



ONAP PNF Plug and Play for Casablanca (R3, 4Q 2018)







- ONAP and PNF Plug and Play for 5G RAN
- 5G Use Case Team



PNF Plug and Play CASABLANCA IMPROVEMENTS OVERVIEW

- ONAP and PNF Plug and Play for 5G RAN
- 5G Use Case Team

Casablanca R3 Summary Overview

TOPIC	ICON	DESCRIPTION
PNF Registration Handler (PRH) Improvements		New VES Event domain for PNF registration with corresponding support in VES collector, DMaaP and PRH.
SO Workflow enhancements		Introduction of dedicated 5G use case work-flow
Service Configuration Improvement		Service configuration improvements from PNF Controller (APP-Cr, SDN-Cr) to PNF after PNF registration to PRH
Security Enhancements		Authentication, Certificates, User name & password and intra-ONAP security.
Modeling enhancements		Modeling enhancements to support 5G PNF in ONAP. Inheritance, and PNF characteristics for sharing. Focusing on PNF connectivity. PNF-SDK.
PNF Onboarding / Package		Defining <i>PNF Onboarding Package</i> . Extending framework to work with PNFs. Defining PNF Package framework.

PRH Enhancements

DESCRIPTION

PNF Registration Handler (PRH) Enhancements.

(1) New VES Event domain for PNF Registration –

Create new VES event domain for PNF registration with corresponding support in VES collector, DMaaP and PRH. In Beijing the PnP Use case used the “*other*” domain to register VES events. For Casablanca, we propose using a dedicated domain “*pnfRegistration*”. New DMaaP topic corresponding to new domain.

(2) VES EXTENSIONS - As a result, VES collector and VES agent content will change with field updates using the new domain. Extensions for pnfRegistration fields. Corresponding VES Schema change.

(3) DU SIMULATOR UPDATE – The registration VES event used by the DU Simulator (or actual PNF) will need to update its JSON payload to match the changes above.

(4) PRH & AAF INTEGRATION – PRH needs to interface to AAF for Intra-ONAP security. PRH needs to use certificates and tokens for authentication to be allowed to exchange events. PRH needs this authorization to publish to DMaaP topics.

(5) REVIEW LIBRARIES – comply to Linux foundation requirement for licensing & security vulnerabilities. Risk estimation.

(6) DEMO – Demo of PRH w/ PNF PnP in 5G Use Case



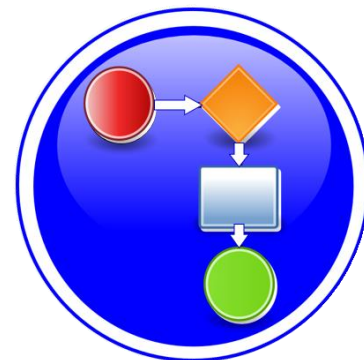
PROJECTS

PNF Registration Handler, DMaaP, DCAE

PNF PnP: SO Workflow Enhancements

DESCRIPTION

- (1) SO WORKFLOW ENHANCEMENTS** –
Dedicated 5G BTS Workflow in SO. (If not model-driven would need special 5G BTS workflow)
- (2) PNF WORKFLOW** – Extensions to Beijing SO Workflow (part of VCPE workflow).
Developed in Beijing not tested or integrated.
- (3) MODEL DRIVEN** – SO not yet model driven.
Need to solve vis-à-vis a SO work flow specific to service & resource use case.
- (4) UPDATE PNF WORKFLOW** – needs to be officially tested, accepted (in Casablanca).
- (5) PNF Controller TO SO INTERACTION** –SO calls PNF Controller (SDN-R, Generic API call vs REST call)
- (6) DFX (Design for Excellence)** – Resilience, Performance, Scalability, Stability, Multi-site.



PROJECTS

SO

SERVICE CONFIGURATION ENHANCEMENT

DESCRIPTION

- (1) Service configuration Enhancements** to ONAP Controller to PNF *service configuration* exchange with PNF.
- (2) PROTOCOL DEFINITION** – Better definition around the Protocols supported (and/or support more protocols). What ONAP controller supports what PNF and what protocols are supported. NetConf, Ansible, Chef.
- (3) Configuration Extensions** – New parameters needed for Casablanca use cases. Vid script to pushing data, ID config, ID where data comes from. Generic configuration support.
- (4) PNF PnP Config** – Finishing PNF PnP by sending down config data.
- (5) (OPTIONAL) Vendor Data** – Extensions to Service Configuration with Vendor specific configuration data can be developed (vendor dependent).



PROJECTS

ONAP Controller (SDN-R), VID, SO,
SDC/CDT

SECURITY ENHANCEMENTS

DESCRIPTION

- (1) PNF AUTHENTICATION** – DCAE must authenticate the HTTP/TLS connection from the PNF. DCAE to integrate the HTTP and TLS authentication functionality by AAF.
- (2) VENDOR CERTIFICATES** – Handling Vendor Certificates for TLS/SSH for PNFs.
- (3) USER NAME & PASSWORDS** – Provisioning. DCAE & PNF management of *User Name & Passwords*.
- (4) SECURITY BETWEEN COMPONENTS** – DMaaP & PRH to authenticate w/ other ONAP components.



PROJECTS

PNF Registration Handler, DCAE, AAF,
ONAP Controller, DMaaP

PNF PnP: MODELING ENHANCEMENTS

DESCRIPTION

- (1) PNF MODELING** – Modeling enhancements to support 5G PNF in ONAP. Model Inheritance definitions for PNF. SDC modeling improvements from Beijing PnP use case.
- (2) PNF SHARING** – SDC model updates for PNF characteristics focusing on PNF inter-connectivity.
- (3) PNF-SDK** – SDK provided from Vendors. This will help modeling the Physical “Box” (PNF) and network functions.
- (4) CDT ENHANCEMENTS** - Improving CDT to handle complex config templates, multiple templates per PNF, identify different sources for template data, integrating CDT into SDC, expanding CDT usage to other controllers.



PROJECTS

SDC, CDT

PNF ONBOARDING / PNF PACKAGE

DESCRIPTION

PNF Onboarding and PNF Package

(1) PNF PACKAGE DEFINITION – Defining *PNF Onboarding Package*. Extending framework to work with PNFs. Defining PNF Package framework.

- A. **PNF ARTIFACTS DEFINITION** – Vendor specific/provided artifacts to add to the (new PNF) package.
- B. **PNF ARTIFACTS DISTRIBUTION**



PROJECTS:
SDC, APP-C



PNF Plug and Play IN CASABLANCA (R3)

- ONAP and PNF Plug and Play for 5G RAN
- 5G Use Case Team

PNF Plug and Play Stages

Design Time

A



PNF Modeling

Resources Definition/Services Definition
SDC: PNF (physical element) Modeling
Distribution of types



B



PNF Instance Declaration

PNF Infrastructure Service Declaration
First part of PNF instantiation
DCAE & AAI Entry with PNF ID (e.g. MAC address)



C



PNF Boot-strapping

PNF Powers up and Boot-straps
PNF performs a “Plug and Play” procedure
Equipment vendor proprietary steps

D



PNF Contacts ONAP

PNF connects to ONAP via a Registration Event
PNF Registration Handler (PRH) processes the event
Generic (not vendor proprietary)

E



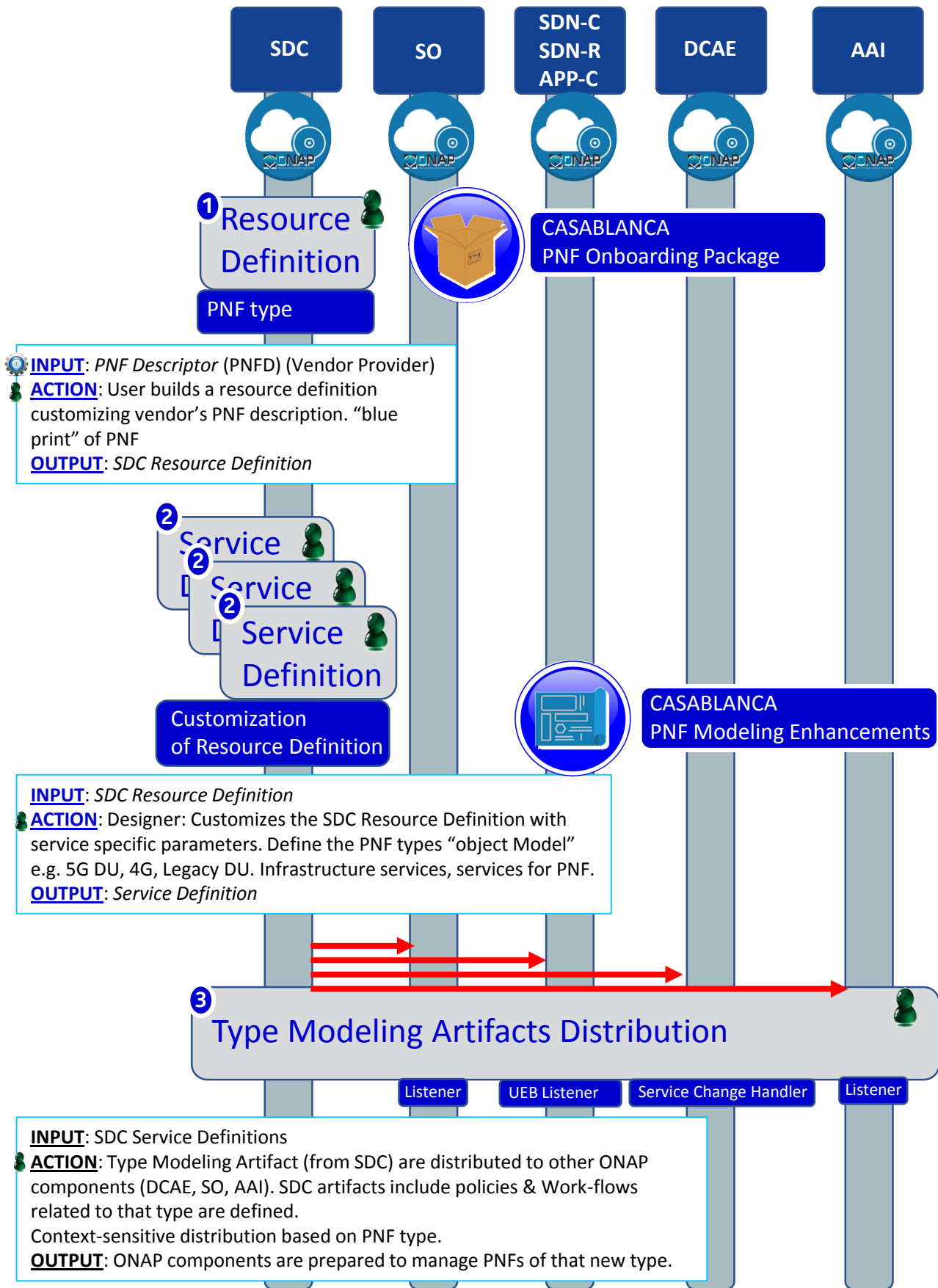
PNF Activation

Connection points configured
Second part of PNF service instantiation
PNF configured and ready to provide service

Run-Time (Instances)

ACTORS	DESCRIPTION
PNF	PHYSICAL NETWORK FUNCTION (PNF) – A Network Function that is hosted on a physical hardware device, not in the cloud infrastructure.
DHCP	DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP) – Protocol to assign IP addresses to a network element (NE). The IP address can be dynamically assigned or static based on MAC address of PNF.
SEGW	SECURITY GATEWAY – Used to set up IPSec tunnels to protects against unsecured traffic entering an internal network of a operator; used by enterprises to protect their users from accessing and being infected by malicious traffic.
CA/RA	CERTIFICATE AUTHORITY / REGISTRATION AUTHORITY – Used to generate a service provider certificate for the PNF.
Initial EM	INITIAL EM – Provides basic configuration and software download services to the PNF. This might be a equipment vendor specific solution. Also, responsible for identifying a PNF.
SDN-C	SOFTWARE DEFINED NETWORK CONTROLLER (SDN-C) – A controller for Layer 0 to 3 devices. Manages transport and network connections.
DCA&E	DATA COLLECTION, ANALYTICS AND EVENTS (DCAE) – Gathers performance, usage, and configuration data from the managed environment. Collect, store data and provides a basis for analytics within ONAP. For PNF Plug and Play can potentially perform analytics on the Plug and Play process, statistics, logs.
A&AI	ACTIVE & AVAILABLE INVENTORY – The PNF is identified as available inventory and tracked through a key which is the PNF ID. When onboarded the PNF gets an entry in A&AI and can then be tracked, requested, and seen by the ONAP components for service requests or other queries.
SO	SERVICE ORCHESTRATOR – Serves as a mediator and coordinator of service requests.
APP-C	APPLICATION CONTROLLER (APP-C) - A controller for Layer 4 to 7 applications. Manages the life cycle of virtual applications, virtual network functions (VNFs), and components. APP-C manages the 5G DU & 4G DU.
PNF Registration Handler	PNF Infrastructure Manager – A microservice in DCAE used during PNF Plug-n-Play to process the PNF Registration event.

Design Time (ONAP)



PNF PnP: MODELING ENHANCEMENTS

DESCRIPTION

- (1) PNF MODELING** – Modeling enhancements to support 5G PNF in ONAP. Model Inheritance definitions for PNF. SDC modeling improvements from Beijing PnP use case.
- (2) PNF SHARING** – SDC model updates for PNF characteristics focusing on PNF inter-connectivity. DCAE-DS Micro-service modeling.
- (3) PNF-SDK** – SDK provided from Vendors. This will help modeling the Physical “Box” (PNF) and network functions.
- (4) CDT ENHANCEMENTS** - Improving CDT to handle complex config templates, multiple templates per PNF, identify different sources for template data, integrating CDT into SDC, expanding CDT usage to other controllers.



PROJECTS

SDC, CDT

PNF ONBOARDING / PNF PACKAGE

DESCRIPTION

PNF Onboarding and PNF Package

(1) PNF PACKAGE DEFINITION – Defining *PNF Onboarding Package*. Extending framework to work with PNFs. Defining Package framework.

- A. **PNF ARTIFACTS DEFINITION** – Vendor specific/provided artifacts to add to the (new PNF) package.
- B. **PNF ARTIFACTS DISTRIBUTION**

TOSCA Meta data - main service template, TOSCA template.

Artifact Package. Separated by types of artifacts. Separations by folder for different types. Place artifacts in categories. Anyone can choose which artifacts to receive.

Definitions – Specifies definitions such as CM, FM and PM definitions

(1) Protocols Supported – PNF package. CM Protocol is in PNF onboarding package. (Chef, Ansible, NetConf)

(2) Controller – What is the PNF controller

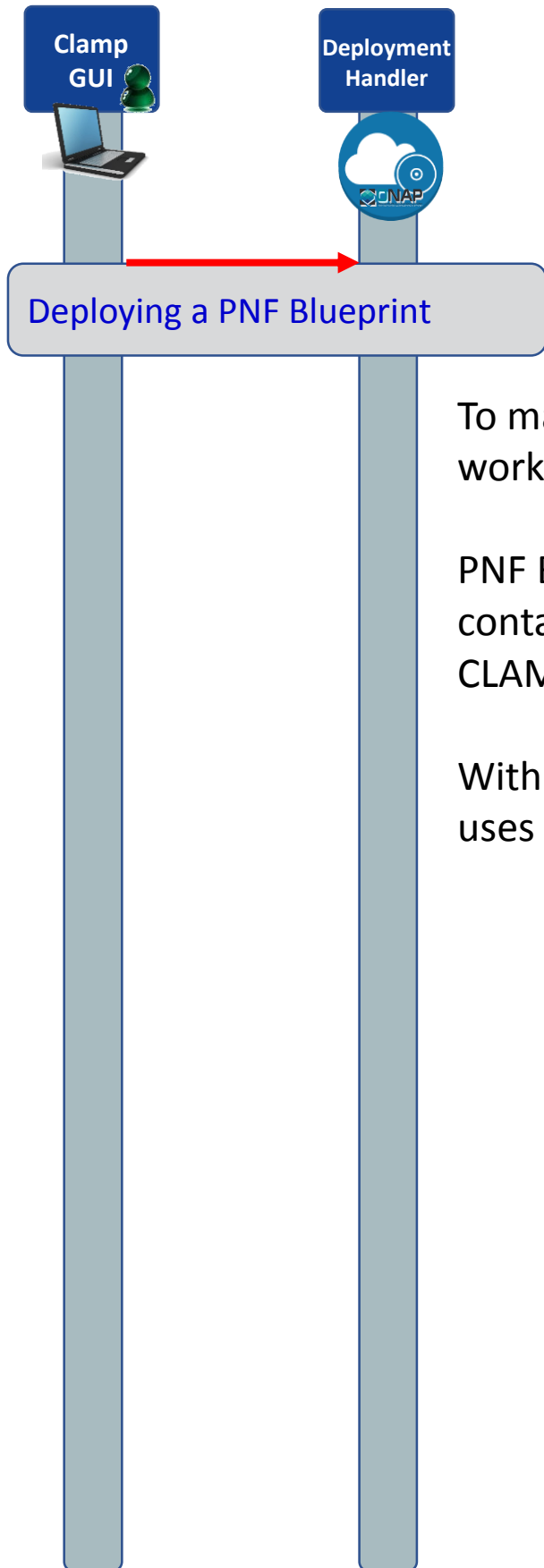


PROJECTS:

SDC, APP-C

STEP	DESCRIPTION
1	<p>RESOURCE DECLARATION – A user on the VID performs a Resource Declaration. This uses the Service definition created in SDC. The user on the VID can define known information about the PNF. The user can (optional) provide the following information</p> <p>PNF RESOURCE Definition</p> <ul style="list-style-type: none"> Resource Type – Type of Resource. NEW type: PNF (pre-defined in SDC) NAME – Name of the PNF type CATEGORY – e.g. Infrastructure TAGS – User-definable tags (default name of the PNF) DESCRIPTION – Textual description CONTACT ID – Designer (user of ONAP) VENDOR – PNF Vendor (e.g. Nokia) VENDOR RELEASE – Vendor release VENDOR MODEL NUMBER – PNF Model value (link to A&AI) EVENTS – Monitoring Event definitions. Define design-time templates. CLAMP (runtime monitoring), DCAD (design time design template attach to VNF). Define templates & attach them. <p>Note: The user may provide whatever information in the above fields they know. Note: Consumer vs Enterprise deployments. Consumer systems pre-registered, distributed throughout a region. For a consumer deployment you might not know the MAC address/Serial number (PND IF) until the PNF connects to ONAP.</p>
2	<p>SERVICE Definition (uses a PNF)</p> <ul style="list-style-type: none"> NAME – Name of the Service (mandatory) CATEGORY – e.g. Network L1...L4, VOIP call Control, Mobility TAGS – User-definable tags (default name of the PNF) DESCRIPTION – Textual description of service (mandatory) CONTACT ID – Designer (user of ONAP) (mandatory) PROJECT CODE – ID (mandatory) Ecomp-Generated Naming – Name Naming Policy – Policy to be used to assign a name to a service by SO/SDNC SERVICE TYPE – Type of service SERVICE ROLE – The Role of this service. ENVIRONMENTAL CONTEXT – distributed environments Specific Service(?) – PNF, allotted resource from a CU Service <p>The “basic” model are extended. Inherit (OO) from existing model. Vendor takes standard node types and creates their own extension. CDT (Configuration Design Tool) (GUI) to build artifacts to be used by APP-C (Tosca models) for a configure Template.</p>
3	<p>DISTRIBUTION – Event Monitoring Templates distributed. (?)</p>

Deployment Handler (VES Collector)



To make a VES Collector in DCAE work properly

PNF Blueprint will be docker container. May be deployed from CLAMP or Cloudify Orchestrator.

Within VES Collector schema uses "Adder" (existing)

STEP	DESCRIPTION
1	<p>DEPLOYMENT HANDLER PNF BLUEPRINT – The Deployment handler is necessary to use, to give it the PNF blueprint so that later on in the Plug and Play flow, DCAE will recognize the PNF. The PNF Blueprint will be docker container. The PNF blueprint May be deployed from CLAMP or Cloudify Orchestrator to DCAE. Within VES Collector schema uses “Adder” (existing).</p>

PNF Resource Declaration

BSS Portals
VID
AAI UI



AAI



OPT

4

Resource Declaration & Create A&AI PNF Entry



A&AI entry of Inactive PNF, PNF Type Resource Declaration

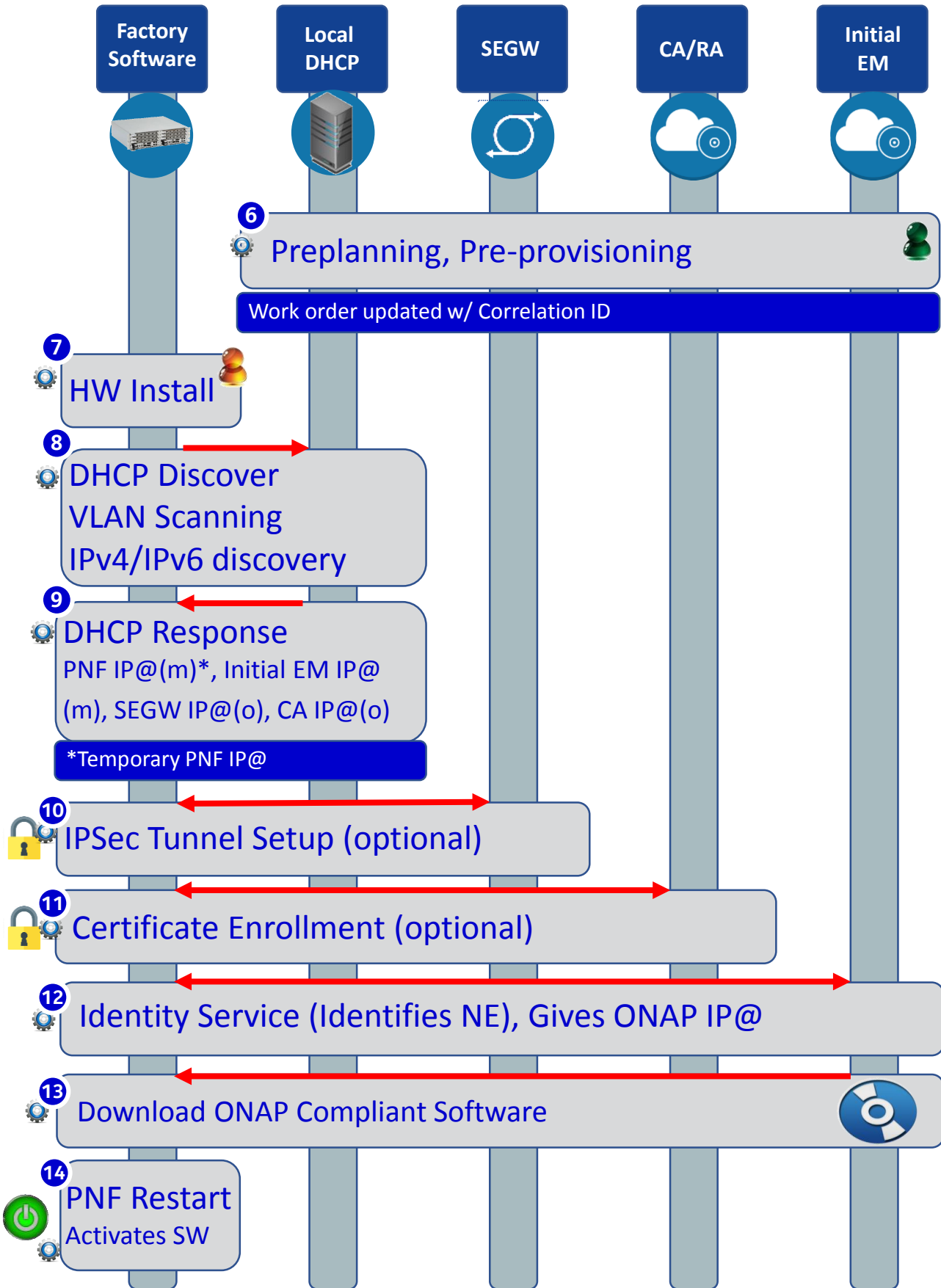











Inactive PNF
A&AI entry

Steps 15-22 accomplishes this purpose but service providers can choose to implement this flow to augment (e.g. service providers inventory management system)

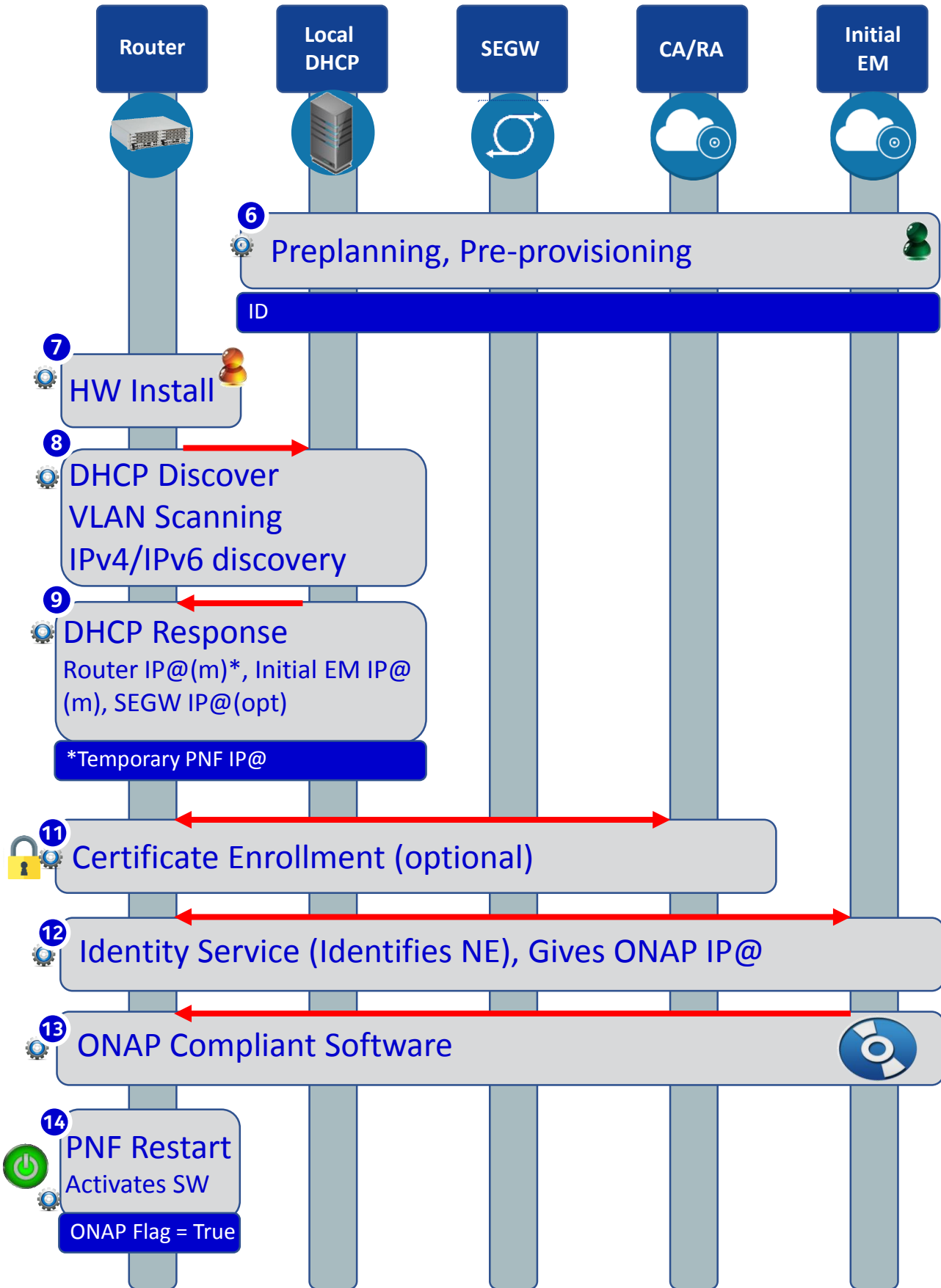
STEP	DESCRIPTION
4	<p>RESOURCE DECLARATION – A user on the VID performs a Resource Declaration. This uses the Service definition created in SDC. The user on the VID can define known information about the PNF. The user can (optional) provide the following information</p> <p>PNF RESOURCE Definition</p> <ul style="list-style-type: none"> Resource Type – Type of Resource. NEW type: PNF (pre-defined in SDC) NAME – Name of the PNF type CATEGORY – e.g. Infrastructure TAGS – User-definable tags (default name of the PNF) DESCRIPTION – Textual description CONTACT ID – Designer (user of ONAP) VENDOR – PNF Vendor (e.g. Nokia) VENDOR RELEASE – Vendor release VENDOR MODEL NUMBER – PNF Model value (link to A&AI) EVENTS – Monitoring Event definitions. Define design-time templates. . <p>The PNF entry in AAI is created by the PRH with the PNF ID (or correlation ID) address. After this step, the PNF is considered to be created but inactive within ONAP. It can then be later used in the second part of service instantiation. See Step 28.</p> <p>(OPTIONAL) IP address of PNF may be set during this step</p>









PNF Plug and Play Steps (for 5G DU)



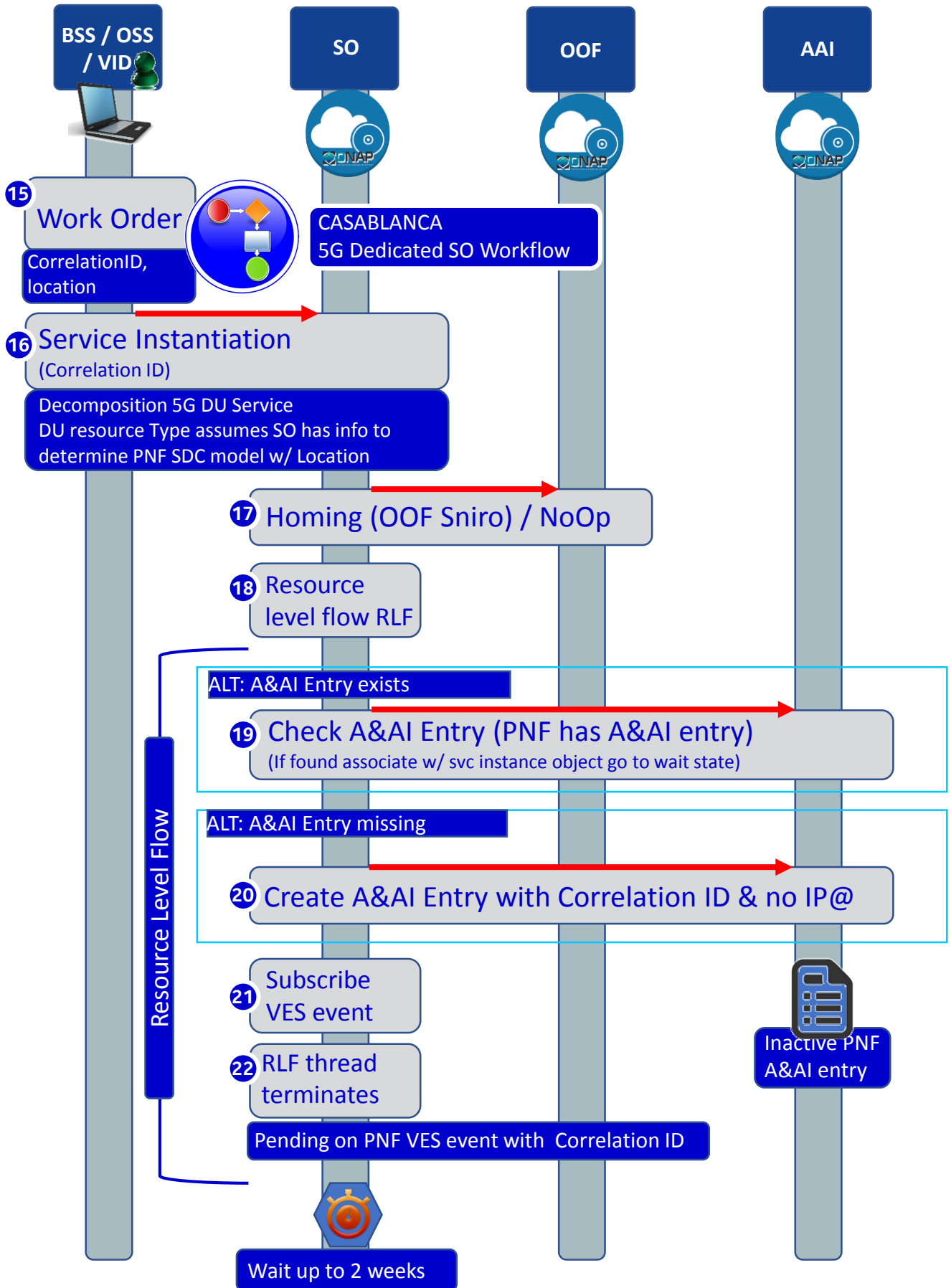
STEP	DESCRIPTION (Plug and Play Vendor steps for Infrastructure components)
6 	<p>PRE-PLANNING, PRE-PROVISIONING – There is data which is programmed into the system for the PNF Plug and Play operation. The user programs the local DHCP IP address(@), the Security Gateway IP@, the CA/RA certificate information, the management plane IP address (the ONAP IP@), the software service IP@ for use by the PNF during the onboarding process.</p> <p>Note: <i>The CU is instantiated ahead of time with the expected DUs that it should be connected to (that is outside the scope of this flow).</i></p> <p>Note: The user name & password which the PNF needs to know to contact and get through the vAAA server before it contacts ONAP.</p>
7 	<p>HW INSTALL – The physical hardware is installed at the site. Site licensing, real estate contacts, zoning, and physical hardware of the PNF is installed by technicians. Power, backhaul, and antennas are installed and connected.</p>
8 	<p>INITIAL NETWORK ACCESS – A DHCP Discover procedure is executed when the PNF powers on, VLAN Scanning is performed, and IPv4/IPv6 discovery is done. The DHCP Discover message exchange provides an entryway into the network and is designed as an procedure for a network element to be able to find connection to the network from “scratch”. VLAN Scanning and IPv4 vs IPv6 discovery is done as well.</p>
9 	<p>DHCP RESPONSE – The DHCP response returns a PNF IP address, the initial EM IP address, Security Gateway IP address (optional), and certificate authority IP address (opt). It is possible the PNF IP address is a temporary IP address used for initial connectivity purposes, and that a permanent PNF IP address will be granted later.</p>
10 	<p>IPSEC TUNNEL – An IP Sec Tunnel is established which uses cryptography to provides a secure connection. IPSec has two security services: Authentication header and an encapsulating security payload with tunnel and transport modes.</p>
11 	<p>CERTIFICATE ENROLLMENT – The process where the PNF gets a service provider certificate from the Certificate authority. The certificate is then used to authenticate and verify the PNF.</p>
12 	<p>IDENTITY SERVICE – The identity service is there to identify the PNF. It also returns the ONAP (DCAE) IP address.</p>
13 	<p>ONAP COMPLIANT SOFTWARE – The PNF contacts the initial EM and downloads the ONAP Bootstrap software. This is a software package that is meant to perform the remaining steps of PNF registration and activation onto ONAP</p>
14 	<p>PNF RESET – The PNF is reset so that the downloaded ONAP Bootstrap software becomes activated and is then ready to continue to PNF registration</p>

PNF Bootstrapping Steps (for Routers)



STEP	DESCRIPTION (Plug and Play Vendor steps for Infrastructure components)
6 	<p>PRE-PLANNING, PRE-PROVISIONING – There is data which is programmed into the system for the PNF Plug and Play operation. The user programs the local DHCP IP address(@), the Security Gateway IP@, the CA/RA certificate information, the management plane IP address (the ONAP IP@), the software service IP@ for use by the PNF during the onboarding process.</p> <p>Note: <i>The CU is instantiated ahead of time with the expected DUs that it should be connected to (that is outside the scope of this flow).</i></p> <p>Note: The user name & password which the PNF needs to know to contact and get through the vAAA server before it contacts ONAP.</p>
7 	<p>HW INSTALL – The physical hardware is installed at the site. Site licensing, real estate contacts, zoning, and physical hardware of the PNF is installed by technicians. Power, backhaul, and antennas are installed and connected.</p>
8 	<p>INITIAL NETWORK ACCESS – A DHCP Discover procedure is executed when the PNF powers on, VLAN Scanning is performed, and IPv4/IPv6 discovery is done. The DHCP Discover message exchange provides an entryway into the network and is designed as an procedure for a network element to be able to find connection to the network from “scratch”. VLAN Scanning and IPv4 vs IPv6 discovery is done as well.</p>
9 	<p>DHCP RESPONSE – The DHCP response returns a PNF IP address, the initial EM IP address, Security Gateway IP address (optional), and certificate authority IP address (opt). It is possible the PNF IP address is a temporary IP address used for initial connectivity purposes, and that a permanent PNF IP address will be granted later.</p>
11 	<p>CERTIFICATE ENROLLMENT – The process where the PNF gets a service provider certificate from the Certificate authority. The certificate is then used to authenticate and verify the PNF.</p>
12 	<p>IDENTITY SERVICE – The identity service is there to identify the PNF. It also returns the ONAP (DCAE) IP address.</p>
13 	<p>ONAP COMPLIANT SOFTWARE – The PNF contacts the initial EM and downloads the ONAP Bootstrap software. This is a software package that is meant to perform the remaining steps of PNF registration and activation onto ONAP</p>
14 	<p>PNF RESET – The PNF is reset so that the downloaded ONAP Bootstrap software becomes activated and is then ready to continue to PNF registration</p>

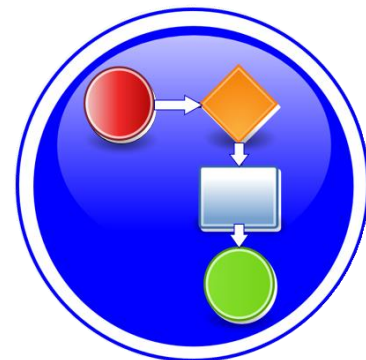
Service Instantiation Process (Part 1)



PNF PnP: SO Enhancements


DESCRIPTION

- (1) PNF WORKFLOW** – Coded in Beijing but needs yet to be integrated, tested, and accepted. Note: One PNF workflow (SO) that has two entry points: (1) instantiate & wait (Step 16) (2) Update (Step 34). One BPMN.
- (2) SO TO PNF Controller INTERACTION** – SO calls SDN-R (Generic API call vs REST call (?)). How should SO recognize which controller to use. List of operations.
- (3) PNF WORKFLOW ENHANCEMENTS** – Investigate the use of a Generic PNF workflow (will it work for 5G PNF). Investigate if enhancements (customizations) are needed to the PNF Workflow.
- (4) MODEL DRIVEN** – SO not yet model driven. Need to solve vis-à-vis a SO work flow specific to service & resource use case. *Controller type* to be used w/ PNF should be modeled in SDC.
- (5) DFX (Design for Excellence)** – Resilience, Performance, Scalability, Stability, Multi-tenants (multi-tenants access). Multi-site (single instances of SO).

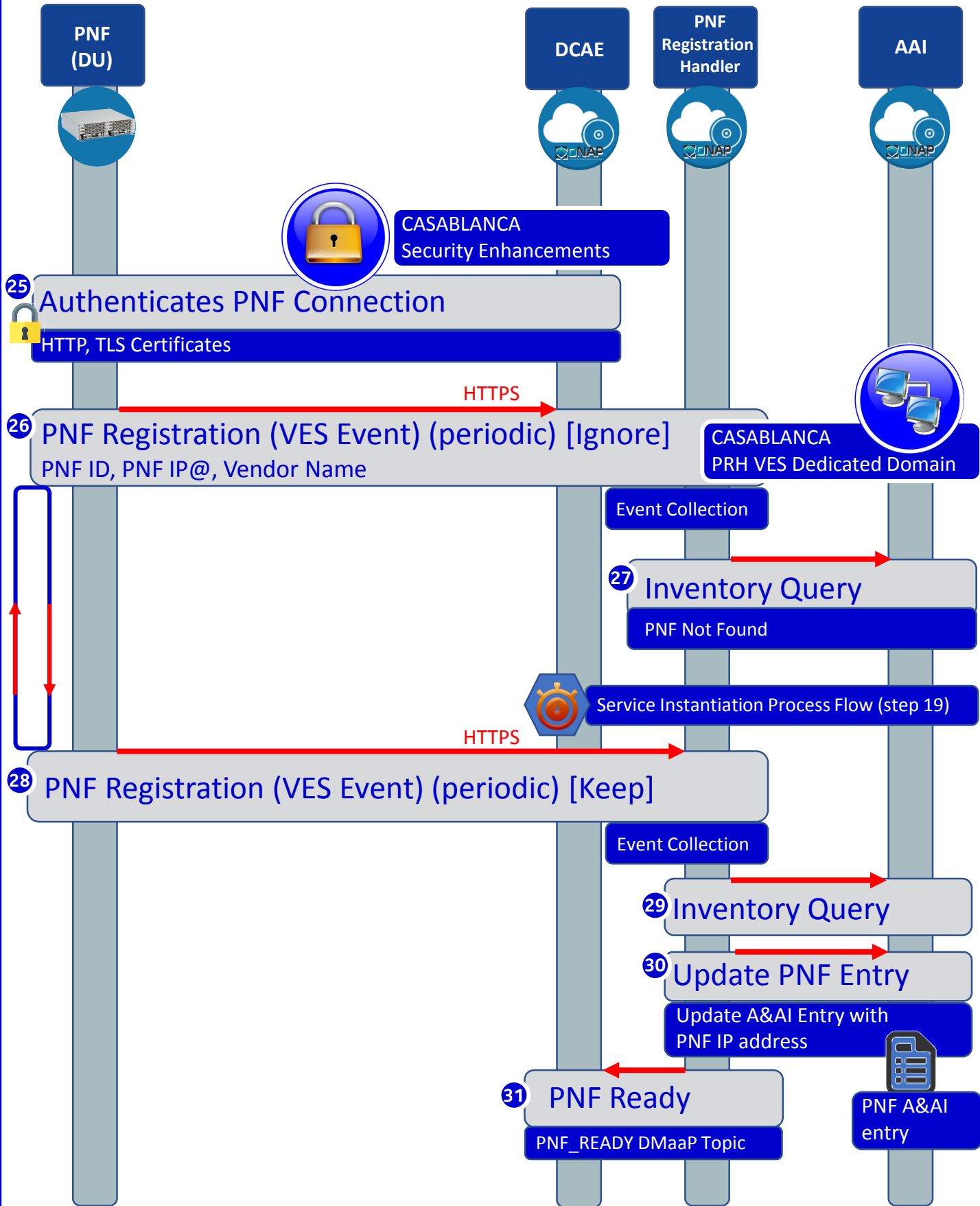


PROJECTS

SO, SDN-R, SDC, AAI

#	DESCRIPTION
15	WORK ORDER – The work order (AT&T work order process) determines which PNF to use for this Service/work order. BSS is told the correlation ID. Typically, the PNF will be known before the PNF comes on-line. Orchestrated with a equipment order (to vendor) and location value for the PNF.
16	SERVICE INSTANTIATION – The user on the VID creates a service instantiation providing a correlation ID. The service is decomposed for a 5G DU PNF. The DU resource types assumes that there is enough information to determine the PNF SDC model. The configuration parameter is provided manually (as part of service instantiation data).
17	HOMING – The SO instantiation is homed with the OOF. Dependencies stated on PNF. The homing latency constraints are based on CPE address (location). As part of the service definition a latency needs to be less than [x]. This is a service constraint. Homing dependencies should come from SDC or VID. PNF homes to a CU. [FUTURE] Homing identifies the place where a VNF is instantiated. For PNF there is no “cloud” resources needed (CU); ONAP instantiations/data-centers want to define which ONAP instantiation takes care of a PNF [FUTURE].
18	RESOURCE LEVEL FLOW (RLF) - The resource level flow thread starts. This thread is responsible for carrying out the creation of an A&AI entry in the following steps (steps 18 through 21).
19	CHECK A&AI ENTRY – The RLF thread in SO checks the A&AI entry for the PNF. If SO discovers that there is an A&AI entry with both the correlationID and the PNF IP@ then it can continue. If found it can associate it with the service instance.
20	CREATE A&AI ENTRY – A&AI entry created by SO for PNF using the available information and the correlation ID. This is done in anticipation of the PnP PNF VES event.
21	CREATE DMaaP TOPIC LISTENER – The RLF thread (process) subscribes to the DMaaP Topic that will complete the service instantiation. It allows ONAP to intercept the VES event that will eventually come from the PNF when it reaches a point in the PNF Plug and Play process that it is ready to contact ONAP. The RLF specific resource thread indicates that it cares about the VES event with this correlation ID. Essentially it activates a “listener” of the PNF VES event. DCAE is the normal VES event Listener which creates a DMaaP Topic. SO saves the state information looks and sees if it is one of the DMaaP topics it is waiting for.
22	RLF THREAD TERMINATES – The Resource Level Flow (RLF) thread in SO terminates. When the VES event is received at a later point in time, it can be processed accordingly. Additionally, these steps 15-22 prepare ONAP with the pre-requisite information so that when the VES event comes from the PNF it will not be discarded. This is denoted by stopwatch icon  . At a later step in the PNF Plug and Play this thread becomes relevant again at the other stopwatch icon. The RLF thread/process stops processing and wait for an asynchronous event (to avoid a long running event). Writes a process, kamunda handler for an event that rehydrates it. (this reuses the SO rainy day handling)

PNF Registration Steps



pnfRegistration VES Event

Field	Type	Required?	Description
version	number	Yes	Version of the event header (currently: 3.0) 3.0
eventName	string	Yes	pnfRegistration_vendor_pnfName where <i>pnfName</i> is specified by the vendor and is a PNF type; e.g. pnfRegistration_Nokia_5gDu
domain	string	Yes	Event domain enumeration: 'fault', 'heartbeat', 'measurementsForVfScaling', 'mobileFlow', 'other', 'sipSignaling', 'stateChange', 'syslog', 'thresholdCrossingAlert', 'voiceQuality', ' pnfRegistration '
eventId	string	Yes	Event key that is unique to the event source registration_yyyyyyyy where <i>yyyyyyyy</i> is an integer starting at 0 and incremented by 1 for every pnfRegistration event sent by this PNF
eventType	string	No	pnfRegistration
nfcNamingCode	string	No	Network function component type: 3 characters (aligned with vfc naming standards) Not used
nfNamingCode	string	No	Network function type: 4 characters (aligned with vnf naming standards) Not used
sourceId	string	No	UUID identifying the entity experiencing the event issue (note: the AT&T internal enrichment process shall ensure that this field is populated) Not used
sourceName	string	Yes	Name of the entity experiencing the event issue PNFid (unique PNF instance ID = PNF correlation ID = pnf-name stored in AAI ; e.g. NOK6061ZW3)
reportingEntityId	string	No	UUID identifying the entity reporting the event, for example an OAM VM (note: the AT&T internal enrichment process shall ensure that this field is populated) Not used
reportingEntityName	string	Yes	Name of the entity reporting the event, for example, an EMS name. May be the same as the sourceName. For synthetic events generated by DCAE, it is the name of the app generating the event. PNFid (unique PNF instance ID = PNF correlation ID = pnf-name stored in AAI ; e.g. NOK6061ZW3)
priority	string	Yes	Processing priority enumeration: 'High', 'Medium', 'Normal', 'Low' Normal
startEpochMicrosec	number	Yes	the earliest unix time aka epoch time associated with the event from any component--as microseconds elapsed since 1 Jan 1970 not including leap seconds current time
lastEpochMicrosec	number	Yes	the latest unix time aka epoch time associated with the event from any component--as microseconds elapsed since 1 Jan 1970 not including leap seconds current time
sequence	integer	Yes	Ordering of events communicated by an event source instance (or 0 if not needed) 0
internalHeaderFields	internalHeaderFields	No	Fields (not supplied by event sources) that the VES Event Listener service can use to enrich the event if needed for efficient internal processing. This is an empty object which is intended to be defined separately by each provider implementing the VES Event Listener. Empty Not used

pnfRegistration VES Event

Field	Type	Required?	Description
pnfRegistrationFieldsVersion	number	Yes	Version of the pnfRegistrationFields block (currently: 1.0)
serialNumber	string	Yes	TS 32.692 serialNumber = serial number of the unit; e.g. 6061ZW3
vendorName	string	Yes	TS 32.692 vendorName = name of manufacturer; e.g. Nokia. Maps to AAI equip-vendor.
oamV4IpAddress	string	No ¹	IPv4 m-plane IP address to be used by the manager to contact the PNF. Maps to AAI ipaddress-v4-oam.
oamV6IpAddress	string	No ¹	IPv6 m-plane IP address to be used by the manager to contact the PNF. Maps to AAI ipaddress-v6-oam.
macAddress	string	No	MAC address of unit.
unitFamily	string	No	TS 32.692 vendorUnitFamilyType = general type of HW unit; e.g. BBU.
unitType	string	No	TS 32.692 vendorUnitTypeNumber = vendor name for the unit; e.g. Airscale. Maps to AAI equip-type.
modelName	string	No	TS 32.692 versionNumber = version of the unit from vendor; e.g. AJ02. Maps to AAI equip-model.
softwareVersion	string	No	TS 32.692 swName = active SW running on the unit; e.g. 5gDUv18.05.201.
manufactureDate	string	No	TS 32.692 dateOfManufacture = manufacture date of the unit in ISO 8601 format; 2016-04-23.
lastServiceDate	string	No	TS 32.692 dateOfLastService = date of last service in ISO 8601 format; e.g. 2017-02-15.
additionalFields	hashMap	No	Additional registration fields if needed, provided as key-value pairs.

PRH Enhancements

PNF Registration Handler (PRH) Enhancements.



(1) New VES Event domain for PNF Registration – Create new VES event domain *pnfRegistration* for PNF registration with corresponding support in VES collector, DMaaP and PRH. PnP Use case was using the “*other*” domain to register VES events. For Casablanca, we propose using a dedicated domain. VES separation of events. VES agent update in PNF.

(2) VES EXTENSIONS - As a result, VES collector and VES agent content will change with field updates using the new domain. Extensions for PNF registration fields. Corresponding VES Schema change (VES message 6.0 standard)

(3) PNF REGISTRATION EXCHANGE UPDATE – The registration VES event used by the DU Simulator (or actual PNF) will need to update its JSON payload to match the changes above.

(4) TOPIC CREATION – Once DMaaP is secured, creation of new *pnfRegistration* DMaaP Topic. Topic needs to be pre-provisioned. *pnfReady* event.

(5) AAF & PRH – Intra-ONAP Security. PRH integration with AAF for security. Refactor VES.

(6) FAILURE HANDLING – Error handling for when registration fails. (1) send response didn't find AAI keep sending (2) avoid multiple PNF ready to SO for same PNF. (3) AAI unavailable ONAP components not running (4) PNF sending erroneous info. (5) Failures on (a) PNF registration (b) DMaaP PNF Ready (c) AAI (d) Platform (6) VES Schema validation (7) **PNF timeout & max# tries (actual DU).**

(7) SO INTEGRATION – SO WF Integration. Service Instance (Timeout = wait for 2 weeks). External inventory monitoring system.

(8) REQUIREMENTS PROJECT – Add requirements: for all equipment providers their PNFs have to use this event.

PROJECTS

PNF Registration Handler, DMaaP, DCAE

SECURITY ENHANCEMENTS

HTTP

- ONAP to eliminate username and password for HTTPS.

TLS

- DCAE authenticates Vendor or Service Provider X.509v3 certificate for TLS connection.
- ONAP User is able to install Vendor Root CA certificate as trust anchor in ONAP.
- ONAP supports 3 level chain (Root CA, Sub CA and End-Entity certificates).
- Vendor is able to install ONAP Root CA as trust anchor on NF for mutual TLS authentication.

CA

- Provide CA services to NFs in ONAP for development and testing; enrollment, authentication.
- Support CMPv2 for NF for certificate enrollment and end-entity key renewal in ONAP for development and testing.
- Support integration with Service Provider CA/PKI in ONAP.

SSH/SFTP

- Create RSA public/private key pair for ONAP Controllers and File Collector for SSH/SFTP access into the NF for CM/PM.
- Provision SSH username/public key on NF for Ansible or NetConf access from ONAP Controllers for CM and SFTP.
- Client shouldn't accept username / password for SSH authentication.

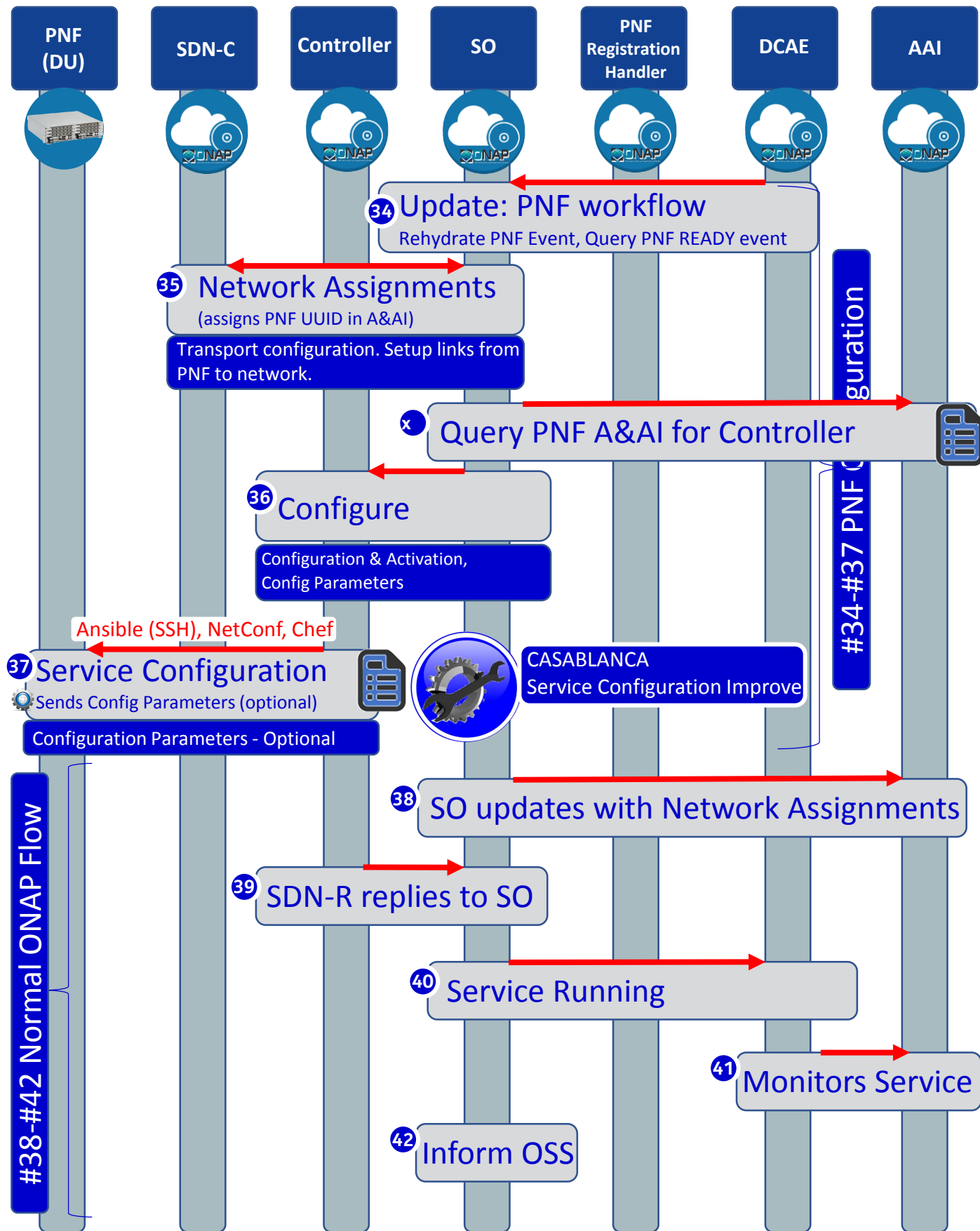


PROJECTS

PNF Registration Handler, DCAE, AAF,
ONAP Controller, DMaaP

STEP	DESCRIPTION
23	DHCP Request –ONAP Onboarding S/W performs a DHCP procedure with vDHCP
24	DHCP Response – DHCP response returns a ONAP IP address
25	Authenticate PNF – The PNF is authenticated through a vAAA.
26 & 28	<p>PNF REGISTRATION – The PNF periodically generates a VES Event (json schema extend for discovery event) to DCAE which is the “triggering” event that tells ONAP that the PNF is trying to register. This event contains the Correlation ID (PNF ID), which will serve as an identifying key within A&AI to seek for that particular PNF instance. The event also contains the PNF OAM IP address and the vendor name. PNF sends the Event over an HTTPS connection which may be authenticated with a username and password. The Event is “standardized” and is the same for all hardware (PNF) irrespective of equipment vendor, thus there needs to be ONAP compliant software. The PNF must natively support or have an adapter to be ONAP capable.</p> <p>Note [FUTURE]: A (new) “<i>PNF Infrastructure Manager</i>” may evolve in the future to include other management functions, as there may be a need for an entity that owns the interactions with device interactions w.r.t. ONAP. Management of devices vs containers. I/F manages & consumes services. VIM/Multi-Cloud. Multi-VIM PNF plugin. Multi-VIM would call the PNF infrastructure manager.</p>
27 & 29	INVENTORY QUERY – PNF Registration Handler performs an inventory Query to A&AI using the Correlation ID (based on the PNF ID) as the key. The AAI instance for this PNF ID must have already been created. If it has, then this is a valid, expected PNF. If not, then this is not a valid or not found a response is given to the PNF. In Step 32, PNF A&AI entry is found.
30	<p>UPDATE PNF ENTRY IN AAI – The PNF entry in AAI is updated with the PNF IP address. After this step, the PNF is considered to be active in ONAP and becomes available as an network element to fulfill service requests.</p> <p style="text-align: right; font-size: small;">Patch AAI MO command If {!entry} {error & exit} If {entry} {overwrite & send PNF Ready}</p>
31	PNF READY - PRH publishes a PNF Ready event on the DMaaP bus to which SO subscribes. SO receives the PNF Ready event, determines that it is an event it is waiting for and rehydrates the appropriate RLF to restart the Service Instantiation
(15-22)	SERVICE INSTANTIATION PROCESS (PART 1) – Steps 15-22, the Service Instantiation Process (part 1) occurs in parallel to these steps. When that process reaches the pending point (denoted by ) it rejoins the flow here. PNF previously declared.
32	PNF REGISTRATION RESPONSE - There is discussion whether in the failure cases of PNF registration if a response back from ONAP should be sent. Under consideration for Casablanca release (R3)

PNF Activation Steps (ONAP)



SERVICE CONFIGURATION ENHANCEMENT


DESCRIPTION

- (1) Service configuration Enhancements** to ONAP Controller to PNF *service configuration* exchange with PNF.
- (2) PROTOCOL DEFINITION** – Framework for how SDN-R will support NetConf, Ansible, Chef. All 3 are expected to be supported with PNFs. How is the protocol agreement done?
- (3) Configuration Extensions** – New parameters needed for Casablanca use cases. Vid script to pushing data, ID config, ID where data comes from. Generic configuration support.
- (4) PNF PnP Config** – Finishing PNF PnP by sending down config data.
- (5) (OPTIONAL) Vendor Data** – Extensions to Service Configuration with Vendor specific configuration data can be developed (vendor dependent).






PROJECTS

ONAP Controller (SDN-R), VID, SO,
SDC/CDT

STEP	DESCRIPTION
34	SO NOTIFIED - PNF Infrastructure Manager Notifies SO. SO listens to the DMaaP hook. A trigger. Wait for PNF onboarded. Calls SDN-C.
35	NETWORK ASSIGNMENTS – SDN-C assigns an IP Address for PNF. The IP @ assigned to the PNF is drawn either from the DHCP server, IP address Pool, or a Static IP@. Managing physical/virtual links to PNF. Between CU & DU. Transport connectivity setup. SDNC makes assignments, the resource model have external/internal connection points (named). For each point, attributes say L1/L2 connection. If L3 who assigns the IP address. Each point, SDNC knows if and what to assign. Set either through SDNC (L0-L3) or APP-C (L4-L7). Driven by TOSCA Model.
36	ACTIVATE – Configuration & Activation of the PNF Depends on the resource type. The controller requires input data based on PNF type. Either VF-C or APP-C orchestrate with SO. The IP@ is retrieved SDNC instance manager for PNF and the DHCP server may be updated. Pass on configuration parameter(s). (Future) retrieve VNF a configuration parameter.
37	 SERVICE CONFIGURATION – APP-C calls Ansible to configure PNF’s (Configuration Parameter) NetConf messages from SDN-C to PNF. (1) Configuration Parameter (optional) – SDN-R/APP-C gives the Controller IP@ to the DU. In R3, SDN-R/APP-C may pass configuration parameter(s) to the 5G DU, this will also give a configuration parameter (e.g. CU IP@). (2) OAM IP@ (optional) - The permanent OAM IP address is given to the PNF. The IP address may come from vAAA, or drawn local pool of IP addresses. SDN-C performs the IP address selection. SDN-C knows if a permanent IP address should be assigned. (3) Transport configuration (optional) – Transport configuration is given to the PNF. (4) Location (optional) – the Location configuration may be given to the PNF. (5) Software Version (optional) – In Casablanca it could be specified a Software Version. http://onap.readthedocs.io/en/latest/submodules/appc.git/docs/APPC%20LCM%20API%20Guide/APPC%20LCM%20API%20Guide.html
38	SDN-C Updates A&AI – SO updates A&AI with Network Assignments (from step 35)
39	SDN-C replies to SO – SDN-C replies to SO are the service configuration step.
40	Service Running – SO publishes a “Service running” event to which DCAE subscribes.
41	Monitors Service - DCAE reads A&AI entry and sets up monitoring for the new service. DCAE publishes “Service monitored” event to which SO subscribes. For monitoring events, the DU will be managed by the CU (in the FUTURE an M-Plane will be setup to ONAP to DU
42	OSS Inform - SO responds to User/BSS/OSS that the service is active.

PNF Final Download & Activation (Vendor Specific)



STEP	DESCRIPTION
43 	CONFIGURATION (Optional) – The configuration information is downloaded from [ONAP, EMS, or another PNF] to the DU. This information provides operational configurations and settings which are vital for service. They would be pre-provisioned and allow the PNF to operate with specified configurations, optimizations, RF settings, connectivity, and L1/L2 algorithmic settings.
44 	SOFTWARE DOWNLOAD (Optional) – Software download from [ONAP, EMS, or another PNF] to the DU. This software download is optional and is specific to a vendor.
45 	DU RESTART – The 5G PNF (DU) is ready to provide service using the configuration provided to it. Typically, a test call is performed to verify service is working end-to-end.

VNF vs PNF Comparison





TOPIC	VNF	PNF
Concept	Application fulfills the role of a network function.	It is a network element, a physical entity, which can implement the role of a network function.
Physical Characteristic	Application without dedicated hardware; Virtualized applications require specific capabilities; Run on different vendor servers. SRIOV, Inter-DPDK. Hardware capabilities.	Has an actual physical asset that is deployed and associated directly with the PNF.
On-boarding	To onboard a VNF is to “bring it into ONAP” i.e. the VNF images, component VNF-C provide descriptors of these NFs. Deployment model, # components, functions. Configuration parameters. VNF is not tied or optimized for a specific hardware, only requiring perhaps some capability to be supported.	For PNF provide the descriptors. Only provide the meta-data. PNF S/W specifically optimized to run on dedicated hardware. (Now) Not the software image. (Future) ONAP will provide the software image repository.
Plug and Play	The model triggers the orchestration.	(See this slide package for PNF Plug and Play) at the end of PnP the PNF can provide service.
Characteristics	5G CU could be a VNF since there is no need to have an association to a physical environment.	5G DU must be PNF. PNFs are Elements which may need to interact with the physical environment. PNF is “High-Touch” technology. E.g. Emit radio waves in a geographical area.
Configurability & Deployment	Easily adaptable to functions that you expect. E.g. Packet gateway to reconfigure as different NFs. Services easily create instances reconfigures including deployments (for different applications). Use a different instances of the VNF to provide a new service. For a VNF you can easily “delete” and “create” a new VNF to perform a new function. Configured dynamically.	PNF has a “fixed” set of capabilities but can’t easily reconfigure it. One PNF in multiple services. Different capabilities exposed by the PNF. Reuse the same PNF with different services configuration. For a PNF you would not “destroy” a PNF but rather re-configure it. Can be configured dynamically.
ONAP Interaction	ONAP is started with VNF. VNF is “deployed” on-demand. Control from the ONAP perspective when a deployment of a VNF happens. DCAE – same Configure – Chef, Ansible	PNF do not “deploy” application. Do not use multi-VIM. Only “configure” the application, the PNF is deployed. A technician goes to site and “deploys” a PNF. DCAE – same Configure –Implementation of PNF client. Communication protocol, Client
Design Time Modeling	Model VNF. Templates. Onboarded before. In Run-time. Make sure properly identify specific PNF instance already deployed. Vs a dynamically created instances. VNF instances could be created & instantiated dynamically. SDC may assumed instantiation of network function.	PNF cannot be instantiated, a PNF is only instantiated when it “powers up” and connects to ONAP. Service Orchestration. PNF is instantiated by nature of a PNF installation & commission procedure.
Service Orchestration	VNF cloud, #VM resources consumption, define components implement different functions. Where & What will be deployed.	Physical location, pre-provisioned capabilities, performance monitoring. Components installed. RUs for specific functions.
Resources	VNF dynamically assigned resources.	PNF statically associated (hardware) resources.
Capacity	VNF Capacity can be dynamically changed	PNF is static (number of cells supported)



PNF Plug and Play Project Impacts

- ONAP and PNF Plug and Play for 5G RAN
- 5G Use Case Team

VID IMPACT

ONAP Project	IMPACT
Management Design	(After modeling, and instantiation) “in the middle” Policy Design changes? (check w/ Policy Project) CDT (APPC) - Networking Design – SDN-C design tool for networking design. Creates Yang files. Config Design
VID & PNFID SUPPORT 	<p>With Seshu (SO) decided will continue vCPE work-flow extensions. Show in integration team, interim test. VID Impact, the API of that SO work-flow is extended, which must consume the CORRELATION ID (PNF ID). The PnP registration workflow can be included into a broader use case work-flow. i.e. can “Cut & paste” to the vCPE/VOLTE work-flow. Any workflow that deploys a service. VID uses different APIs of different ONAP components. VID deploy VCPE. VID creates a new cell, format; calls extended API. Client call. GUI to SO/AAI. VID GUI uses REST APIs of other modules. Display parameters of other ONAP modules.</p> <p>#1 – <u>PNFID SUPPORT</u> – VID to support PNFID (Correlation ID) for SO instantiate VCE/VoLTE Work-flow from Beijing (R1). SO work-flow API.</p>
VID & INSTANTIATION 	<p>#2 – <u>SERVICE INSTANTIATION</u> – For R3, a 5G RAN deployment work-flow, want pnfRegistration use case supported by 5G RAN work-flow, with new SO work-flow API. Kamunda BPMN engine & external API. SO API internal calls mapped to Kamunda. Sub-work flow to deal w/ pnfRegistration. VID would have to support instantiation of that work-flow. May be a new screen in VID.</p>
VID & MULTI-PNF 	<p>#3 – <u>MULTI-PNFID</u> - today we are asking VID to provide an additional PNFID to the work-flow. Integration want to use VOLTE have 2 instances of PNF (need 2 PNF ID). Infrastructure w/ 2 routers PNF create 1 service. 1 PNF:1 Service > n PNFs:1 Service. Slices share 1 PNF. 1 PNF:n Services. PNFID = Correlation ID. Study item (backlog).</p>
VID & WORK ORDER 	<p>#4 – <u>WORK ORDER</u> (Optional) – Supporting Work Order. Supported with service specific applications. Inventory systems. Future extension to ONAP.</p>
VID & AIA CREATION	<p>#5 – <u>VID A&AI INSTANCE CREATION</u> – (optional) (slide 19/Step 4) – VID supporting a PNF A&AI Instance creation.</p>

PNF REGISTRATION HANDLER IMPACTS

PNF Registration Handler (PRH) Project Impacts

NEW pnfRegistration DOMAIN



(1) New VES Event domain for PNF Registration – Create new VES event domain *pnfRegistration* for PNF registration with corresponding support in VES collector, DMaaP and PRH. PnP Use case was using the “*other*” domain to register VES events. For Casablanca, we propose using a dedicated domain. VES separation of events. VES agent update in PNF.

(2) VES EXTENSIONS - As a result, VES collector and VES agent content will change with field updates using the new domain. Extensions for PNF registration fields. Corresponding VES Schema change (VES message 6.0 standard)

(3) PNF REGISTRATION EXCHANGE UPDATE – The registration VES event used by the DU Simulator (or actual PNF) will need to update its JSON payload to match the changes above.

(4) TOPIC CREATION – Once DMaaP is secured, creation of new pnfRegistration DMaaP Topic. Topic needs to be pre-provisioned. *pnfReady* event.

AAF



(5) AAF & PRH INTEGRATION – Intra-ONAP Security. PRH integration with AAF for security.

(6) VES INTEGRATION – To authenticate VES collector and authentication of PNFs connecting to VES Collector. To facilitate this development, the VES S/W is being refactored.

FAILURE HANDLING



(7) FAILURE HANDLING – Error handling for when registration fails. (1) send response didn't find AAI keep sending (2) avoid multiple PNF ready to SO for same PNF. (3) AAI unavailable ONAP components not running (4) PNF sending erroneous info. (5) Failures on (a) PNF registration (b) DMaaP PNF Ready (c) AAI (d) Platform (6) VES Schema validation (7) **PNF timeout & max# tries (actual DU)**.

SO INTEGRATION



(8) SO INTEGRATION – SO WF Integration. Service Instance (Timeout = wait for 2 weeks). External inventory monitoring system. RH to support AAF authentication between RH and SO

REQUIREMENTS PROJECT



(9) REQUIREMENTS PROJECT – Add requirements: for all equipment providers their PNFs have to use this event.

- (a) PNF side: Requirement for PNF Time/Max# Tries
- (b) ONAP side: Timeout (e.g. 2 weeks)

DMaaP meeting – sunil unnava (MR), Dominic lunanova dgl@research.att.com (Bus controller)

Requirements Meeting – steven wright su622b@att.com

VID meeting - Ofir Sansino

SERVICE ORCHESTRATOR (SO) IMPACTS

SERVICE ORCHESTRATOR (SO) PROJECT IMPACTS

WORK FLOW Integration/ Testing (SO executor)

Create work-flow for PNF (Srini)
For configuration for SO
Coded in Beijing but needs yet to be integrated, tested, and accepted.
Note: One PNF workflow (SO) that has two entry points: (1) instantiate & wait (Step 16) (2) Update (Step 34). One BPMN.

AAF & PRH Integration



SECURITY - SO enhancement to support using AAF authentication between **PRH** and **SO** (will SO integration to AAF in general).
ACTION: need more details on PRH to SO security – TLS, Certificates, Client/Server interaction, DMaaP. [Security Development]

SO TO Controller INTERACTION



1. **IDENTIFY THE CONTROLLER:** How should SO recognize which controller to use. STEP37 SO calls (Controller: APP-C, SDN-C, SDN-Cr/APP-Cr (SDN-R), VF-C Identified in PNF A&AI Entry) (Generic API call **vs** REST call (?)). List of operations.
PNFID > PNFD > Controller
2. **HOW TO CALL THE CONTROLLER** - API to the identified Controller. SDN-C (Generic API). North-bound would be SDN-C API.
ACTION: How does SO Call the Controller

PNF WORKFLOW ENHANCEMENTS

Investigate the use of a Generic PNF workflow (will it work for 5G PNF). Investigate if enhancements (customizations) are needed to the PNF Workflow. Sub-Flow. BPMN (separate WF). PNF Auto-discovery WF. Stand-alone WF that can be “plugged” into other WFs.

MODEL DRIVEN

SO not yet model driven. Need to solve vis-à-vis a SO work flow specific to service & resource use case. *Controller type* to be used w/ PNF should be modeled in SDC.

DFX (Design for Excellence)

Resilience, Performance, Scalability, Stability, Multi-tenants (multi-tenants access). Multi-site (single instances of SO).

Controller Type ID



ACTION: Identifying the PNF Controller (set in Design time). What is the API

Slide 19/Alt-2 Step 20



ACTION: “Manual” (Slide 19) vs Automated (Slide 26) (w/ Vimal, Gil)

PROJECT IMPACTS FROM ONBOARDING

ONAP Project	IMPACT
SDC/ Modeling	Modeling Project - (No License management impact – See Futures Section) [See follow-on Slides “MODELING”]
VNF-SDK (PNF-SDK) Validation	<p><u>PNF PACKAGE DEFINITION</u></p> <p>PNF packages similar to VNF packages. PNF Descriptors, artifacts. In PNF not doing deployment process in SDC. Only PNF configuration. Model a PNF. Onboard PNFs (create templates service configuration). Orchestrate a service on a PNF. Service provisioning. Life cycle: Template/service orchestrated. For PNF every PNF vendor makes this package. Need specific PNF properties. Image details. ONAP updates the image.</p> <p><u>VALIDATION OF A SDK PACKAGE</u></p> <p>VNF-SDK (validation, Package definition, verification tool) – package compliant. Allows creation/validation of packages. PNF-SDK <i>validates</i> the package.</p>
WORK FLOW (SDC)	Create work-flow for PNF (Srini) SDC Impacts related to work-flow. ACTION: Sample Work-flow for PNF.
MONITORING (SDC)	Monitoring definitions – SDC has a side monitoring template designer. Way to define monitoring alarms etc; In AT&T there is a project; IN ONAP code is there finalizing code; pluggable modeler for monitoring. DCAE as part of onboarding specify what VES template. DCAE-DS [Design Studio] define microservices for monitoring. How is PNF monitored & correlated. If [x] goes down how is this correlated. SDC would define the Modeling what needs to be monitored and how they would correlated with other events from other NE. Thresholds. [Baby step to process get an alarm from PNF, YAML file describes fault VES event, Fault meta-data; alarms generate]. Alarms raises are documented in SDC. Upload an “Artifact” file (Alarm Dictionary / Fault Meta-data / YAML, YANG). Vendor Specific. Demo and separate discussion. How monitored – processing in DCAE-DS (Design Studio time). Based on design time data DCAE is done in.

DCAE-DS IMPACTS

OVERVIEW - DCAE-DS generates the **templates** for monitoring the models. DCAE-DS is model-driven. It specifies which monitoring microservice are utilized in monitoring a specific service model. Cloudify blueprints specify the requirements on micro-service and are configured by a user. Configurations are distributed to components who subscribe to that specific type of artifact.

DCAE-DS TEMPLATES – monitoring templates composition of micro-service to be used (open/closed loop). The templates are *Cloudify Blueprints*. E.g. Micro-Service collectors, analytics, monitoring. VES collectors, holmes. A micro-service that is part of a monitoring flow that a designer can design that can be reused for difference service models. A building block represented by TOSCA models. First needs to be represented by development team. Monitoring template certified.


DCAE-DS GUI - DCAE-DS is a pluggable designer in SDC provides a GUI to the user that selects/composes the micro-services, or use predefined templates, for specific flows. E.g. SNMP type of flow or different protocol. User can configure different micro-services according to requirements to the model.

PNF PLUG AND PLAY – Cloudify Blueprints (for a [1:X] service) has (UUID, Micro-service values, Properties, service specific policies). What are we trying to Monitor? SDC Service-Package attached to VF-Level.

MODELING IMPACTS

Notes:

- 1) **EXTERNALS** - Not trying to model the internals of PNFs. What is exposed by the box is what is modeled.
- 2) **INTERRELATIONS** - Focus on relations of PNFs/VNFs. Interworking between PNFs/VNFs.
- 3) **VISIBILITY** - CP/UP visibility
Not M-Plane (as this is 3GPP standardized)
- 4) **MODELING ANALYSIS** - Modeling activity to assess PNF, and check SDC model is sufficient to cover Casa use cases if additional parameters need to be added (e.g. relations between other NFs). Expanding the “Release 0 model” for Casa. PNF type vs PNF instance. Design-time vs Run-time model.

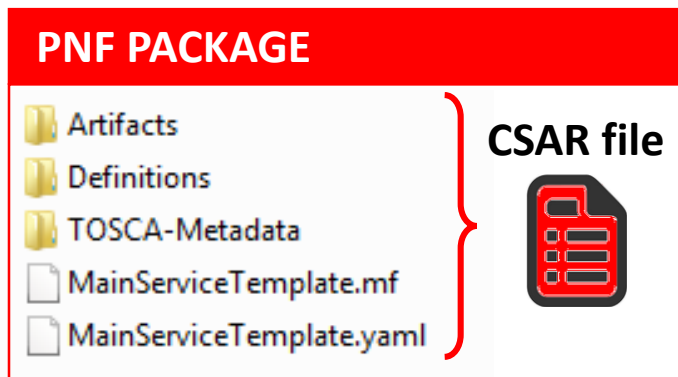
 Suggested VES Event Entry - Fault' Domain Datatypes
For Alarm Dictionary Index (in **Dublin**)

Alarm Index	Dictionary	number	No	Alarm Dictionary Index, (since optional if left blank would mean dictionary is not used)
----------------	------------	--------	----	--

PNF PACKAGE

PNF has no onboarding package.

Just model the PNF from the modeling screens.



CSAR – decompile info stored in SDC model.

In VNF flow. Onboard the VNF. VNF cataloged as a version to be used. Check-in/check-out. After onboarding can add more artifacts and certify the VNF. A “building block” to be used in different services. Generic, the structure will be the same. E.g. 2000 ports vs 10 ports. “Ports”. How to comm w/ PNF what to do w/ PNF. Specific work-flow or configuration. PNF & VNF similar. SO will orchestrate, already exists in ecosystem.

Modeling of the Service. E.g. Connection point what will connect to the PNF.

ARTIFACTS

DEFINITIONS

PNF – 5G Base Stations

Backhaul Ports – PNF & VNF and want to communicate. In a VNF can describe a port a TOSCA.

Model onboarded understand what can connect to what. CP connections. Can see they can connect. Model needs to capture info for modeling parts representing connections. Model allow someone designing service to connections. Or requirements from VNF/PNF from the model. A virtual link. One VNF & PNF connected via virtual network/link.

PNF Work-flows – initialization, triggered when connecting to PNF. Configuration/registration that needs to be done. DNS pre-loaded. Location. Policies attached to PNF, High volume # of PNF deployments, port-allocation. *Capabilities. Triggered by orchestrator as part of the instantiation.*

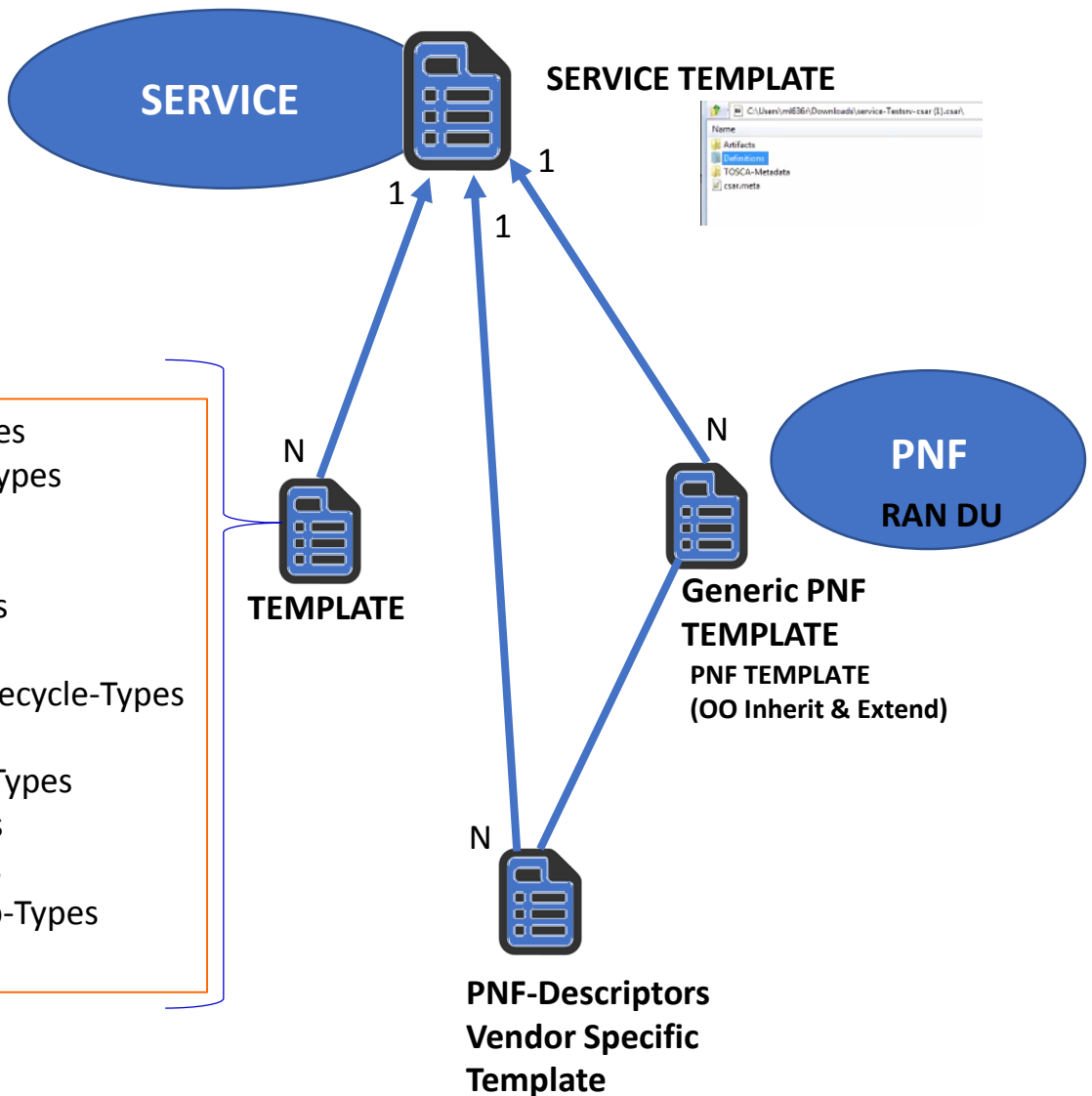
PNF Policies -

Tilt – (Antenna Tilt - RF) – not related to PNF / VNF communicate.

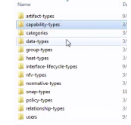
Software Version

Modeling Project, VNF-SDK (validation, Package definition, verification tool) – package compliant

SDC MODELING (Design Time)



- Artifact-Types
- Capability-Types
- Categories
- Data-Types
- Group-Types
- Heat-Types
- Interface-Lifecycle-Types
- NFV-Types
- Normative-Types
- ONAP-Types
- Policy-Types
- Relationship-Types
- Users



```

sdccatalog-be> src> main> resources> import> tosca> heat-types> Generic_PNF
Open New folder
Name Date modified Type Size
Generic_PNF 9/10/2017 12:49 JSON File
Generic_PNF 9/10/2017 12:49 YAML File
Generic_PNF 9/10/2017 12:49 Compressed (zip...)
tosca-definitions-version: tosca-simple-yaml-1.0.0
nodes:
  - org.openecomp.resource.abstract.nodes.PNF:
    derived from: tosca.nodes.Root
    properties:
      nf_function:
        type: string
      nf_role:
        type: string
      nf_type:
        type: string
  
```

Controller Type
["common fields"] ...
Vendor-field1

PNFD Definition in ETSI-NFV-IFA014v242

Attribute	Qualifier	Cardinality	Content	Description
pnfdId	M	1	Identifier	Identifier of this Pnfd information element. It uniquely identifies the PNFD.
functionDescription	M	1	String	Describes the PNF function
provider	M	1	String	Identifies the provider of the PNFD.
version	M	1	Version	Identifies the version of the PNFD.
pnfdInvariantId	M	1	Identifier	Identifies a PNFD in a version independent manner. This attribute is invariant across versions of PNFD.
name	M	1	String	Provides the human readable name of the PNFD.
pnfExtCp	M	1..N	PnfExtCpd	Specifies the characteristics of one or more connection points where to connect the PNF to a VL. See clause 6.6.4.
security	M	0..1	SecurityParameters	Provides a signature to prevent tampering.
geographicalLocationInfo	M	0..1	Not specified	It provides information about the geographical location (e.g. geographic coordinates or address of the building, etc.) of the PNF. The cardinality 0 is used when the location is unknown.

Basic Content of PNF template **PNF-D (DESCRIPTOR)**

Contents	Description
pnfdId	Identifier of this Pnfd information element. It uniquely identifies the PNFD.
provider	Identifies the provider of the PNFD.
PNFD version	Identifies the version of the PNFD.
pnfdInvariantId	Identifies a PNFD in a version independent manner. This attribute is invariant across versions of PNFD. (pnfdInvariantId would be inside the meta-data in ONAP)
name	Provides the human readable name of the PNFD.
security	Provides a signature to prevent tampering.
pnfInformation	Describes the PNF information
pnfSoftwareVersion	Software Version supported PNFD.

VERSION MODELING

Diagram of Software Version Management for a PNF



PNF-Descriptor (version)

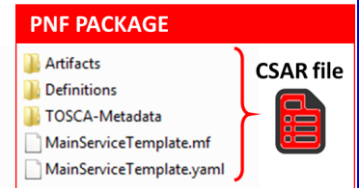
Vendor Provided

PNFD version = 6



PNF-Package (version)

Minimal PNFPackage version = 7.1
(SDC Versions the Package)



PNF Software (version)

[Detected Software, Expected Software]

DETECTED PNF S/W [Part 1] 2.1 [Part 2] 2.2 (A&AI)

ONAP EXPECTED PNF S/W 3.0 (modeling)





PNF Hardware (version)

Hardware Version

Firmware Version

Product Model version

PNF MODELING Information (IN SDC)

Contents	Description
pnfid*	Identifier of this Pnf information element. CORRELATIONID (A&AI)
pnfType (template)*	Type of Resource. NEW type: PNF (pre-defined in SDC)
Category*	PNF category, e.g. infrastructure
Vendor (template)*	Identifies the vendor of the PNF.
Name*	Provides the human readable name of the PNF.
vendorrelease *	Vendor release
vendormodelNumber*	PNF Model value (link to A&AI)
functionDescription*	Describes the PNF function
pnfExtConnPt (modelling def. of connection pt not a template) 	Specifies the characteristics of one or more connection points where to connect the PNF to a VL. Align ETSI SOL-001
contactId (metadata)	Designer (user of ONAP)
pnfSWversionList	The EXPECTED software to be supported by the PNF.
PackageVersion	The version of the PNF Package.
NF Controller 	Controller for PNF (APP-C, SDN-R, SDN-C, VF-C)

```

nodeTemplate {
  type: org.onap.sdc.resource.cp.extCP
  metadata {
    ...
  }
  name: ExtCP
  type: CP
  category: General
  subcategory: Network Element
  resourceVendorName: 3TC (Tosca)
  resourceVendorRelease: 1.0.0.0
  properties {
    ...
  }
  ...
}

```

• Content of PNF software version List

Contents		Description
softwareList	description	Describes the main feature of the this software version
	swVersion	Software version

***Already supported in Beijing**

C:\Users\m636r\Downloads\service-Testsv-csar (1).csar\

Name

- Artifacts
- Definitions
- TOSCA-Metadata
- csar.meta

File Edit View Favorites Tools Help

Add Extract Test Copy Move Delete Info

C:\Users\m636r\Downloads\service-Testsv-csar (1).csar\Definitions\

SERVICE LEVEL PACKAGE

Name	Size	Packed Size	Modified	Created
artifacts.yml	3 098	1 169	2018-03-19 09:55	
capabilities.yml	8 306	1 748	2018-03-19 09:55	
data.yml	45 549	6 222	2018-03-19 09:55	
groups.yml	3 527	1 257	2018-03-19 09:55	
interfaces.yml	1 019	486	2018-03-19 09:55	
nodes.yml	130 477	11 667	2018-03-19 09:55	
policies.yml	3 631	861	2018-03-19 09:55	
relationships.yml	5 360	1 560	2018-03-19 09:55	
resource-Estneutroncp-template.yml	3 064	1 060	2018-03-19 09:55	
resource-Neutronnet-template.yml	2 223	846	2018-03-19 09:55	
resource-Neutronport-template.yml	3 145	1 074	2018-03-19 09:55	
resource-Vfw-template-interface.yml	246 202	7 771	2018-03-19 09:55	
resource-Vfw-template.yml	70 134	2 255	2018-03-19 09:55	
resource-VfwComputeNodesHeatVfw-template.yml	786	394	2018-03-19 09:55	
resource-VfwComputeNodesHeatVpg-template.yml	786	394	2018-03-19 09:55	
resource-VfwComputeNodesHeatVsn-template.yml	786	394	2018-03-19 09:55	
resource-VfwNodesVfwvcfc-template-interface.yml	31 443	3 862	2018-03-19 09:55	
resource-VfwNodesVpgvcfc-template-interface.yml	31 443	3 862	2018-03-19 09:55	
resource-VfwNodesVsnvcfc-template-interface.yml	31 443	3 862	2018-03-19 09:55	
resource-VfwNodesVsnvcfc-template.yml	24 733	1 763	2018-03-19 09:55	
resource-Testsv-template-interface.yml	25 508	3 553	2018-03-19 09:55	
resource-Testsv-template.yml	243 220	7 143	2018-03-19 09:55	
service-Testsv-template.yml	63 014	5 295	2018-03-19 09:55	

0 object(s) selected

Template, TOSCA level template representing some item
 On-boarded VNF want instance of that virtual firewall
 Place inside all the orchestrator needs

```

topology_template: 03
  node_templates: 04
    vfw 0: 05
      type: org.opencomp.resource.vf.vfw 06
      metadata: 07
        invariantUUID: fa9f72b3-d656-4e08-ae5e-9482ab165d5c 08
        UUID: 0a9e817b-4c98-455a-95d4-71e24713f73d 09
        customizationUUID: -E7432b08-ed4a-43fa-b179-40d2c5ff1b1e 10
        version: '0.2' 11
        name: vfw 12
        description: saad 13
        type: VF 14
        category: Network L4+ 15
        subcategory: Common Network Resources 16
        resourceVendor: example 17
        resourceVendorRelease: '1.0' 18
        resourceVendorModelNumber: '' 19
      properties: 20
        nf_naming: 21
          scomp_generated_naming: true 22
          multi_stage_design: false 23
          availability_zone_max_count: 1 24
          vfw_flavor_name: 4 GB General Purpose v1 25
          public_net_id: 00000000-0000-0000-0000-000000000000 26
          vfw_image_name: Ubuntu 14.04 LTS (Trusty Tahr) (PVHVM) 27
      capabilities: 28
        network.incoming.bytes.rate.vpg.vpg_private_1.port: 29
          properties: 30
            unit: B/s 31
            description: Average rate of incoming bytes 32
            type: Gauge 33
            category: network 34
          disk.read.bytes.vpg: 35
  
```

ACTIVE INVENTORY (A&AI) IMPACTS

ACTIVE & AVAILABLE INVENTORY (A&AI) PROJECT IMPACTS

New A&AI PNF Parameters

~~PNF GEOLOCATION~~ - geographical location (e.g. coordinates or address of the building, etc.). Latitude/Longitude. **THIS ALREADY EXISTS VIA ASSOCIATION TO THE "COMPLEX" OBJECT.** The Complex Object represents a BUILDING or location with geographical information. The AAI PNF will have a UML association to the Complex object.

Software Version

DETECTED SOFTWARE PNF VERSION(S) – in Run-Time when PNF registers with ONAP it can report its (list) of PNF Software that is currently installed. This will be tracked in A&AI entry for that PNF. Entry will also have *Active/Passive*. A&AI already has PNF active S/W version.

Content of PNF software version List

Contents	Description
description	Describes the main feature of the this software version
swVersion	Software version

Christina: This will require schema changes in A&AI to support Passive S/W

Homing



PNF [#1:CU/#2:ONAP] CLOUD HOME (CLOUD SERVER LOCATION) – PNF is served by some regional ONAP cloud servers. Serves in “Rehome” PNF. **CLLI Code** (specifies location, street address, **CloudID**, physical server is deployed). [Potentially a list of locations]
 OOF determine the homing of a NF. Anything you home is determined in the context of a deployment. (Homing) Policy used as a f(service). Data center might have been divided into cloud regions. Service VMME running in NE area (distances, regions, tenants where to instantiate PNF). AAI has COMPLEX node. “Physical Location ID” (8 char CLLI code, lat/long = geolocation info of data center. Cloud region doesn’t span data centers.

Manager IP Address



Manager IP Address – provides an additional IP address for the BTS that is vendor-specific and relevant to the OAM management of the BTS.
SUGGESTION (from Christina A&AI PTL) model the NMS as a PNF itself (and the NMS will have parameters to represent itself; and then PNF can be associated with it).

ACTIVE INVENTORY (A&AI) IMPACTS

PNF A&AI ENTRY (From Beijing)

- PNF has a “*pnf-name*” = Key in AAI.

Pnf-name is first 3 letters of vendorName concatenated with serialNumber for a unique PNF instance ID = PNFid = PNF Correlation ID = pnf-name.

Example: PNFid = NOK6061ZW3. The PNFid is in A&AI pnf-name field.

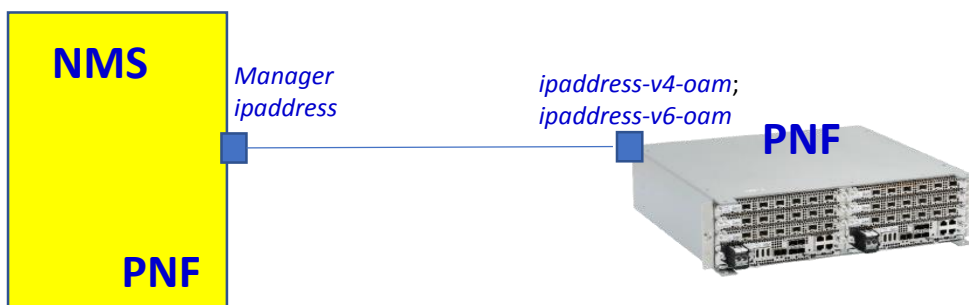
equip-type (PNF Type). *equip-vendor* (optional); *equip-model* (optional);
pnf-id (PNF ID)

(Step 33) adds *ipaddress-v4-oam*; *ipaddress-v6-oam* This is the “manager IP Address” which for a DU might be a CU IP address. IP address on the PNF address itself.

(FYI/ *ipaddress-v4-loopback-0*).

mac-address & *serial-number*,

PNF:: proxy IP address



OAM
FCAPS
Logging
SWM
Identity

1. ONAP -> NMS command
2. Relay (NMS trusted source)
3. Network Analytics – (DCAE AA)

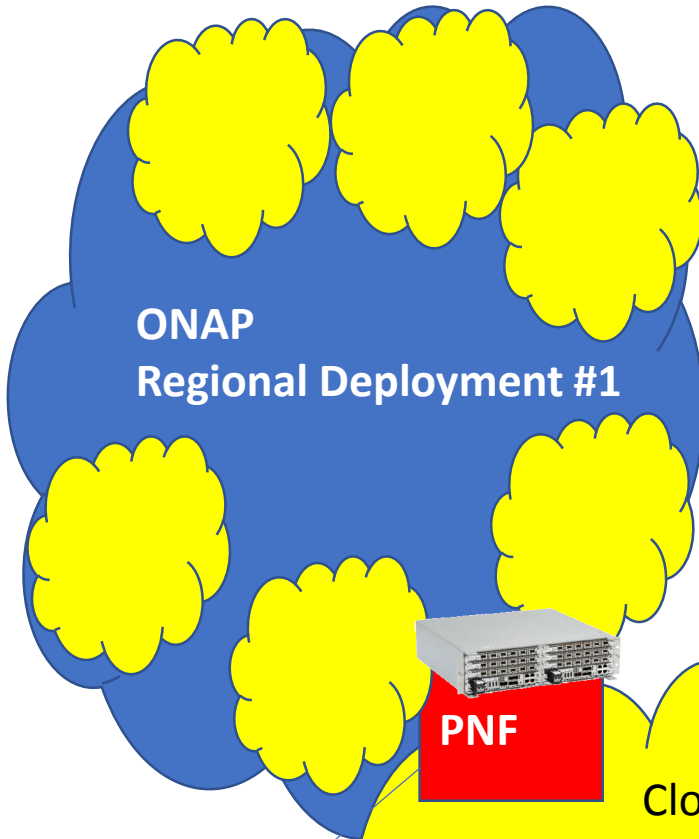
COMPLEX OBJECT

Physical Location

Manhattan
Freedom Tower
123 Main St.



Staten Island



ONAP
Regional Deployment #1

PNF

LATA

PNF
Controller

Cloud Region
Object

Cloud Region #1

Complex
Object

Complex
Object

Complex
Object



DCAE IMPACTS

DCAE PROJECT IMPACTS

**Security
Validation**

Authenticate Connection

MONITORING

Monitoring definitions – SDC has a side monitoring template designer. Way to define monitoring alarms etc; In AT&T there is a project; IN ONAP code is there finalizing code; pluggable modeler for monitoring. DCAE as part of onboarding specify what VES template. DCAD define microservices for monitoring. How is PNF monitored & correlated. If [x] goes down how is this correlated. SDC would define the Modeling what needs to be monitored and how they would correlated with other events from other NE. Thresholds. [Baby step to process get an alarm from PNF, YAML file describes fault VES event, Fault meta-data; alarms generate].

**(PRH DCAE
Plug-in)**

(see PRH Impacts)

SDN-R (Controller) IMPACTS [APP-C]

SDN-R APP-C PROJECT IMPACTS



CC-SDK (SDN-R)

Artifacts from CC-SDK, APP-C

Mobility controller

Artifacts “borrowed” will become part of CC-SDK

Available for all controller persona.

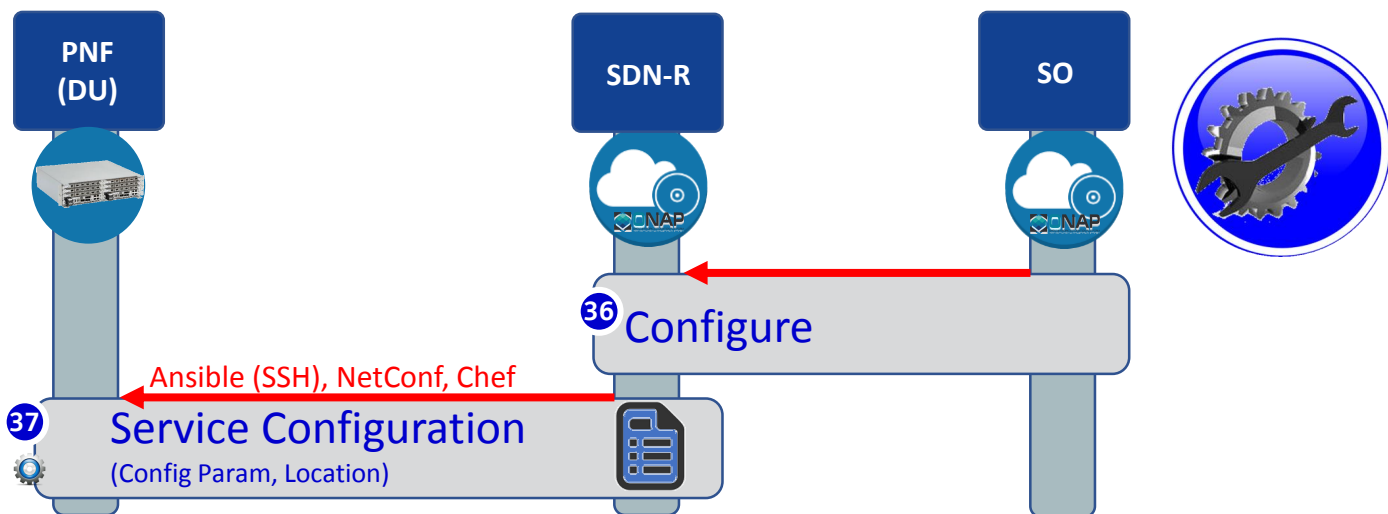
QUESTION: moving towards CC-SDK & common foundation is there anything

On top of that planned for SDN-R.

Some thing specific to wireless, ... perhaps they do not belong in CC-SDK.

Things borrowed from CC-SDK and libraries that are common.

5G Controller (SDN-R) w/ PnP in R3



SDN-R is ONAP controller derived from CC-SDK that combines functionality of APP-C & SDN-C and includes wireless artifacts.

SDN-R FUNCTIONS	DESCRIPTION
PROTOCOLS SUPPORTED	Ansible, Chef, and NetConf (all 3 will be supported)
PNF SUPPORTED	(Radio RAN Wireless) PNF Other PNFs?
PNF DATA SUPPORTED	<p>(1) Configuration Parameter (optional) – SDN-R/APP-C gives the Controller IP@ to the DU. In R3, SDN-R/APP-C may pass configuration parameter(s) to the 5G DU, this will also give a configuration parameter (e.g. CU IP@).</p> <p>(2) OAM IP@ (optional) - The permanent OAM IP address is given to the PNF. The IP address assigned from SDN-C may come from the vAAA, or it may draw from a local pool of IP addresses. SDN-C performs the IP address selection. It knows if a permanent IP address should be assigned to the PNF. Note: this IP@ assignment <i>optional</i>.</p> <p>(3) Transport configuration (optional) – Transport configuration is given to the PNF.</p> <p>(4) Location (optional) – the Location configuration may be given to the PNF.</p> <p>(5) Software Version (optional) – The expected PNF Software Version(s).</p>

SDN-R w/ PnP in R3

SDN-R FUNCTIONS	DESCRIPTION
PROTOCOL SPECIFIED	<p>PNF onboarding package defines of PNF (protocol). PNF info model (SDC) will have (1) protocol (2) controller:</p> <p>(1) Protocols Supported – PNF package. CM Protocol is in PNF onboarding package.</p> <p>(2) Controller type – defined in design time. Controller type is specified in design time. Design time designer specifies which controller is used.</p> <p>Distributed in PNF Modeling artifacts</p>
MODEL DRIVEN DESIGN	<p>APP-C, SDN-C, SDN-R, VF-C as possible controllers. Modeling which controllers will be used by the PNF. Also needs to standardize what it expects from controller. Things controller needs to support.</p>
VENDOR SPECIFIC ADAPTOR	<p>Customized DG (directed graph) element ODL (node in graph database) added with Java. Substitute a value and add fields in a template. SDN-R is following DG abstraction. If there is a vendor specific plug-in in the service model it can be represented as a node in DG and the interaction will be captured in that model.</p>
UPDATING PNF & CONTROLLER RELATION INFO	<p>Updating the controller/protocol (“lifecycle management”).</p>
ERROR LEGS (ERROR FLOWS)	<p>Errors when SDN-R interacts w/ a PNF</p>

SDN-R w/ PnP in R3

SDN-R is ONAP controller derived from CC-SDK that combines functionality of APP-C & SDN-C and includes wireless artifacts.

SDN-R is a sub-project of SDN-C.

“Is SDN-R is a sub-project of SDN-C. If not what is it?”

SDN-R = APP-C for RAN. “ how is SDN-R common to APP-C “

ISSUE:

Concern that SDN-R replicates functions (e.g. SDN-C does IP assignments).

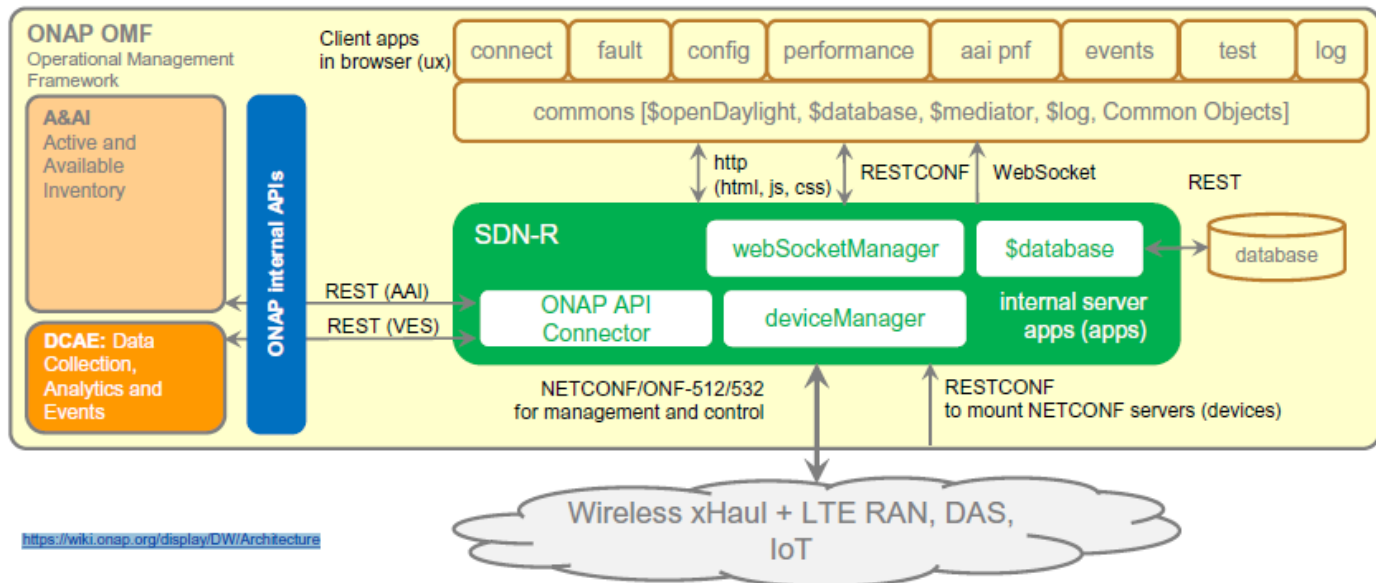
SDN-C configures/creates Networks.

SDC would need to be aware of another SDN-controller, new logic to pass DGs.

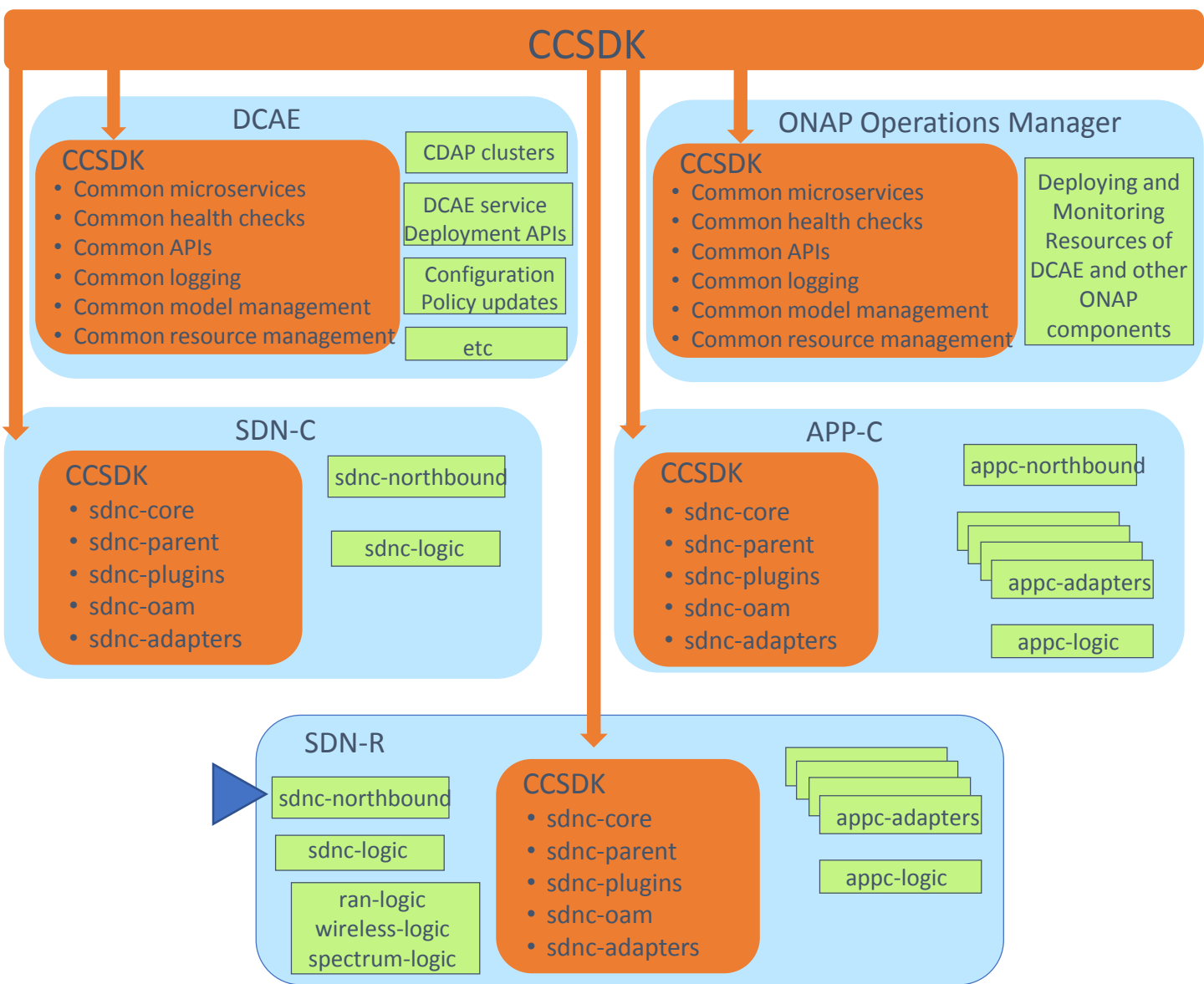
ISSUE:

“SDN” implies a networking controller vs an PNF “App” controller

SDN-R app controller for PNF/VNFs vis a vis LCM.



CC-SDK based Mobility Network Function Controller (MNFC) for Mobility/Wireless



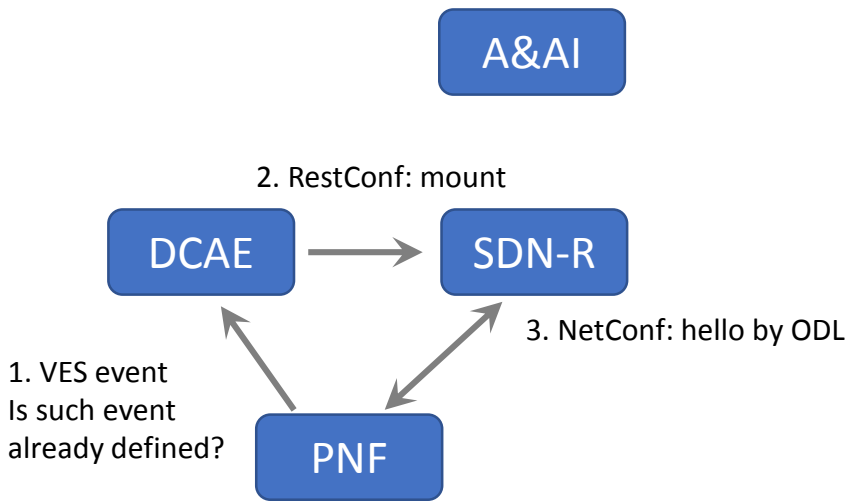
SDN-R

- Evolving to become the one ONAP Controller for Mobility/Wireless PNF/VNF
- Sub-project in SDN-C

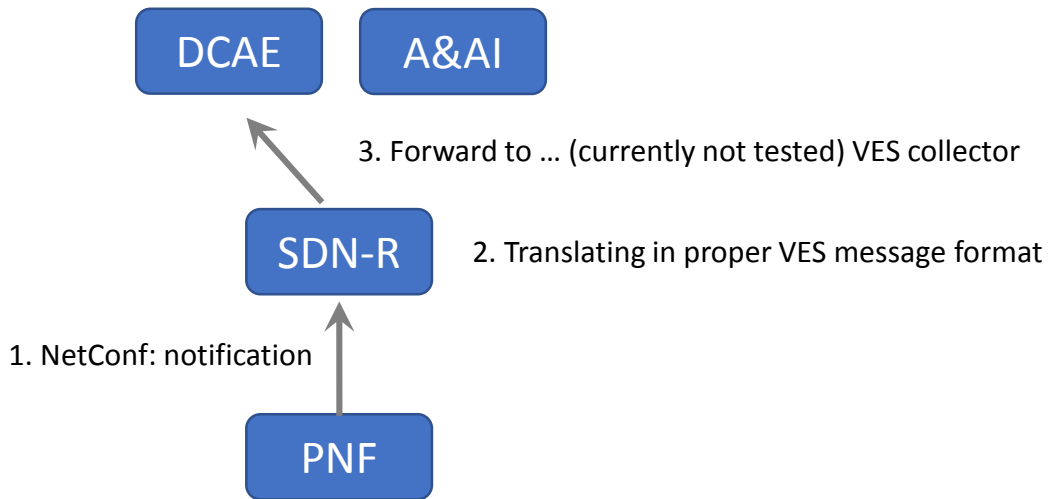
SDN-R intended to be a stand-alone controller
Only organizationally is SDN-R a sub-project of SDN-C

SDN-R uses SDN-C Northbound (verify - ?)

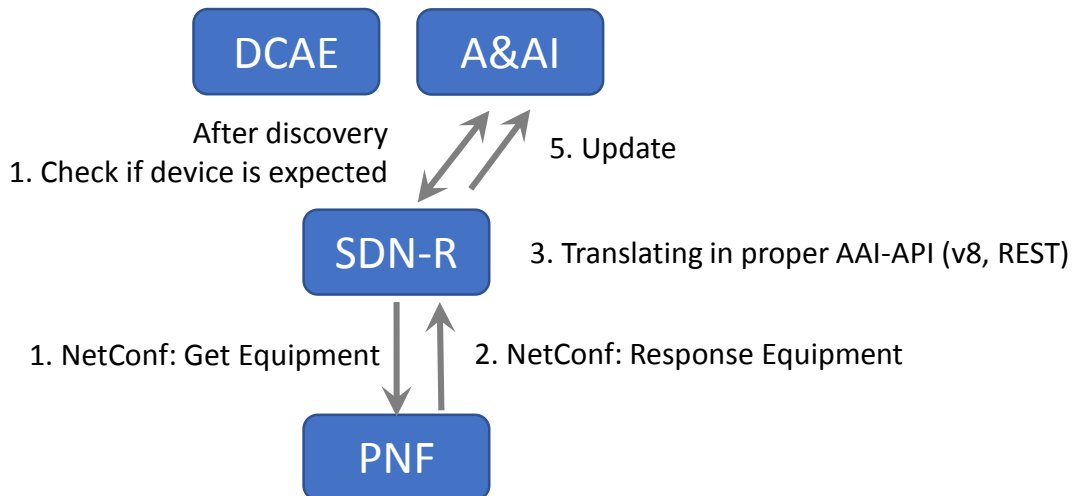
SDN-R Device Discovery



SDN-R Event Flow



SDN-R A&AI Flow





PNF Plug and Play INTEGRATION & SHOWCASING

- ONAP and PNF Plug and Play for 5G RAN
- 5G Use Case Team

STEP	TEST CASE	RE:EASE
1 Resource Definition	1 Resource Definition	R2 (Beijing)
2 Service Definition	2 Service Definition	R3 (SDC: new PNF model)
3 Type Modeling Artifacts	3 Type Modeling Artifacts	R2 (Beijing)
4 Resource Declaration	4 Resource Declaration	R3 (Alt Operator`s Inventory Management system)
5 Create A&AI PNF Entry	5 Create A&AI PNF Entry	R3 (ibid)
13 ONAP Compliant S/W	13 ONAP Compliant S/W	R2 (Beijing)
15 Work Order to SO	15 Work Order to SO	R3 (SO R2 Integration)
16 Service Instantiation	16 Service Instantiation	R3 (SO R2 Integration)
17 Homing OOF Sniro	17 Homing OOF Sniro	R3 (SO R2 Integration)
18 Resource RLF	18 Resource RLF	R3 (SO R2 Integration)
19 Check A&AI Entry	19 Check A&AI Entry	R3 (SO R2 Integration)
20 Create A&AI Entry	20 Create A&AI Entry	R3 (SO R2 Integration)
21 Subscribe VES Event	21 Subscribe VES Event	R3 (SO R2 Integration)
22 RLF Thread Terminates	22 RLF Thread Terminates	R3 (SO R2 Integration)
25 Authenticates PNF Connection	25 Authenticates PNF Connection	R3 (Casablanca)
26 PNF Registration VES Events	26 PNF Registration VES Events	R3 (pnfRegistration domain)
27 Inventory Query	27 Inventory Query	R3 (pnfRegistration domain)
29 Inventory Query	29 Inventory Query	R3 (pnfRegistration domain)
30 Update PNF Entry	30 Update PNF Entry	R3 (pnfRegistration domain)
31 PNF Ready	31 PNF Ready	R3 (pnfRegistration domain)
34 Update PNF WF	34 Update PNF WF	R3 (SO R2 Integration)
35 Network Assignments	35 Network Assignments	R3 (SO R2 Integration)
36 Configure	36 Configure	R3 (SO R2 Integration)
37 Service Configuration	37 Service Configuration	R3 (controller updates)
38 SO Updates w/ Assginments	38 SO Updates w/ Assginments	R2 (Beijing)
39 Controller Replies	39 Controller Replies	R2 (Beijing)
40 Service Running	40 Service Running	R2 (Beijing)
41 Monitors Service	41 Monitors Service	
42 Inform OSS	42 Inform OSS	

INTEGRATION TEAM IMPACTS

INTEGRATION TEAM IMPACTS

SHOWCASING

DEMO CONTENT – [Closed] What will be **showcased**? Test send registration event. Instantiation Pt1/Pt2 (Update A&AI). PRH service request (VES event & DMaaP topic). APP-C Ansible configure. PNF sends event, receives ansible event. Start with R1 use case (VoLTE / vCPE) upgraded w/ mechanisms of R2. DU Emulator (for registration).

ACTUAL PNF, DU Emulator

DU EMULATOR – [Closed] Nokia will provide a simple DU emulator [Mar 16 2018]. Capable of sending PNF registration request (Step 26, 28). Capable of receive configuration command from APP-C via Ansible (Step 37) and recording result of successful reception (or failure) in a log.

Test Case Description (Demo Document) [Open Point]

(1) **Demo Document** – Document describing demo (use case group?) <https://wiki.onap.org/display/DW/vCPE+Use+Case+Tutorial%3A+Design+and+Deploy+based+on+ONAP+Amsterdam+Release>
 (2) **Test case description** – Documenting the test case. Start with VoltE and modify it.

LOGISTICS (Open Point)

(1) **DEMO ANNOUNCEMENT** – “come see this demo” – Integration ONAP Wiki. Video. Schedule ONAP Wiki Events Calendar. Integration project. (SME = x).
 (2) **LOGISTICS** – *Contacts* Helen Chen, Yang Xu. Intel Windriver Lab, T-Lab (AT&T Lab, Bedminster), and/or use CMCC Lab. ONAP “Open Lab”. ONAP installed in a lab. Demo shown via conference. Virtual Demo (dial in).
 (3) **RELEASE MANAGER** – Coordinate w/ Joe Gildas. Joe Gildas release manager (status of project). M4 Voting.

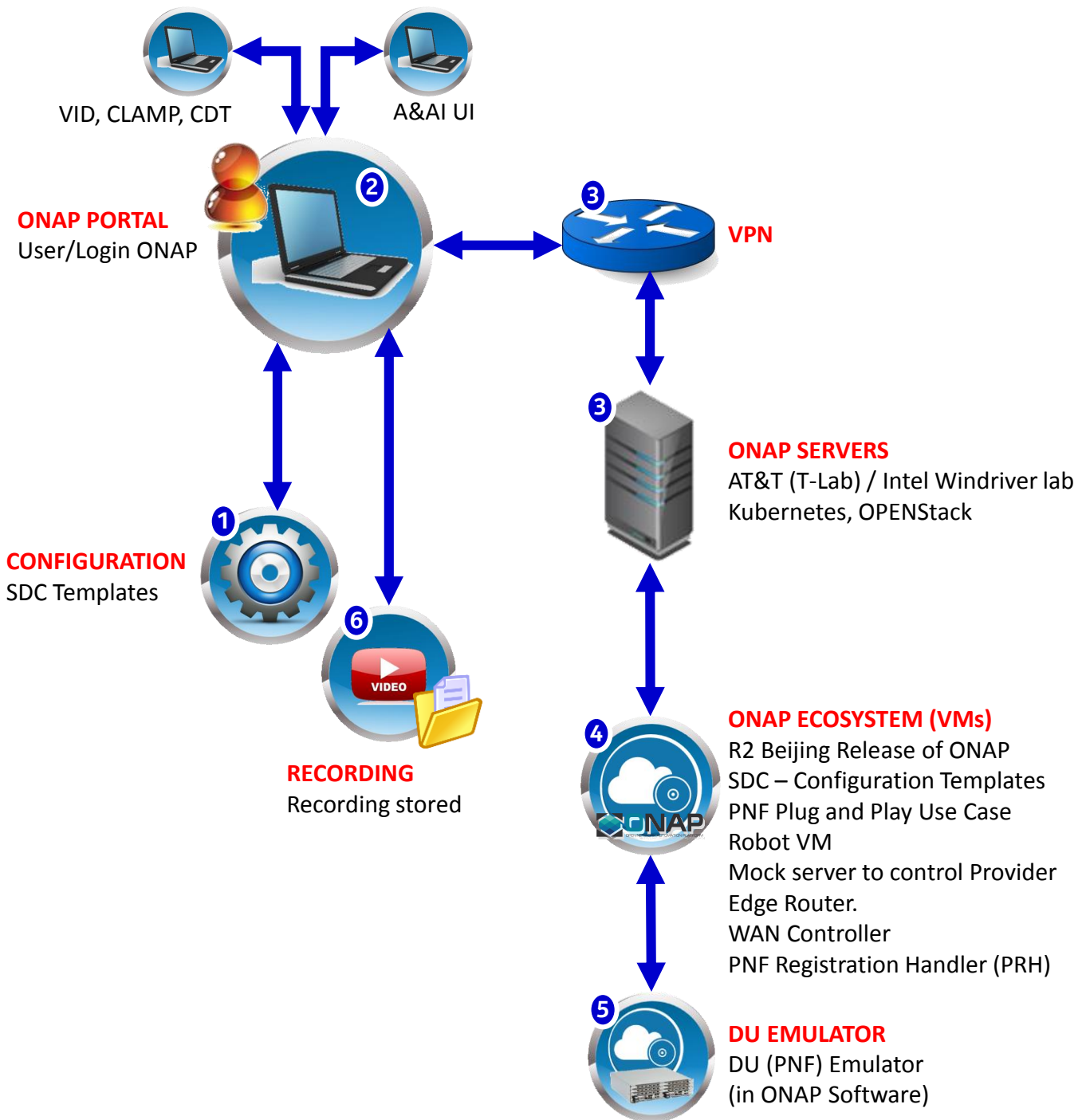
AUTHENTICAT ION

AUTHENTICATION – Authentication is optional, and for R2 Demo we will not have any authentication. Could be considered for Casablanca (R3). Amsterdam authentication flow not useful for PNFs. Not use second vDHCP & vAAA.

CONTROLLER CONFIGURATI ON

CONFIGURATION: IP address (from DHCP). Username & Password. Configured in controller (manually added to ONAP). VES configuration (do not need username & password to be configured on VES)

DEMO ARCHITECTURE



STEP	DESCRIPTION
1	<p>CONFIGURATION – SDC Design templates need to be configured in preparation of the Demo & Showcasing. The appropriate PNF and VNF designs are designed, validated and exported to the other components of ONAP.</p>
2	<p>PORTAL & GUI – The ONAP Portal is used to access the appropriate GUIs and interfaces necessary to operate and configure ONAP. The VID and CLMAP GUI are used to configure the appropriate information for the showcase. The A&AI GUI are used to show the created entries in A&AI for the PNF.</p>
3	<p>VPN – The appropriate security gateways and/or VPN networks are configured. The appropriate security setups are authenticated against. Passwords and IP addresses that are needed to connect to the ONAP servers go through this VPN or security gateway (as appropriate)</p> <p>ONAP SERVERS – The ONAP Servers that host the ONAP ecosystem are connected to</p>
4	<p>ONAP ECOSYSTEM (VM) – The ONAP ecosystem has all of the appropriate Virtual Machines necessary to operate. This has the R2 Beijing Release of ONAP. All of the PNF Plug and Play Use Case updated software is available in the ONAP Ecosystem. The Robot VM, Mock server to control Provider Edge Router, and WAN Controller are established.</p> <p>The PNF Registration Handler a new DCAE plug-in are available in this ONAP ecosystem which is used to register the PNF into ONAP.</p>
5	<p>DU EMULATOR – The DU Emulator is used to emulate the responses and connection to ONAP. The DU emulator establishes a VES HTTPS connection with the PRH during the registration process and receives a APP-C response back via ansible.</p>
6	<p>RECORDING – A recording is made of the showcase and demo for later upload/download and playback for demonstration purposes.</p>

Need a integration details on SDC modeling/CSAR package



PNF Plug and Play ROADMAP (After Casablanca)

- ONAP and PNF Plug and Play for 5G RAN
- 5G Use Case Team

FUTURE FUNCTIONS

ONAP Project	IMPACT
Licensing Management	Licensing Impact – meta-data managing licensing. PNF (DU#55) – Service on DU (5G) [feature xyz] Licensing Management (FUTURE)
(VNF 5G Flow)	[in Casablanca] a use case for VNF & PNF bringup.

PNF PACKAGE

ALARM DEFINITIONS

Alarm Dictionary
(Vendor provided)



YAML Definitions
(Vendor provided)



PNF Alarm #22
#22 S/W problem xyz
VES = fault fields; "fault" domain publish DMaaP
Clamp, Analytic, Holmes – [#22 event]
Dictionary looks up #22 ->

MEASUREMENT DEFS

Measurement
Dictionary
(Vendor provided)



Measurement
Schema
(Vendor provided)



YAML Definitions
(Vendor provided)



NF PACKAGE

Artifacts
Definitions
TOSCA-Metadata
MainServiceTemplate.mf
MainServiceTemplate.yaml

CSAR file



CONFIGURATION DEFS

Configuration
Schema
(Vendor provided)



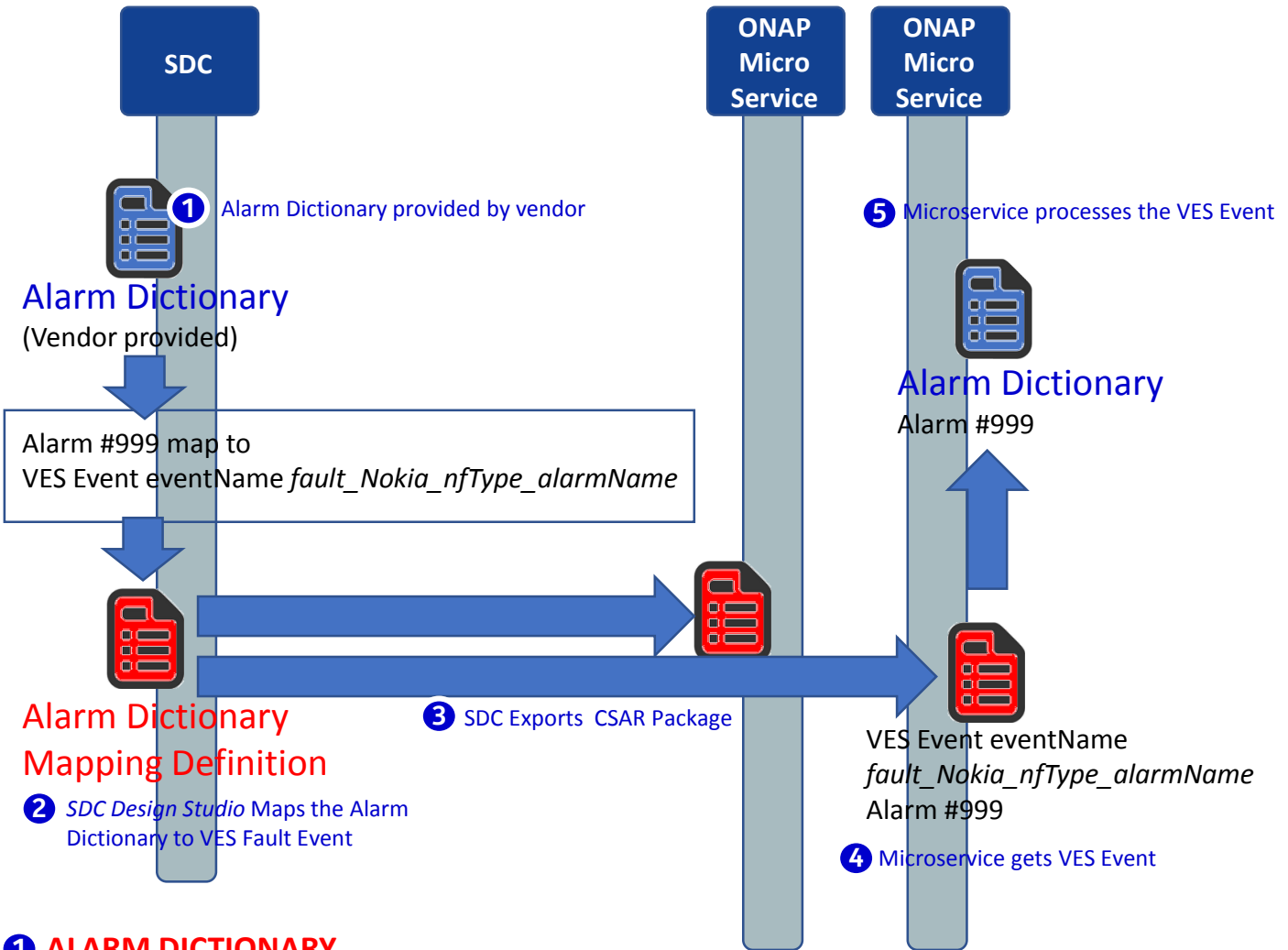
YAML Definitions
(Vendor provided)



Need to define a common "template" that all vendors
Provide dictionaries for. DCAE-DS responsible for
reading these files. Closed Loop. Vendor describe
alarms being sent. Definition what alarms correlated
to (collecting, triggers). CLAMP performs analysis,
design of who uses it is SDC. Holmes monitoring
micro-services (to receive alarms).

Communication STANDARDS we want to support?
[Data Format]

Alarm Dictionary Usage



1 ALARM DICTIONARY

Alarm Dictionary defines all alarms/faults published by xNF (x=V or P)
Based on 3GPP TS32.111, ETSI, and VES document (v6.0)

2 SDC DESIGN STUDIO MAPS VES FAULT Event to Alarm Dictionary

SDC Design studio does mapping of Alarm dictionary entries to VES Fault Events to produce a “mapping” definition in the CSAR package. (RATHER than mS doing the mapping because it is more model driven)

3 SDC DISTRIBUTES DEFINITIONS

SDC creates a definition of how to start-up service. SDC exports the *CSAR package* with the VES Fault to Alarm dictionary mapping definitions.

DEFINITIONS & ARTIFACTS (CSAR PACKAGE)

1. VES-Alarm mapping definition passed by SDC (CSAR Package) to ONAP components
2. DCAE micro-service gets CSAR package

4 MICRO SERVICE GETS FAULT EVENT

Microservice has subscribed to fault domain DMaaP Topic and receives the VES Fault Event from xNF in run-time.

5 MICRO SERVICE PROCESSES EVENT

Microservice processes the VES Event using the Alarm Dictionary

Alarm Dictionary Usage

ALARM DICTIONARY PURPOSE


- (1) DICTIONARY** - it allows for a readily accessible body of the entire set of alarms & faults that are managed by a PNF. It would allow for an operator to see all of the alarms & faults of a PNF without having to wait for individual alarms & faults to arrive in ONAP.
- (2) Analytics facilitator** – A dictionary would allow for a variety of vendor specific (or vendor agnostic) analytics applications to be developed. There are a variety of fields in the Alarm Dictionary that would facilitate such analytics capabilities as correlation, escalation, isolation, recovery actions, self-healing, and life cycle management functions.
- (3) GENERAL ANALYTICS** – The strength of ONAP is the potential ability to coordinate information from multiple sources, different vendors, and disparate types of NFs. A dictionary can form the foundation for generalized analytics that are vendor agnostic.

FAULT DICTIONARY PURPOSE

- (1) FAULTS vs ALARMS** - Fault can be a condition encountered in run-time that does not necessarily create a customer-facing alarm. An alarm is intended to result in a visual notification to a service provider to take action. An analogy would be the “Check engine” light in your car which would correspond to an Alarm. A solenoid, a carburetor, or distributor fault all might lead to a “Check engine” light. A driver (service provider) may not be able to directly act on the specific fault (or indeed care about the fault); but when the “check engine” light went on would know to take some action (go to the service station).

NF ALARM DICTIONARY FIELDS (Template)



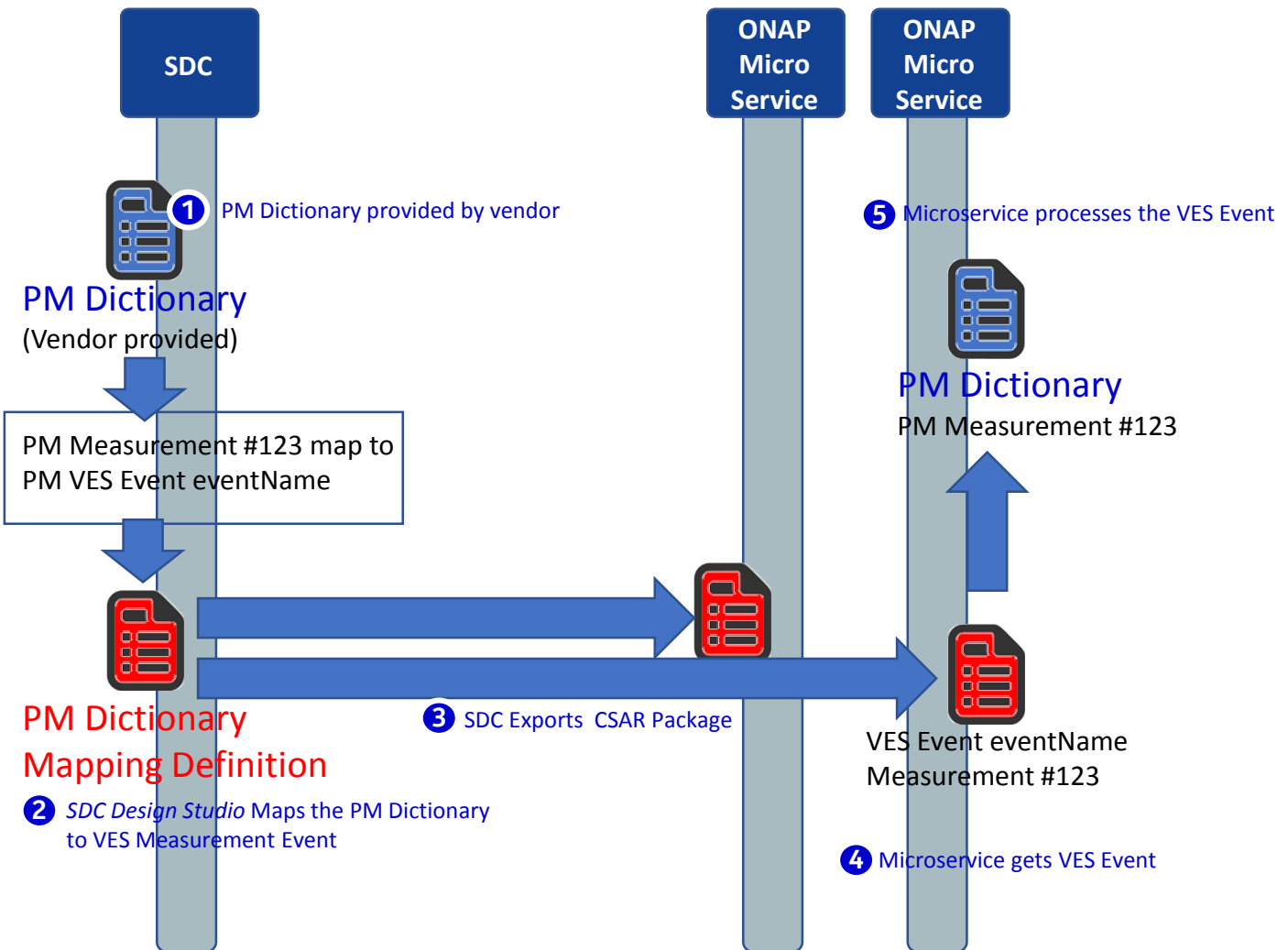
ALARM FIELD	DESCRIPTION
Alarm Dictionary Index 	<p>Gives the Identifier for the alarm. This is also the Identifier that is used in the VES event so it can be used to associate the event with the definition entry.</p> <p>The VES Event <i>EventID</i> would encode the Alarm number which will correspond to the Alarm Index.</p> <p>EXAMPLE: 12345</p>
Alarm Name	<p>Alarm Name which will be used in the Event Name. Note <i>this maps to the alarmCondition in the VES Fault Event in faultevent fields.</i></p> <p>EXAMPLE: Synchronization Lost</p>
Event Type	<p>Indicates the type of alarm. The types are: Communications Alarm, Processing Error Alarm, Environmental Alarm, Quality of Service Alarm, Equipment Alarm, Integrity Violation, Operational Violation, Physical Violation, Security Service Violation, Mechanism Violation, or Time Domain Violation. Note <i>this maps to the eventCategory in the VES Fault Event in faultevent fields.</i></p> <p>EXAMPLE: Quality of Service Alarm</p>
Meaning of Alarm	<p>Provides a descriptive meaning of the alarm condition. This is intended to be read by an operator to give an idea of what happened.</p> <p>EXAMPLE: Synchronization has been lost</p>
Effect of Alarm	<p>Provides a description of the consequence of the alarm condition. When this alarm condition occurs. This is intended to be read by an operator to give a sense of the effects, consequences, and other impacted areas of the system.</p> <p>EXAMPLE: Loss in Quality of Service</p>
Managed Object(s)	<p>Managed object (MO) associated with this Alarm. Note <i>this maps to the eventSourceType in the VES Fault Event in faultevent fields.</i></p> <p>EXAMPLE: Clock (MO)</p>
Probable Cause	<p>Provides the probable cause qualifier for the alarm. Probable causes are found in 3GPP TS 32.111 Annex B drawn from ITU-T M.3100 and from ITU-T Recommendation X.721, X.733, and X.736</p> <p>EXAMPLE: lossOfSynchronisation</p>
Probable Cause Number	<p>Probable Cause Number the numeric value associated with the Probable Cause</p> <p>EXAMPLE: 76</p>
Specific Problem	<p>(Optional) It provides further qualification on the alarm than probable Cause. This attribute value shall be single-value and of simple type such as integer or string. Defined in ITU-T Recommendation X.733 Clause 8.1.2.2. Note <i>this is the 3GPP Specific problem not be confused with the specificProblem field of the VES Fault Event in faultevent fields.</i></p>
Proposed Repair Actions	<p>It indicates instructions for proposed repair actions. These are defined in ITU-T Recommendation X.733 clause 8.1.2.12.</p> <p>EXAMPLE: Reset the BTS, ONAP Controller does x</p>
Clearing Type	<p>Indicates whether the alarm is automatically or manually cleared</p> <p>EXAMPLE: Automatic</p>
Additional Text	<p>This field contain further information on the alarm. This attribute provides <i>vendor specific</i> alarm information. A specific condition for this optional population is when an alarm presented by the EM has different values of perceived severity, and / or alarm type.</p> <p>EXAMPLE: Specific data 10</p>
Associated Fault(s)	<p>Indicates the associated faults that triggered this alarm. List of fault(s) associated with the alarm cross indexed against a vendor provided fault information.</p> <p>EXAMPLE: Fault 99999</p>

NF FAULT DICTIONARY FIELDS (Template)



DEFINITION FIELD	DESCRIPTION
Fault Id	Gives the Identifier for the alarm. This is also the Identifier that is used in the VES event so it can be used to associate the event with the definition entry. EXAMPLE: 99999
Fault Name	Alarm Name which will be used in the Event Name. Note <i>this maps to the alarmCondition in the VES Fault Event in faultevent fields.</i> EXAMPLE: Loss of Synchronization
Fault Description	Provides a descriptive meaning of the alarm condition. This is intended to be read by an operator to give an idea of what happened. EXAMPLE: Synchronization due to PTP IEEE1588 Failure
Managed Object(s)	Managed object (MO) associated with this Alarm. Note <i>this maps to the eventSourceType in the VES Fault Event in faultevent fields.</i> EXAMPLE: Clock (MO)
Effect of Fault	Provides a description of the consequence of the alarm condition. When this alarm condition occurs. This is intended to be read by an operator to give a sense of the effects, consequences, and other impacted areas of the system. EXAMPLE: Loss of synchronization affect QoS
Associated Alarm(s)	Indicates the associated faults that triggered this alarm. List of fault(s) associated with the alarm cross indexed against a vendor provided fault information. EXAMPLE: 12345
Proposed Repair Actions	It indicates instructions for proposed repair actions. These are defined in ITU-T Recommendation X.733 clause 8.1.2.12. EXAMPLE: Reset BTS
Additional Text	This field contain further information on the alarm. This attribute provides <i>vendor specific</i> additional fault information.

PM Dictionary Usage



1 PM DICTIONARY

PM Dictionary defines all measurements published by xNF (x=V or P)

Based on 3GPP TS32.503, ETSI, and VES document (v6.0) [has Cloud scaling counters]

2 SDC DESIGN STUDIO MAPS VES FAULT Event to PM Dictionary

SDC Design studio does mapping of PM dictionary entries to VES Fault Events to produce a “mapping” definition in the CSAR package.

3 SDC DISTRIBUTES DEFINITIONS

SDC creates a definition of how to start-up service. SDC exports the *CSAR package* with the VES Fault to PM dictionary mapping definitions.

DEFINITIONS & ARTIFACTS (CSAR PACKAGE)

1. VES meas mapping definition passed by SDC (CSAR Package) to ONAP components
2. DCAE micro-service gets CSAR package

4 MICRO SERVICE GETS MEASUREMENT EVENT

Microservice has subscribed to fault domain DMaaP Topic and receives the VES Fault Event from xNF in run-time.

5 MICRO SERVICE PROCESSES EVENT

Microservice processes the VES Event using the PM Measurements Dictionary



APPENDIX & Meeting Notes



DISCUSSION MAY 03, 2018

SDN-R supports all 3

CC-SDK controller

Should support all 3

How does that get implemented

PNF agnostic/future-proof

PNFs will support one

ADAPTORS/MEDIATORS

Adaptor – No adaptor

PNF talks directly to ONAP

Adap/transl/mediators

For embedded base.

5G “going native”

PNF – Descriptor

Protocols supports

PNF Package defines

The Meta-models Tbsupported

mm microwave PNF unchanged

ID PNF

PNF #62

SDN-C
UUID

PNF #62

A&AI

Mac Address
IP Address

Correlation ID
(UUID)
PNF #62

Gets Assigned a UUID

Just like any VNFID

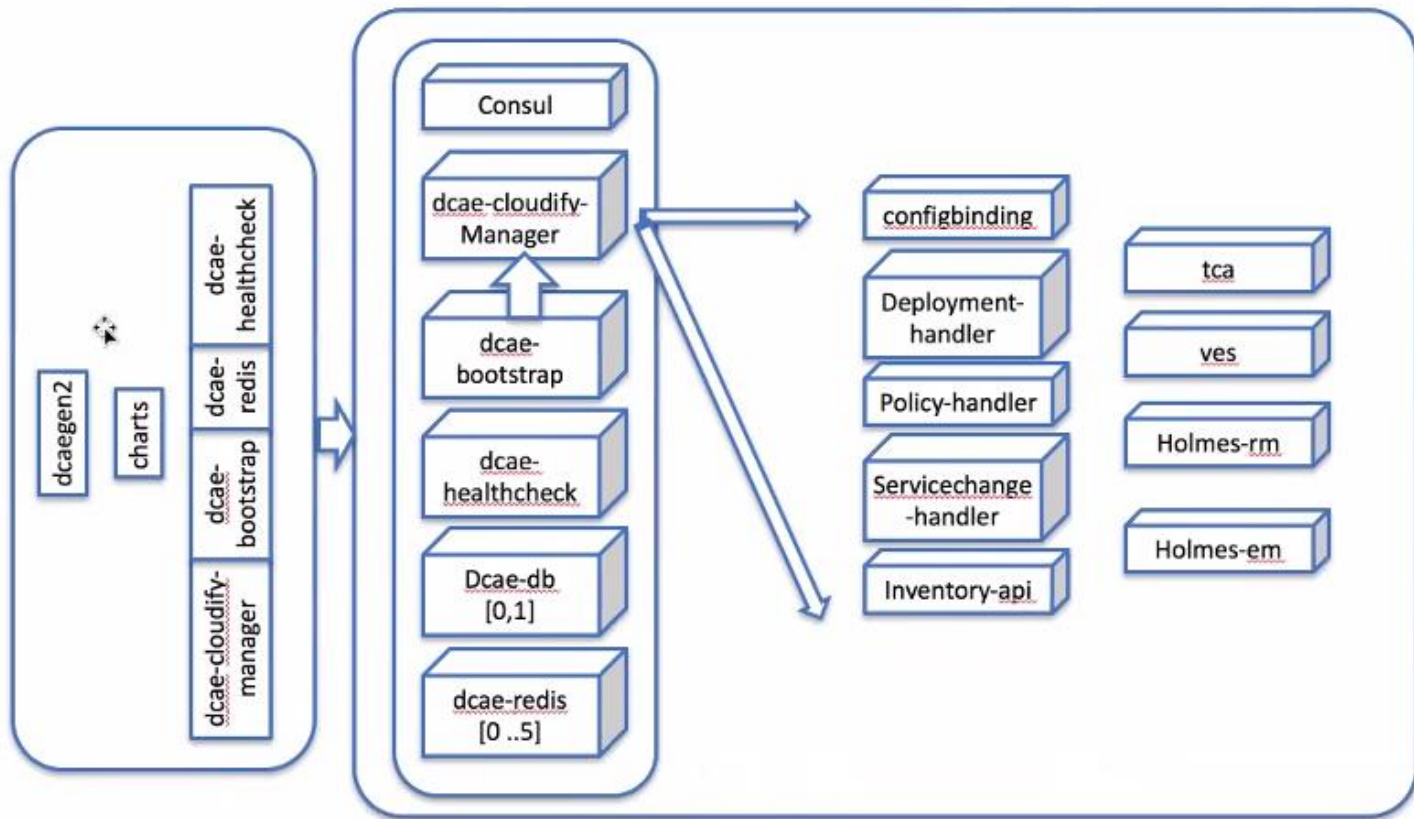
From then on processes of ONAP

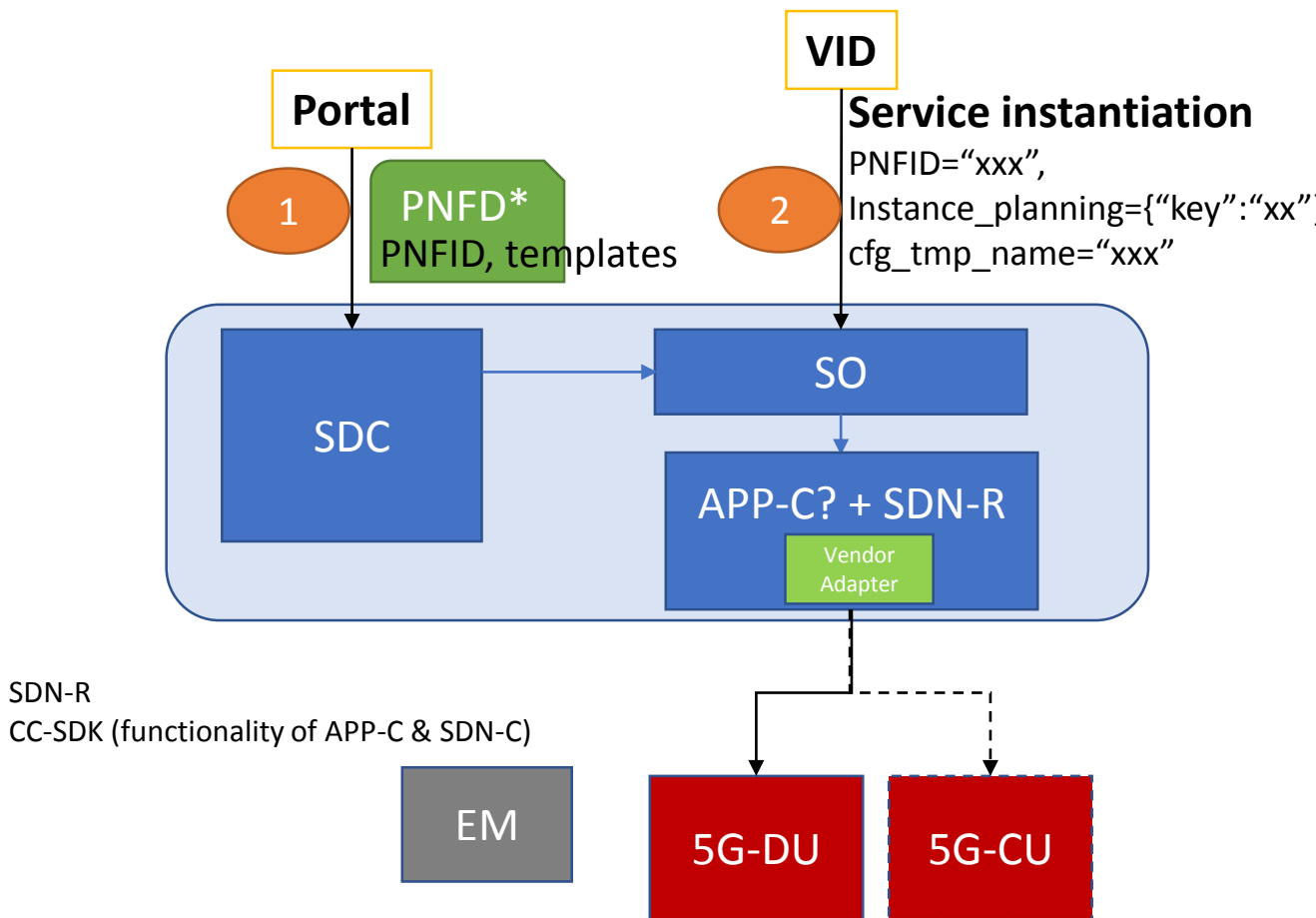
Work on UUID

CorrelationID is no longer used.

UUID assigned by SDN-C (rules how UUIDs assigned)

DCAE Kubernetes Deployment



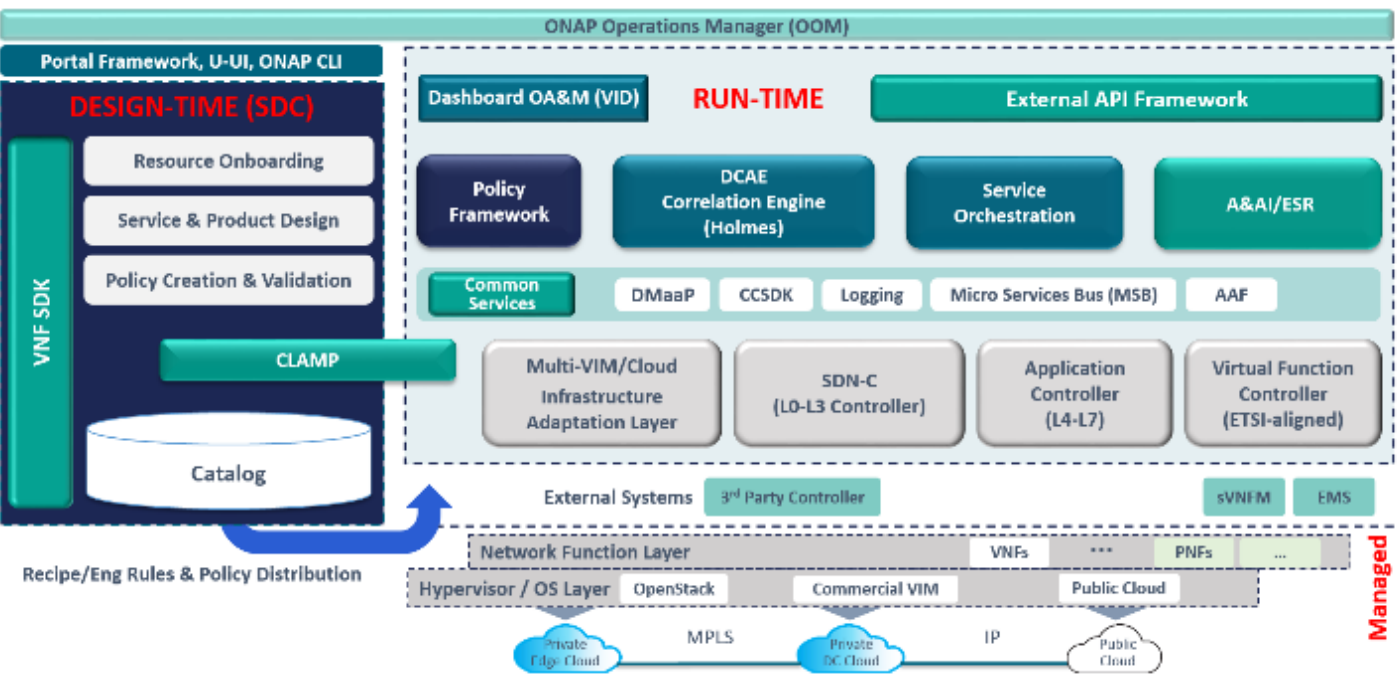
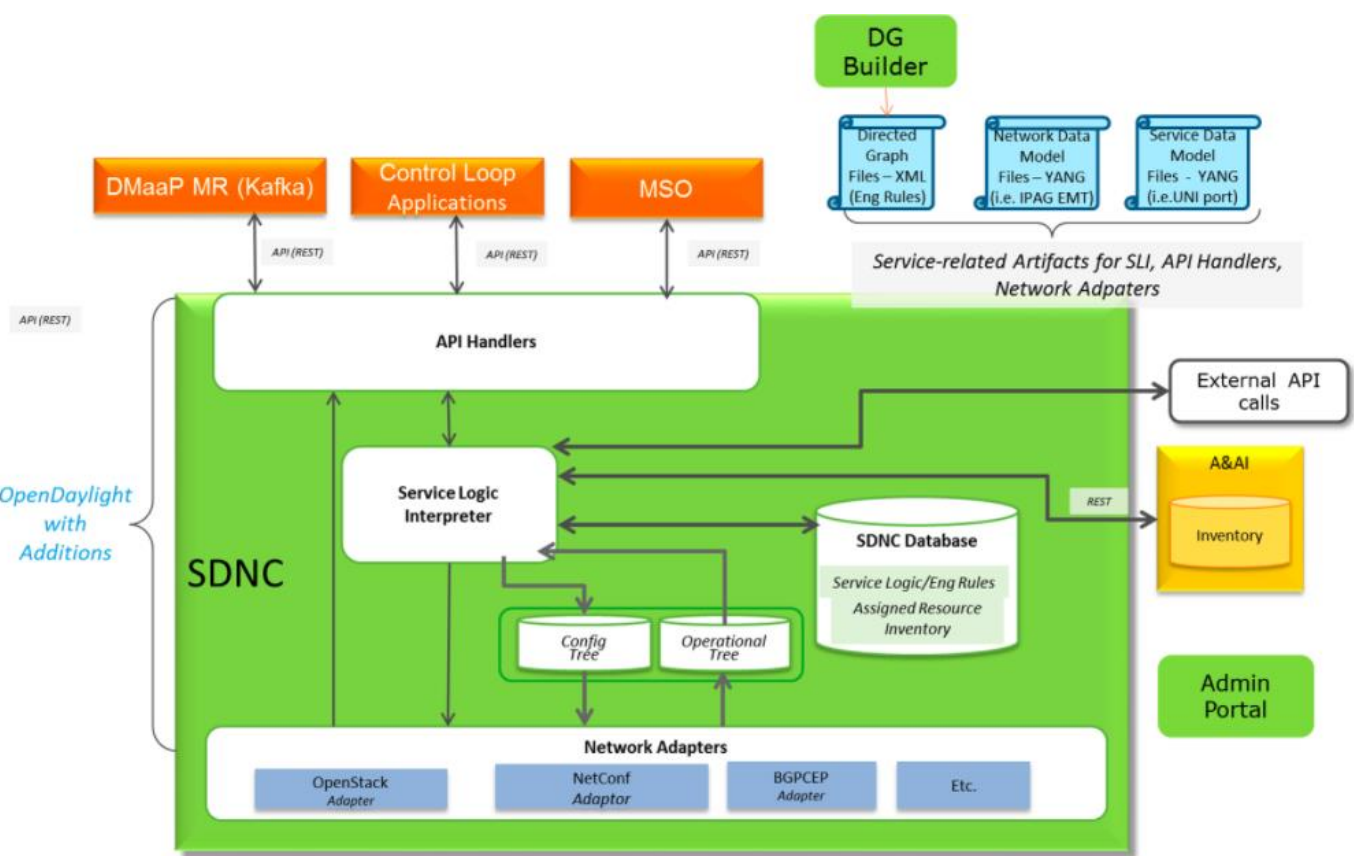


Design time

- (1) Onboarding PNFD
 - PNFID
 - Templates, including PNF/VNF templates, Configuration templates

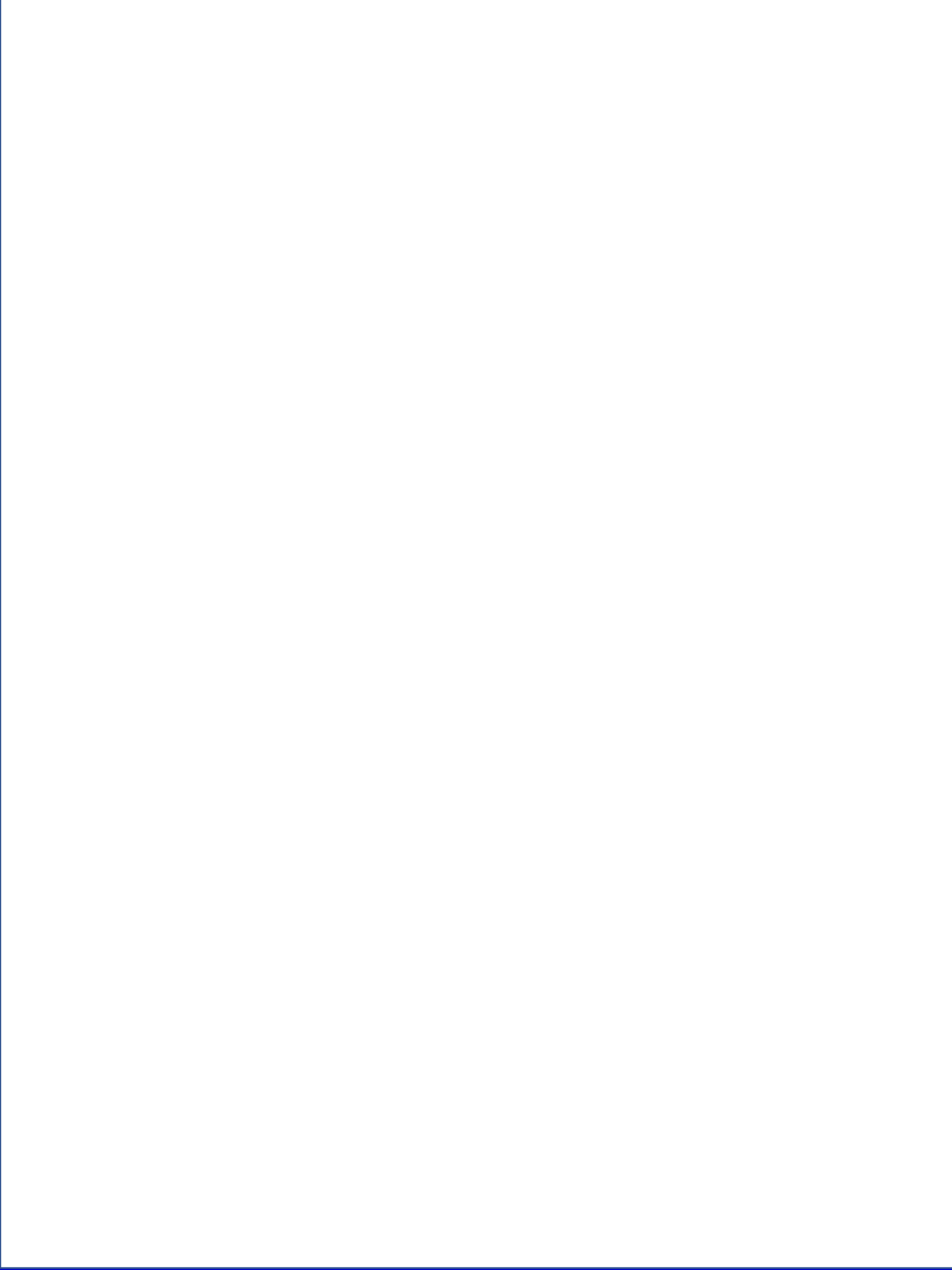
Run time

- (2) service instantiation
- (3) generate configuration data
- (4) configure PNF/VNF via EM
- (5) CU-DU inter-connect



Design onboarding/ Policy/API...	Closed Loop Design and performance	Instantiation portal	Automation rules execution	Data Collection Analytics and Events	Real time Inventory	Camunda- based Orchestration	VIM adaptation	SDN Controller	Application Controller (VNFs/PNFs)
SDC	CLAMP	VID	Policy	DCAE	A&AI	SO	Multi VIM	SDN-C	APP-C





- Release 2 Use Cases
 - Beijing Functional Requirements for TSC Approval
 - Beijing Release Approved Functional Requirements
 - Change management functional requirement
 - Hardware Platform Enablement in ONAP
 - Manual scaling functional requirement
 - Manual Scaling Impacts to ONAP Projects
 - Scale Out Use Case Meetings
 - Scale Out Use Case Tracking**
 - PNF support functional requirement
 - Merged list of R2 functional requirement candidates
 - ONAP – Centralization & Externalization of Parser I
 - R2 functional requirements candidates (extracted fr
 - R2 list of prioritized features, outcomes of Paris-Sa
 - Use case proposal: 5G- RAN deployment, Slicing, I
 - Use Case proposal: Enterprise vCPE
 - Use Case proposal: ONAP Change Management
 - Use case proposal: ONAP service provision and act
 - Use Case proposal: SD-WAN
 - Use Case proposal: VoLTE for R2
 - Use Case Proposal - VNF Scale Out
- Use Case Evaluation Process
- Use Case Goals & Selection Criteria
- Use Case Subcommittee Meeting Minutes
- Modeling sub-committee
- Architecture Subcommittee
- Proxy List
- Architecture/Usecase subcommittees joint discussions

Pages / ... / Manual scaling functional requirement 13 JIRA links

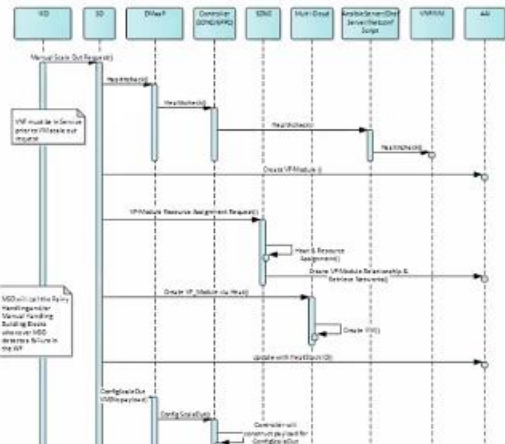
11	VNFRQTS	@Steven Wright	VNFRQTS-159 - VNF Requirements improvements to support Beijing Functional Requirements	IN PROGRESS
12	vLB/vDNS use case	@Marco Platania	INT-434 - The vLB/vDNS use case should be updated to support the manual scale out use case	DONE

Testing

Current Status

- Major Blocker: APPC is not getting configuration data for the vLB (There was a requirements gap/conflict as to how this would work and there is not enough time in Beijing. This problem will be worked in Casablanca)
- VID-226 - VF Scaling workflow not triggered CLOSED Payload to SO is not being configured properly. It could be a problem with the level of ModelInfo.
- VID-226: PROV_STATUS of VNFs are not being set to PROV. This was a process issue. Prov_status is supposed to be moved to PROV by an operator after N Since there is no operator in our test environment it never got changed. This was fixed by modifying "Robot" to update the field. (Currently working around issue by applying PROV_STATUS filter on VID) VID-226 - Manual scale out operation not scheduled/started CLOSED
- All other test cases are to be tested for Beijing Release.

End to End flow to be tested



Testing Components and Status

#	Test	Status
1	Onboard vLB to APPC via CDT	COMPLETE
2	Can configure Manual Scaling request in VID	COMPLETE
3	VID Sends a Manual Scale Out Request to SO	COMPLETE
4	SO Receives Manual Scale Out request	COMPLETE
5	SO Sends Healthcheck request to DMaaP	NOT YET TESTED
6	APPC/SDNC pick up Healthcheck request from DMaaP	NOT YET TESTED
7	APPC/SDNC sends RESTCONF Healthcheck to vLB	NOT YET TESTED
8	vLB returns Healthcheck status to APPC/SDNC	NOT YET TESTED
9	SO receives HealthCheck results	NOT YET TESTED