RFC 4253) by the clients. In addition, server authentication based on X.509 certificates may also be provided [31].

3.3.1 NETCONF Security

In this version of O-RU Management Plane Specification, the security of the NETCONF protocol is realized using SSHv2. O-RAN NETCONF implementations shall implement RFC 6242 [5] that addresses earlier delimiter issues when using RFC 4742.

3.3.2 NETCONF Authentication

This version of the O-RU Management Plane Specification uses **password authentication method for SSHv2** [6]. In addition, client authentication based on X.509 certificates should also be provided [31].

3.3.3 User Account Provisioning

The NETCONF client with suitable privileges may provision user accounts on the O-RU, including the accounts (users) name, password, group (see Section 3.4 for details of groups/privileges) and whether a particular account is enabled or disabled.

- The username name is a string between **3-32 characters**. 1st must be a lowercase letter. The remaining ~lowercase letter or a number.
- The account-type is an enumeration, indicating whether **password or certificate-based authentication** is used for this account.
- The password is a string between **8-128 characters**. Allowed characters in the password field include lowercase and uppercase letters, numbers and the special characters: ! $ % ^ ( ) _ + ~ { } [ ] . – The password leaf is not present for those user accounts associated with certificate-based authentication.
- The access control group associated with an account (see Section 3.4 for details of groups/privileges).
- Whether an account is enabled. The YANG model ensures that at least one user account is always enabled on the O-RU

3.4 NETCONF Access Control

When multiple NETCONF clients (users) are defined, the NETCONF access control mechanism enables the NETCONF server to limit some operations for one client but allow full access for another client.

In order to support interoperable access control management, the NETCONF Server shall use the IETF NETCONF Access Control Model [RFC8341].

Currently six access control **groups** are defined per SSH session: "sudo", "smo", "hybrid-odu", "nms", "fm-pm", and "swm". The table below maps the group **name** to different privileges. Privileges are defined per namespace for read "R", write "W" and execute "X" rpc operations or subscribe to Notifications.

This mapping shall be encoded in the rule list in ietf-netconf-acm.yang model. This rule list shall be unmodifiable by any NETCONF client

Mapping of account groupings to O-RU module privileges

Module Rules	sudo	nms	fm-pm	swm	smo	hybrid-odu
"urn:o-ran:supervision:x.y"	RWX	---	---	---	---	RWX
"urn:o-ran:hardware:x.y"	RWX	RW-	---	---	RW-	R--
"urn:ietf:params:xml:ns:yang:ietf-hardware"	RWX	RWX	R-X	---	RWX	R-X
"urn:ietf:params:xml:ns:yang:iana-hardware"	R--	R--	R-X	---	R--	R--
"urn:o-ran:user-mgmt:x.y"	RWX note1	---	---	---	RWX note1	RWX note1
"urn:o-ran:fm: x.y "	R-X	R-X	R-X	---	R-X	R-X
"urn:o-ran:fan: x.y "	R--	R--	R--	---	R--	R--
"urn:o-ran:sync: x.y "	RWX	RWX	R--	---	RWX	R-X
"urn:o-ran:delay: x.y "	RW-	R--	R--	---	R--	RW-

Neo SASTECH

Module Rules	sudo	nms	fm-pm	swm	smo	hybrid-odu
"urn:o-ran:module-cap: x.y "	RW-	R--	R--	---	R--	RW-
"urn:o-ran:udpecho: x.y "	RW-	R--	---	---	RW-	R--
"urn:o-ran:operations: x.y "	RWX	RW-	R--	---	RWX	RWX
"urn:o-ran:uplane-conf: x.y "	RWX	RWX	R--	---	R--	RWX
“urn:o-ran:beamforming: x.y”	R-X	R-X	R--	---	R--	R-X
"urn:o-ran:lbm: x.y "	RW-	RW-	R--	---	RW-	R--
"urn:o-ran:software-management: x.y "	R-X	R-X	R--	R-X	R-X	R--
"urn:o-ran:file-management: x.y "	--X	--X	--X	---	--X	---
" urn:o-ran:message5: x.y "	RW-	R--	R--	---	R--	RW-
"urn:o-ran:performance-management: x.y "	RWX	RWX	RWX	---	RWX	R-X
"urn:o-ran:transceiver: x.y "	RW-	RW-	R--	---	RW-	R--
"urn:o-ran:externalio: x.y "	RWX	RWX	---	---	RWX	R--
"urn:o-ran:ald-port: x.y "	RWX	RWX	---	---	RWX[note 3]	RWX
"urn:o-ran:interfaces: x.y "	RWX	RWX	R--	---	RWX	R--
"urn:ietf:params:xml:ns:yang:ietf-ip"	RW-	RW-	R--	---	RW-	R--
"urn:ietf:params:xml:ns:yang:ietf-interfaces"	RW-	RW-	R--	---	RW-	R--
"urn:o-ran:processing-elements: x.y "	RW-	RW-	R--	---	RW-	RW-
" urn:o-ran:mplane-interfaces: x.y "	RW-	RW- [note2]	R--	---	RW-	R--
"urn:o-ran:dhcp: x.y "	R--	R--	R--	---	R--	R--
“urn:o-ran:ald: x.y”	--X	---	---	---	--X [note 3]	--X
“urn:o-ran:troubleshooting: x.y”	--X	--X	--X	---	--X	---
“urn:o-ran:trace: x.y”	--X	--X	--X	---	--X	---
"urn:o-ran:laa: x.y "	RW-	RW-	---	---	R--	RW-
"urn:o-ran:laa-operations: x.y "	--X	---	---	---	---	--X

Neo SASTECH

Module Rules	sudo	nms	fm-pm	swm	smo	hybrid-odu
"urn:o-ran:antcal: x.y "	RWX	R--	---	---	R--	RWX
“urn:ietf:params:xml:ns:yang:ietf-netconf-acm”	RW-	R--	R--	R--	RW-	RW-
"urn:ietf:params:xml:ns:yang:ietf-yang-library"	R-X	R-X	R-X	R-X	R-X	R-X
“urn:ietf:params:xml:ns:yang:ietf-netconf-monitoring”	R-X	R-X	R-X	R-X	R-X	R-X
Module Rules	sudo	nms	fm-pm	swm	smo	hybrid-odu
“urn:ietf:params:xml:ns:yang:ietf-netconf-notifications”	--X	--X	--X	--X	--X	--X
"urn:o-ran:shared-cell:x.y"	RW-	RW-	---	---	R--	RW-
"urn:o-ran:ethernet-fwd:x.y"	RW-	RW-	---	---	RW-	R--
“urn:ietf:params:xml:ns:yang:ietf-subscribed-notifications“	---	---	---	---	RWX	---
"urn:o-ran:ves-sn:x.y"	---	---	---	---	RW-	---

Note1: The rule list for "urn:o-ran:user-mgmt:1.0” shall additionally deny reading of the password leaf by any NETCONF client

Note2: The rule list for “urn:o-ran:mplane-int:1.0” shall additionally deny the writing of the **configured-client-info** container for NETCONF sessions with “nms” group privileges.

Note 3: While the rule list for models related to Antenna Line Devices (ALD) permit SMO configuration privileges, the operation of the current architecture, including requiring the use of regular NETCONF RPCs to tunnel heartbeat messages to the ALD, may limit the scalability of scenarios where the SMO is responsible for the ALD Controller function described in sub-section 11.3.

Neo SASTECH

3.5 NETCONF capability discovery

The O-RU advertises its NETCONF capabilities in the NETCONF Hello message. The Hello message provides an indication of support for standard features defined in NETCONF RFCs as well as support for specific namespaces.

NETCONF capabilities are exchanged between the O-RU and the NETCONF client(s). Examples of capabilities include [3]:

- Writable-running Capability
- Candidate Configuration Capability and associated Commit operation
- Discard change operation
- Lock and un-lock operations
- Confirmed commit Capability
- Cancel commit operation
- Rollback on error capability
- Validate Capability
- Startup configuration capability
- URL capability
- XPATH capability
- Notifications
- Interleave capability

All O-RAN O-RUs shall support the XPATH capability, NETCONF Notifications and at least one of the writeable-running and candidate configuration capabilities.

The NETCONF client uses the get RPC together with sub-tree based and XPATH based to recover particular sub-trees from the O-RU. Please see Chapter 6 for more information on NETCONF based configuration management.

In order to avoid interactions between the operation of **supervision watchdog timer** (see section 3.6) and the **confirmed commit timer** (default value set to 600 seconds in RFC 6241), when using the NETCONF confirmed commit capability, a NECTONF client with “sudo” privileges shall ensure the confirmed-timeout is less than the **supervision-notification-interval** timer (default value 60 seconds in o-ran-supervision.yang).

Neo SASTECH

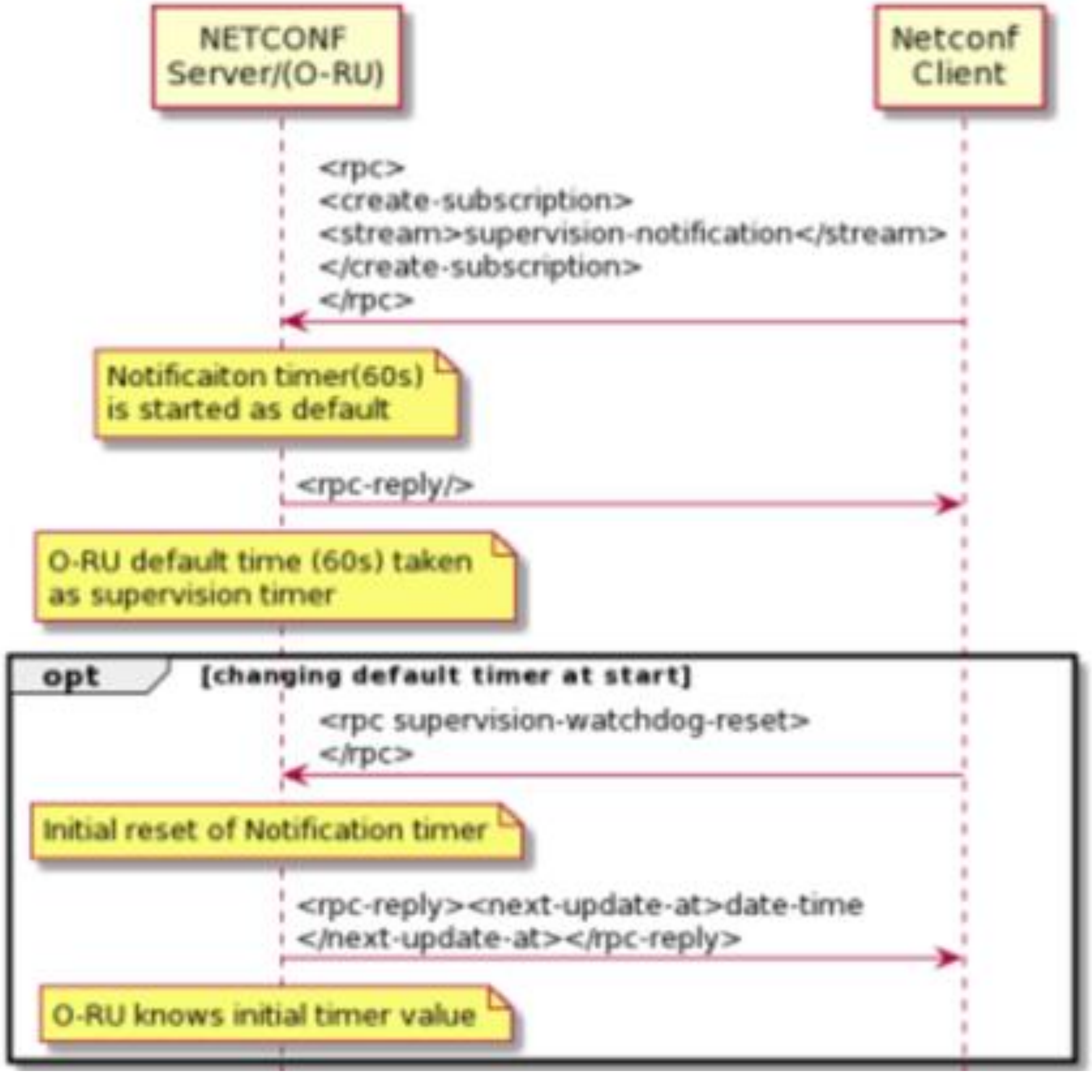
3.6 Monitoring NETCONF connectivity

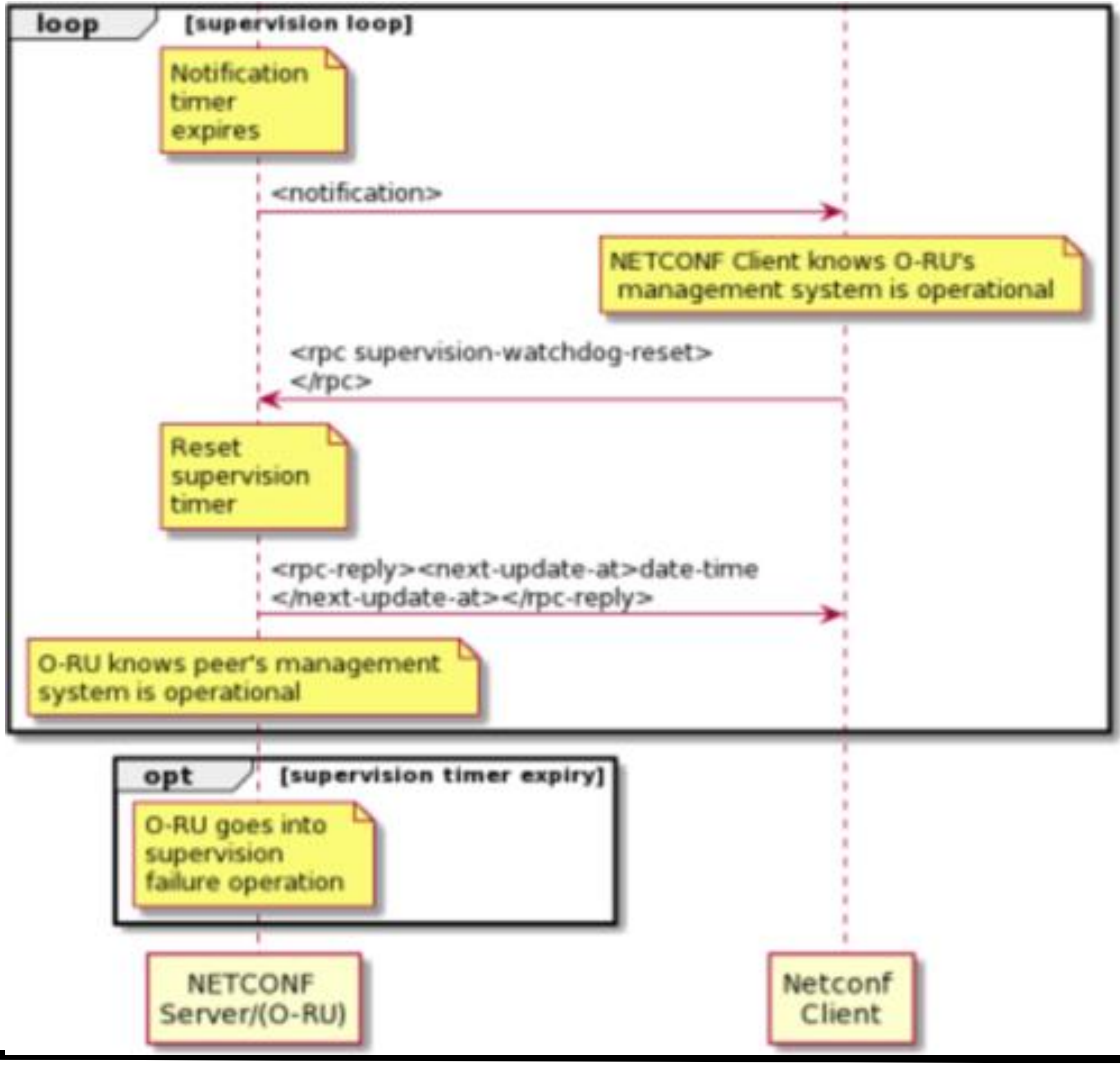
When having a session with a NETCONF client with “sudo” or “hybrid-odu” access privileges, the O-RU operates a **watchdog supervision timer** to ensure that the session to the NECTONF client is persistent, as described in section 3.4. Additionally, the O-RU provides NETCONF Notifications to indicate to remote systems that its management system is operational. This supervision is intended to be used with the NETCONF client associated with the operation of the peer to the O-RAN Radio’s lower layer split.

- **Notification timer**:
  Value: Equal to supervision-notification-interval (default value: 60s)
  Operation: The O-RU sends supervision-notification to those NETCONF clients that have subscribed to receive such notifications. The O-RU sends supervision-notification, at the latest when the timer expires. The O-RU Controller confirms that NETCONF connectivity to the O-RU is operational by receiving the notification.
- **Supervision timer**:
  Value : Equal to supervision-notification-interval (default value: 60s) + guard-timer-overhead (default : 10s)
  Operation: The O-RU goes into supervision failure operation when the timer expires. This means that a NETCONF client with sudo privileges should repeatedly reset this supervision timer. The O-RU confirms that NETCONF connectivity to the O-RU Controller is operational.

Neo SASTECH

Monitoring NETCONF Connectivity





Neo SASTECH

3.7 Closing a NETCONF Session

A NETCONF client closes an existing NETCONF session by issuing the RPC **close-session** command. The O-RU shall respond and close the SSH session. The O-RU shall then re-commence call home procedures, as described in Section 3.2.

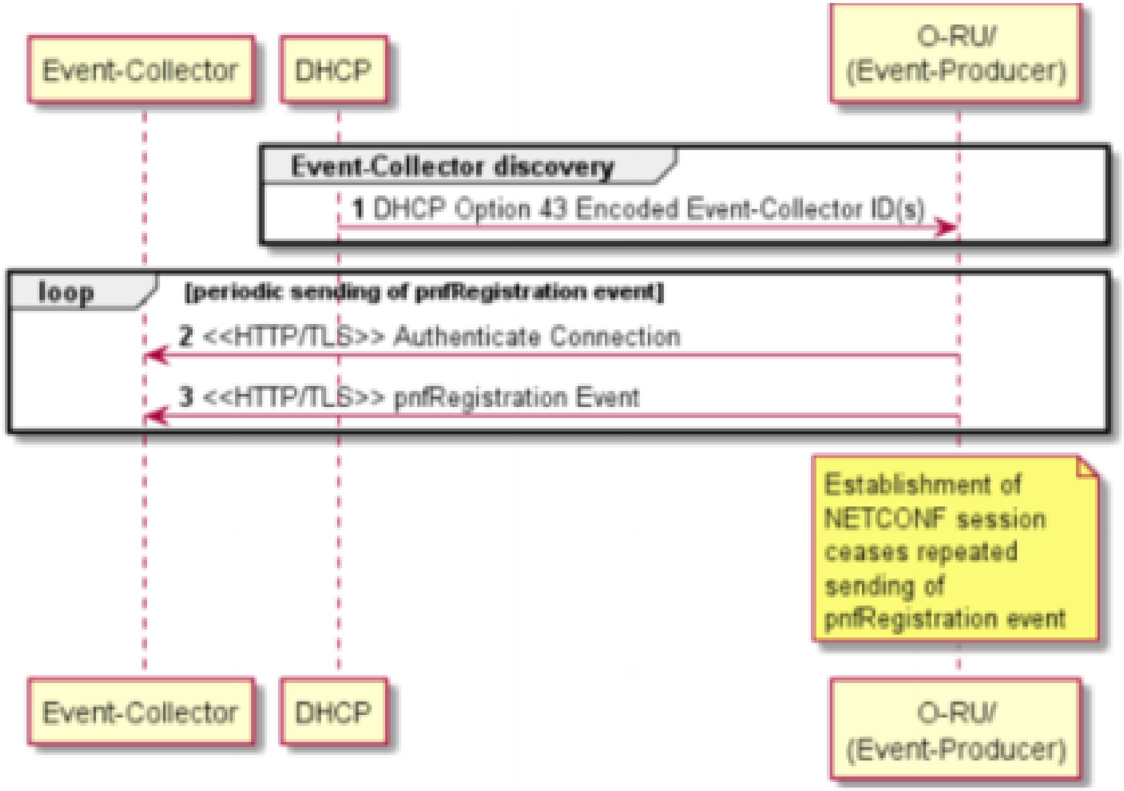
3.8 PNF Registration (V5.0)

The support by an O-RU of PNF Registration to a discovered Event-Collector is optional and hence this section only applies to those O-RUs that support this optional capability.

3.8.1 PNF Registration Procedure

The pnfRegistration notification is a JSON encoded message sent from the O-RU to the discovered Event-Collector using REST/HTTPS. **When performing PNF Registration**, the O-RU shall send the pnfRegistration notification to all discovered Event-Collectors. The sending of the pnfRegistration event is repeated periodically until the O-RU receives a request to establish a NETCONF session from the SMO.

PNF Registration Procedure



Neo SASTECH

3.8.2 Encoding of PNF Registration Notification

The pnfRegistration notification shall include the IP address information necessary for a NETCONF client to establish IP connectivity to the NETCONF Server in the O-RU, i.e., shall include the field oamV4IpAddress when the O-RU has a configured IPv4 interface and/or the field oamV6IpAddress when the O-RU has a configured IPv6 interface.

The contents of the pnfRegistration message are derived from the **O-RU's configuration database**. An O-RU shall support the o-ran-hardware.yang model revision 5.0.0, or later, which defines the schema nodes corresponding to unitFamily and unitType values and the o-ran-operations.yang model revision 5.0.0, or later, which defines the schema nodes corresponding to the version of pnfRegistration fields.

PnfRegistration Field	M/C/O	YANG Operational Data
lastServiceDate	O	/hw:hardware/hw:component/or-hw:last-service-date
macAddress -	O	/if:interfaces/if:interface/o-ran-int:mac-address
manufactureDate	O	/hw:hardware/hw:component/hw:mfg-date
modelNumber	M	/hw:hardware/hw:component/hw:model-name
oamV4IpAddress	C	/if:interfaces/if:interface/ip:ipv4/ip:address/ip:ip
oamV6IpAddress	C	/if:interfaces/if:interface/ip:ipv6/ip:address/ip:ip
pnfRegistrationFieldsVersion	M	/o-ran-ops:operational-info/o-ran-ops:declarations/o-ran-ops:supported-pnf-registration-fields-version
serialNumber	M	/hw:hardware/hw:component/hw:serial-num
softwareVersion	M	/hw:hardware/hw:component/hw:software-rev
vendorName	M	/hw:hardware/hw:component/hw:mfg-name