ONAP PNF Enhancements for Casablanca (R3, 4Q 2018) Casablanca Developer's Conference

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

Jun 11, 2018 version 6

PNF Enhancements Casablanca Summary

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 APP-C/ SDN-R 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 *PNF Onboarding Package*. Extending framework to work with PNFs. Defining PNF Package framework.

PNF Registration Handler (PRH)

(1) New VES Event domain for PNF Registration – Create new VES event domain *pnfRegistration* for PNF registration exchange

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

(4) 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.

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

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

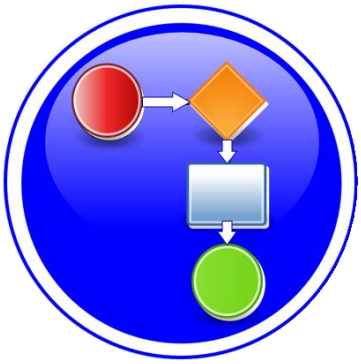
(7) FAILURE HANDLING – Registration failure cases. When & how is PNF notified when registration fails. **(8) SO INTEGRATION** – SO WF Integration.

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) SDN-R TO SO INTERACTION –SO calls 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. (SDN-R = NetConf)(?)

(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-SDK

PNF ONBOARDING / PNF PACKAGE

DESCRIPTION

(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 artifactsPNF ARTIFACTS DISTRIBUTION

CONFIGURATION DEFS

- Configuration Schema (Vendor provided)
- YAML Definitions (Vendor provided)

ALARM DEFINITIONS

- Alarm Dictionary (Vendor provided)
- YAML Definitions (Vendor provided)

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

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

Run-Time (Instances)

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**

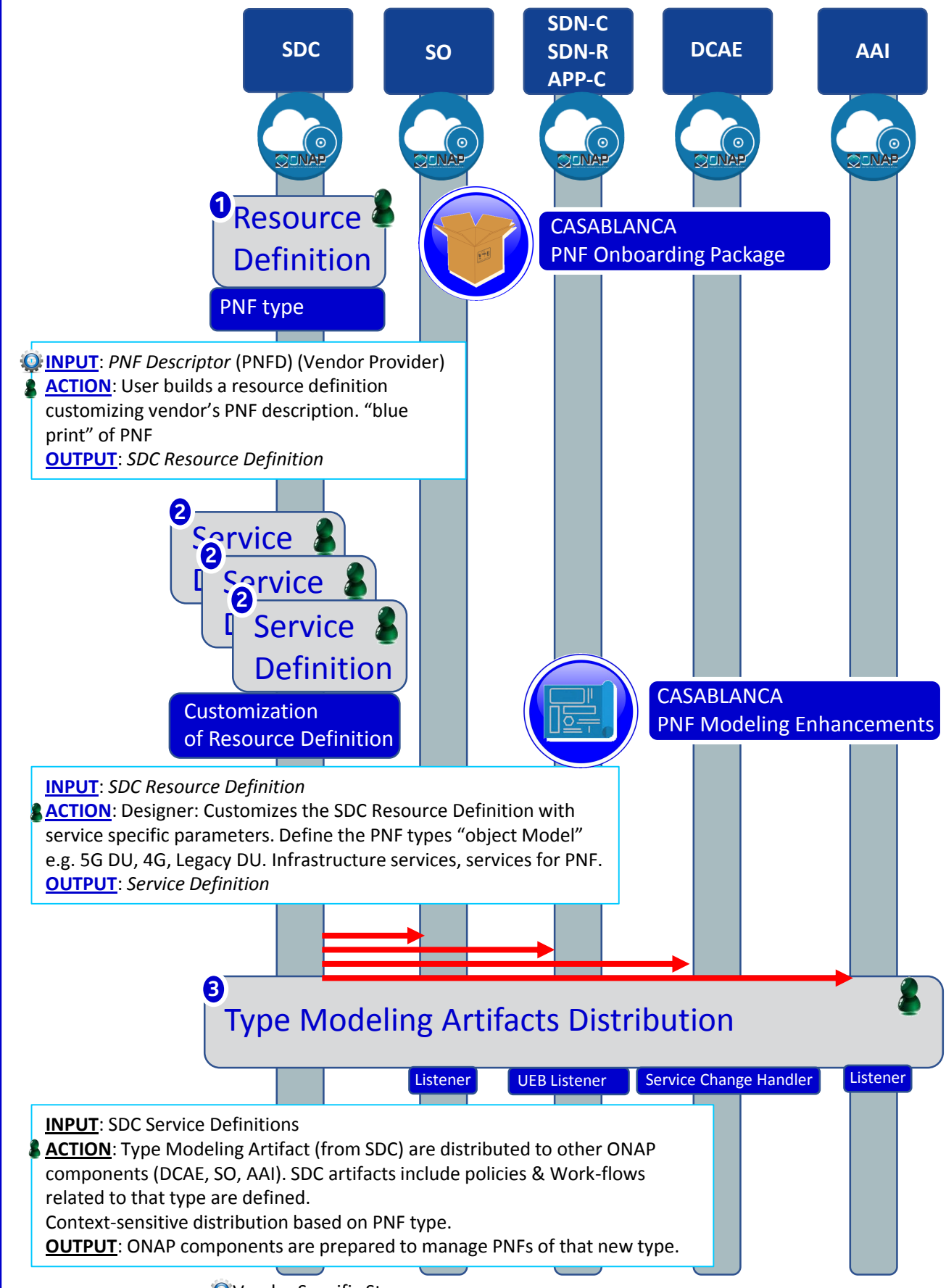
PNF connects to ONAP via a Registration Event
PNF Registration Handler (PRH) processes the event

Generic (not vendor proprietary)

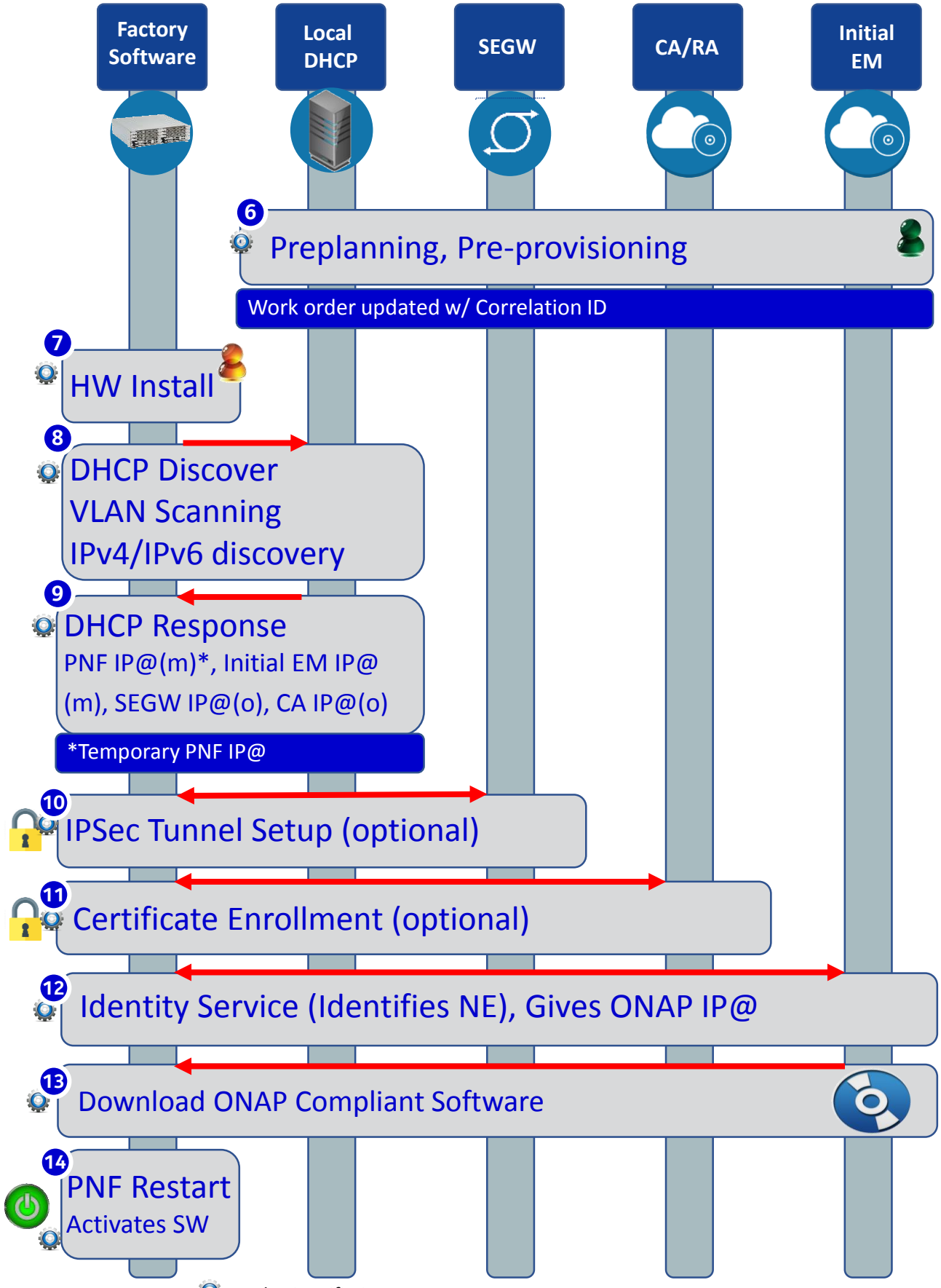
E **PNF Activation**

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

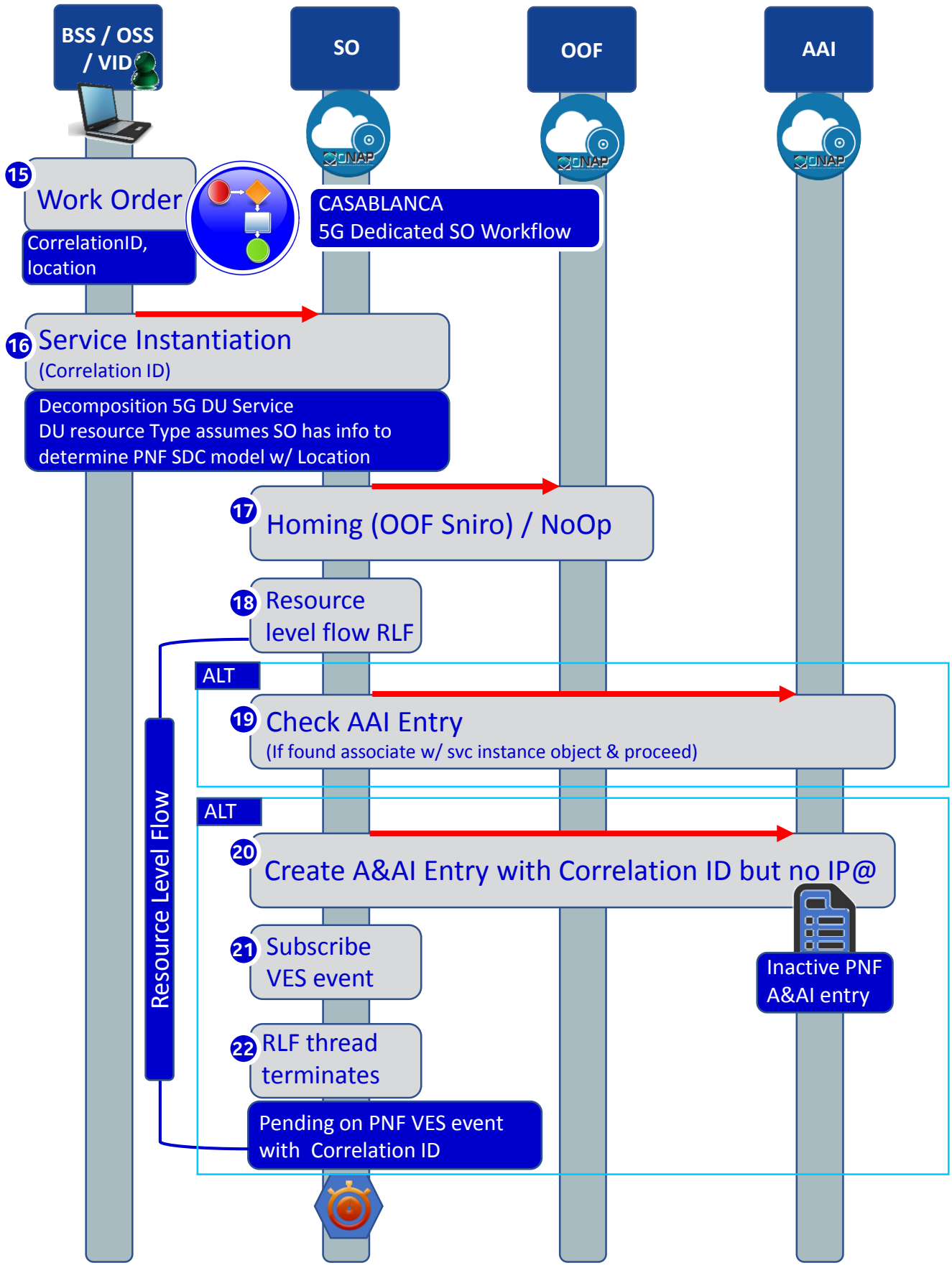
Design Time (ONAP)



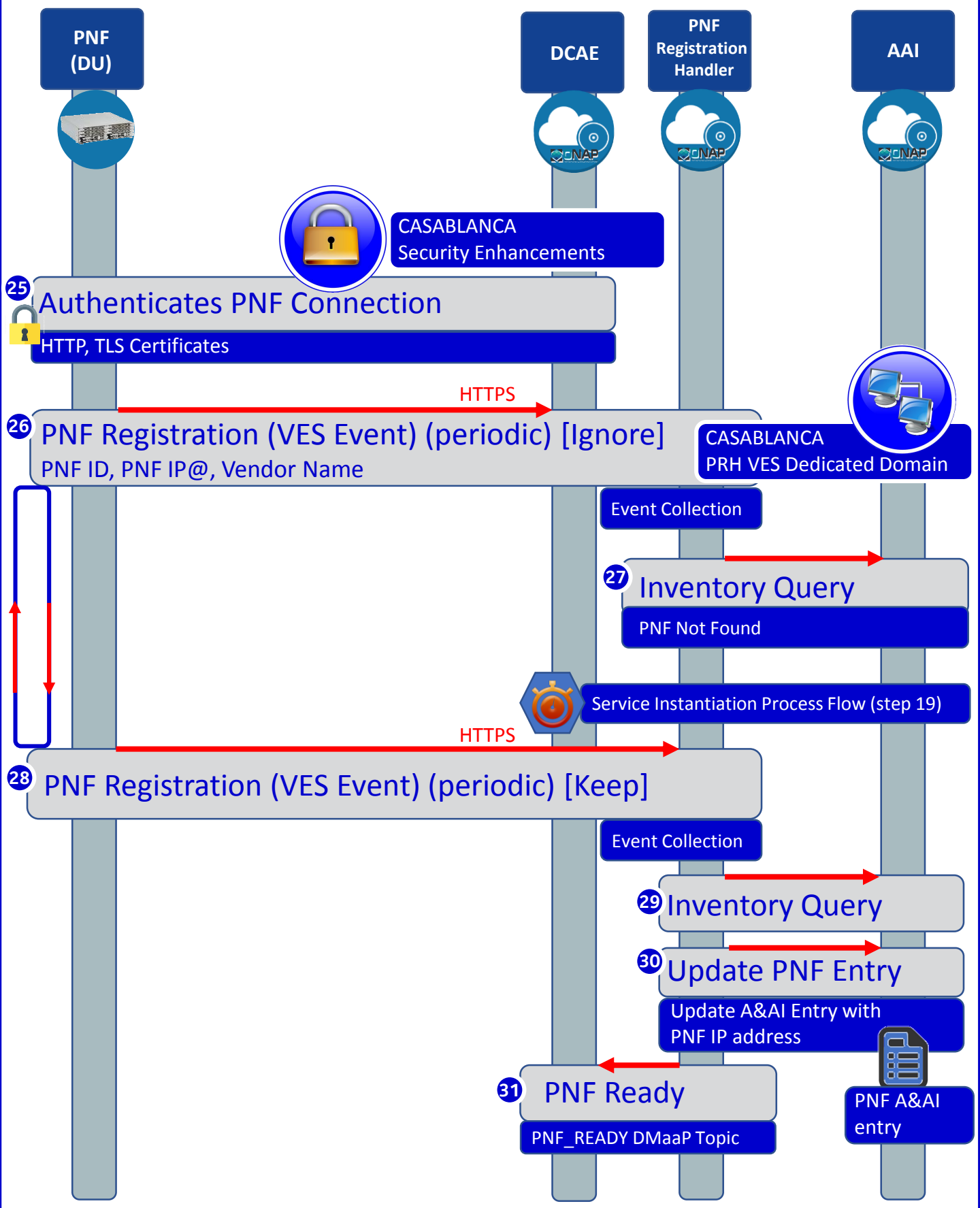
PNF Plug and Play Steps (for 5G DU)



Service Instantiation Process (Part 1)



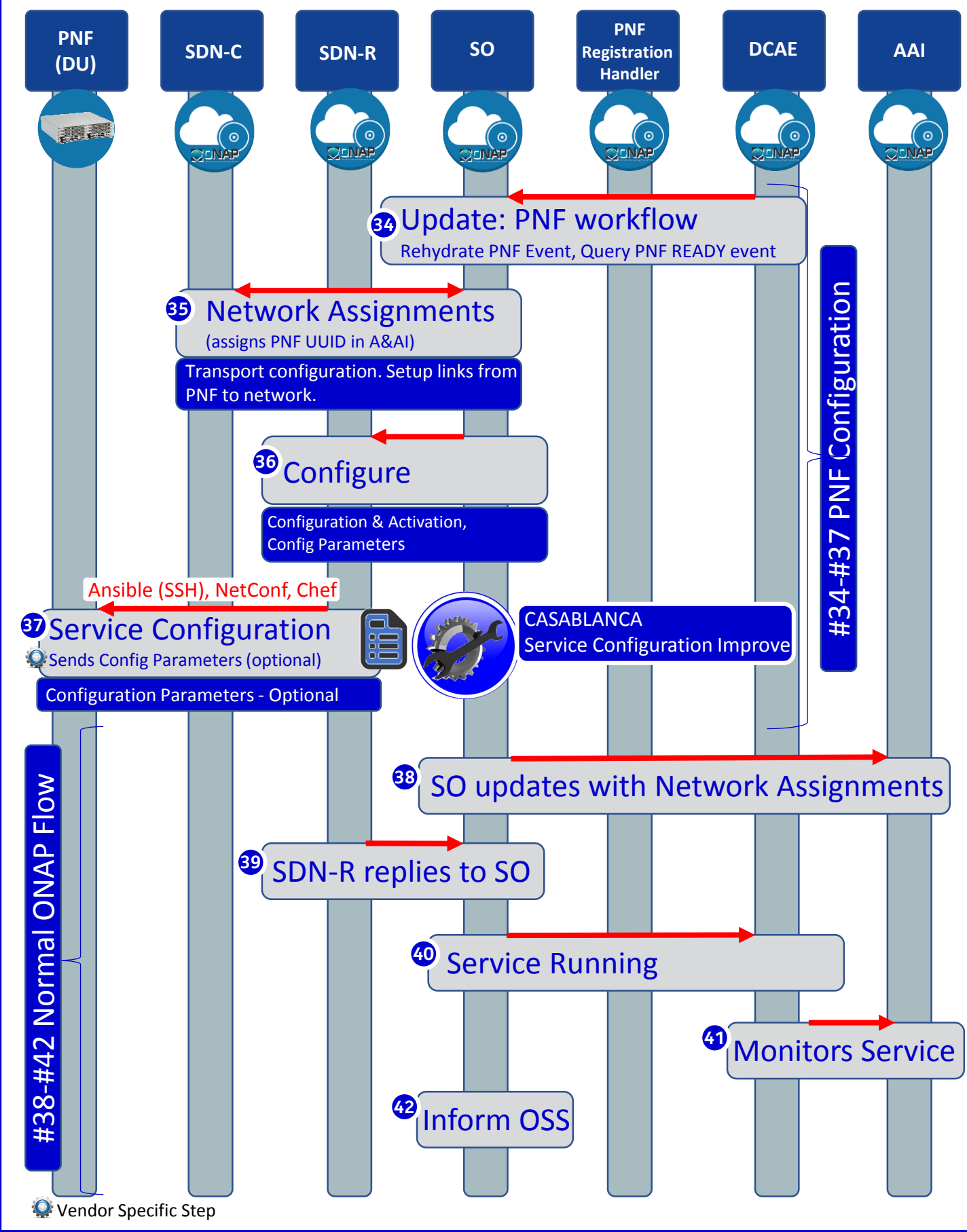
PNF Registration Steps



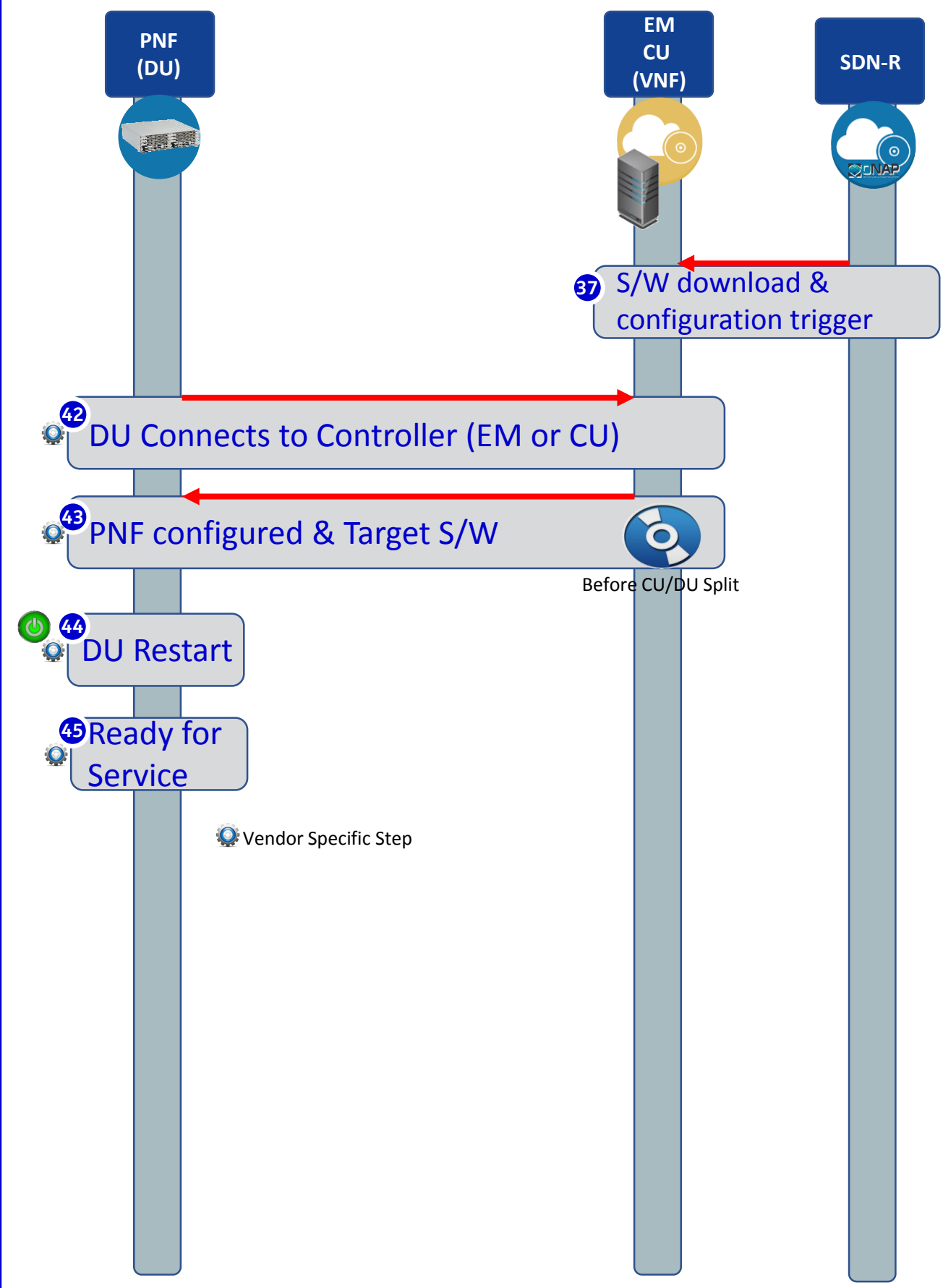
PNF Registration VES Event


```
{   "event": {
      "commonEventHeader": {
        "domain": "pnfRegistration",
        "eventName": "pnfRegistration_5GDU",
          "eventId": "<<SerialNumber>>-reg",
        "eventType": "pnfRegistration",
        "internalHeaderFields": {},
        "lastEpochMicrosec": 1519837825682,
        "nfNamingCode": "5GRAN",
        "nfcNamingCode": "5DU",
        "priority": "Normal",
        "reportingEntityName": "5GRAN_DU",
        "sequence": 0,
        "sourceId": "<<SerialNumber>>",
        "sourceName": "5GRAN_DU",
        "startEpochMicrosec": 1519837825682,
        "version": 1
      },
      "pnfRegistrationFields": {
        "pnfOamAddressList": [
                        {
                                "AddressType": "ipv4",
                                "AddressValue": "10.16.123.234"
                        },
                        {
                                "AddressType": "fqdn",
                                "AdddressValue": "5gdu123456.nj.att.com"
                        ]
                        "pnfVendorName": "Nokia",
                        "pnfFamily": "BBU",
                        "pnfType": "AirScale",
                        "pnfModelNumber": "AJ02",
                        "pnfSerialNumber": "QTFCOC540002E",
                        "pnfSoftwareVersion": "v4.5.0.1",
                        "pnfManufactureDate": 1516406400,
                        "pnfLastServiceDate": 1517206400,
                        "pnfRegistrationFieldsVersion": 1
            }
        }
}
```

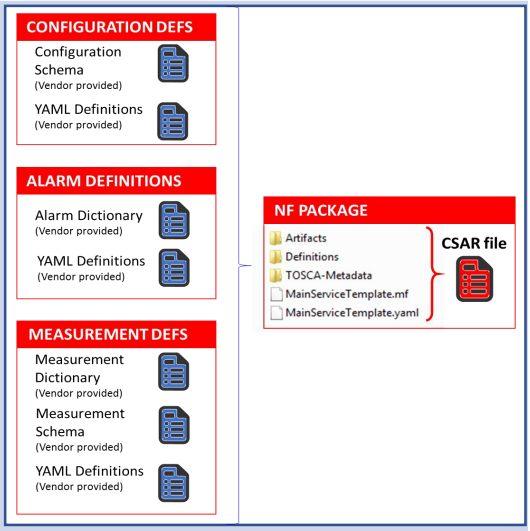
PNF Activation Steps (ONAP)



PNF Final Download & Activation (Vendor Specific)



PNF Vendor Requirements to support PnP

TOPIC	Step	DESCRIPTION
PNF Package Artifacts and Dictionaries	1	NF Vendor needs To provide NF FM, CM, and PM dictionaries and artifacts to be onboarded to the PNF package during design time by SDC. 
PNF Descriptor	1	The “PNF-D” is a descriptor which provides detailed information about their PNF. This is used during design time to model the PNF.
Registration VES Event	26,28	The NF needs to support the new Registration VES Event. The PNF sends this event periodically to ONAP until the PRH finds the PNF AAI entry. The AAI entry is created in the SO Workflow.
Service Configuration	37	Once PRH has successfully found the PNF it can complete the registration process and it will have the ONAP controller send a service configuration message.

ONAP
OPEN NETWORK AUTOMATION PLATFORM

APPENDIX

The complete PnP Use Case Slide Package can be found in the ONAP Wiki:

https://wiki.onap.org/display/DW/Use+case+proposal%3A+5G-+RAN+deployment%2C+Slicing%2C+SON

STEP	DESCRIPTION
1	**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 **PNF RESOURCE Definition** **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. 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.
2	**SERVICE Definition (uses a PNF)** **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 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.
3	**DISTRIBUTION** – Event Monitoring Templates distributed. (?)

STEP	DESCRIPTION (Plug and Play Vendor steps for Infrastructure components)
6	**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. Note: *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).* Note: The user name & password which the PNF needs to know to contact and get through the vAAA server before it contacts ONAP.
7	**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.
8	**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.
9	**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.
10	**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.
11	**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.
12	**IDENTITY SERVICE** – The identity service is there to identify the PNF. It also returns the ONAP (DCAE) IP address.
13	**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
14	**PNF RESET** – The PNF is reset so that the downloaded ONAP Bootstrap software becomes activated and is then ready to continue to PNF registration

Vendor Specific Step

#	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)

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	**PNF DISCOVERY** – 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. Note [FUTURE]: A (new) *"PNF Infrastructure Manager"* 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.
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	**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.
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 DISCOVERY RESPONSE** - The PRH responds to the PNF discovery event of the PNF with a response.

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 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 *optional*. (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.

STEP	DESCRIPTION
42 ⚙	**CONNECTION TO CONTROLLER** – Using the CU IP@ from the previous step, the DU makes contact with the CU. If the CU cannot be reached, the DU shall periodically retry. Note: The CU has already been previously deployed and “plug & play” onboarded procedure before the DU wants to register. This is outside the scope of this use case. Note: After the 3GPP CU/DU split, the signaling interfaces between the gNB CU and DU will be standardized by 3GPP RAN3 (which supports that ability to mix CU and DU PNFs from different vendors).
44 ⚙	**CU CONFIGURES DU** – The configuration information is downloaded 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.
45 ⚙	**DU RESTART** – The PNF (DU) is reset, which allows the new configuration parameters to take hold. And the 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.

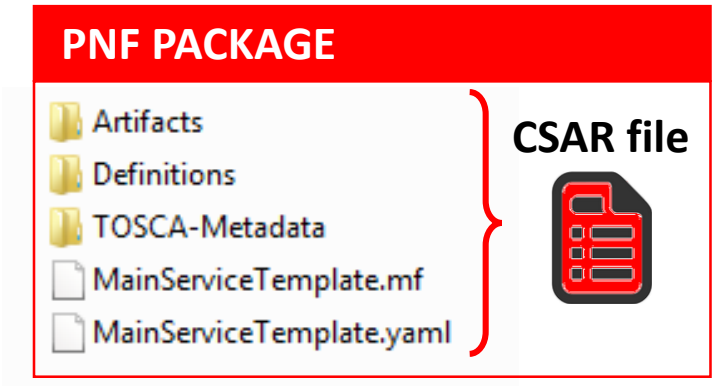
⚙ Vendor Specific Step

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 implements 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 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

ALARM DICTIONARY FIELDS (Template)

ALARM FIELD	DESCRIPTION
Alarm 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.
Alarm Name	Alarm Name which will be used in the Event Name. **Note** *this maps to the alarmCondition in the VES Fault Event in faultevent fields.*
Event Type	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 or Mechanism Violation, or Time Domain Violation. **Note** *this maps to the eventCategtory in the VES Fault Event in faultevent fields.*
Meaning of Alarm	Provides a descriptive meaning of the alarm condition. This is intended to be read by an operator to give an idea of what happened.
Effect of Alarm	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.
Managed Object(s)	Managed object (MO) associated with this Alarm. **Note** *this maps to the eventSourceType in the VES Fault Event in faultevent fields.*
User Label	The "user label" of the object class representing the NE in the Generic Network Resource Model.
Probable Cause	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
Probable Cause Number	Probable Cause Number the numeric value associated with the Probable Cause
Perceived Severity	It indicates the relative level of urgency for operator attention. These are Critical, Major, Minor, Warning, and Cleared, draw from the ITU-T Recommendation X.733. This corresponds to the 3GPP TS32.111 **Note** *this maps to the eventSeverity in the VES Fault Event in faultevent fields.*
Specific Problem	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** *this is the 3GPP Specific problem not be confused with the specificProblem field of the VES Fault Event in faultevent fields.*
Backed Up Status	It indicates if an object (the Monitored Entity) has a back up. Defined in ITU-T Recommendation X.733 clause 8.1.2.4
Threshold Info	It indicates the crossed threshold information of the monitored attribute whose value has crossed a threshold, the threshold settings, or the observed value that have crossed a threshold. Defined in ITU-T Recommendation X.733 clause 8.1.2.7 and also in TS 32.401 sub-clause 5.6.
State Change Definition	This indicates MO attribute value changes. See definition in ITU-T Recommendation X.733 clause 8.1.2.10.
Monitored Attributes	It indicates MO attributes whose value changes are being monitored. See definition in ITU-T Recommendation X.733 clause 8.1.2.11.
Proposed Repair Actions	It indicates instructions for proposed repair actions. These are defined in ITU-T Recommendation X.733 clause 8.1.2.12.
Clearing Type	Indicates whether the alarm is automatically or manually cleared
Additional Text	This field contain further information on the alarm.
Additional Information	This attribute provides *vendor specific* 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.
Associated Fault(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.

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.
Fault Name	Alarm Name which will be used in the Event Name. **Note** *this maps to the alarmCondition in the VES Fault Event in faultevent fields.*
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.
Managed Object(s)	Managed object (MO) associated with this Alarm. **Note** *this maps to the eventSourceType in the VES Fault Event in faultevent fields.*
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.
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.
Proposed Repair Actions	It indicates instructions for proposed repair actions. These are defined in ITU-T Recommendation X.733 clause 8.1.2.12.
Additional Text	This field contain further information on the alarm.
Additional Information	This attribute provides *vendor specific* 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.

SAMPLE YAML FAULT DEFINITION

```
event: {presence: required, action: [ any, up, overTemperature, RECO-rebootPnf, null ],
structure: {
   commonEventHeader: {presence: required, structure: {
         domain: {presence: required, value: fault},
         eventName: {presence: required, value: Fault_Nokia_5GCU_Overtemperature},
         eventId: {presence: required},
         priority: {presence: required},
         reportingEntityName: {presence: required},
         sequence: {presence: required},
         sourceName: {presence: required},
         startEpochMicrosec: {presence: required},
         lastEpochMicrosec: {presence: required},
         version: {presence: required, value: 3.0}
   }},
   faultFields: {presence: required, structure: {
         alarmCondition : {presence: required, value: Overtemperature},
         eventSeverity: {presence: required, value: MAJOR},
         eventSourceType: {presence: required, value: BaseStation},
         faultFieldsVersion: {presence: required, value: 3.0},
         specificProblem: {presence: required},
         vfStatus: {presence: required, value: “Active"}
         alarmInterfaceA : {presence: required},
         additionalInformation: {presence: optional, array: {
         keyValuePair: {presence: required, structure: {
           key: {presence: required, value: Temperature},
           value: {presence: required}
         }
    }}
}}
```

MEASUREMENTS DICTIONARY FIELD

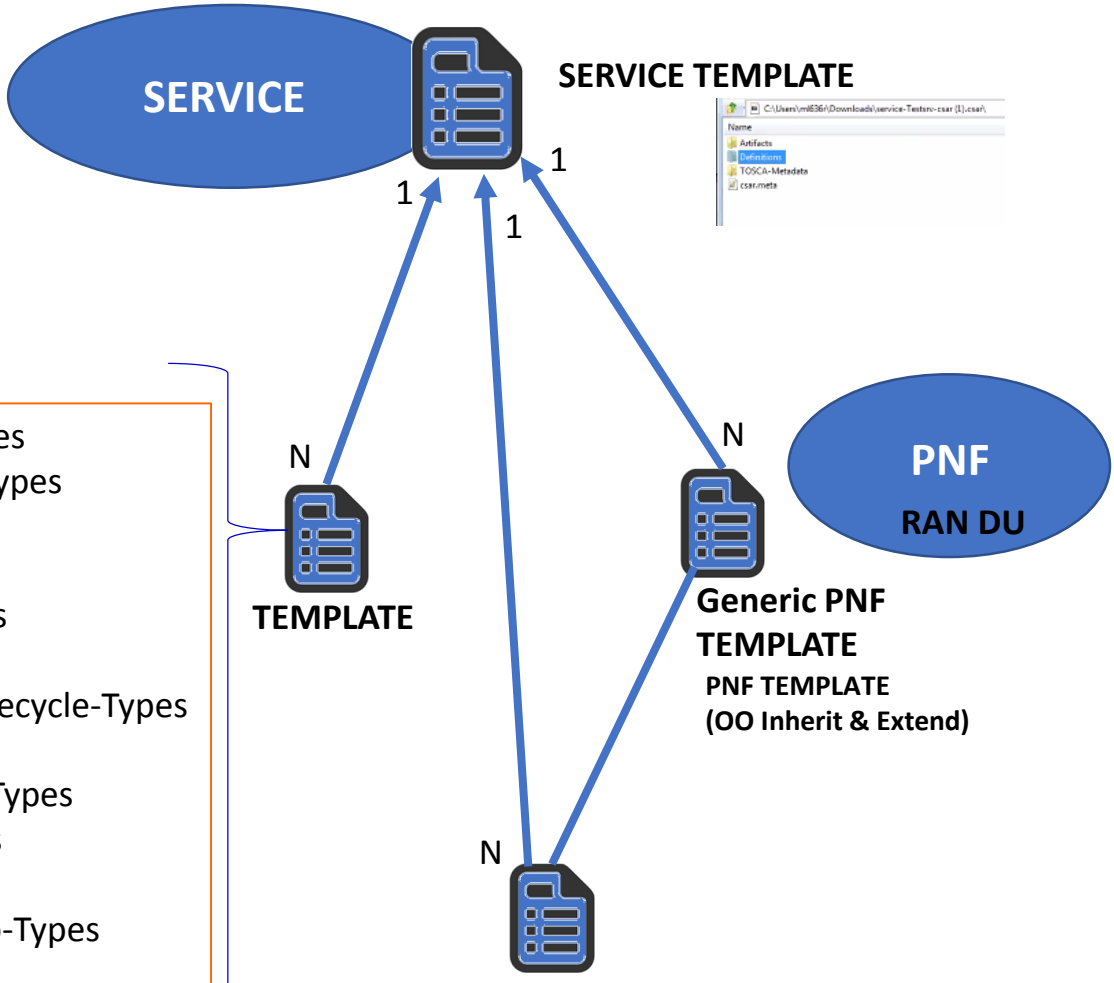
Suggested format is XML

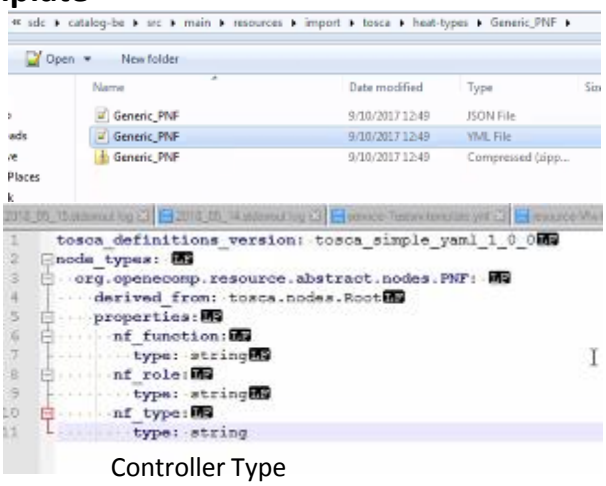
MEASUREMENT FIELDS	
MEASUREMENT FIELD	**DESCRIPTION**
Meas Id	Gives the Identifier for the Measurement.
Meas Type	Meas Type is the Measurement Name in Camel Format
Meas Type 3GPP	Measurement Name in 3GPP Standards defined in 3GPP TS32.425.
Meas Obj Class	Managed object (MO) associated with this Measurement. The objects will be vendor specific and it indicates the NF object for that vendor related to that measurement.
Meas Collection Method	The Collection method for the measurement. Cumulative (CC), Lead, Max, Snapshot, Value
Meas Unit	Unit type for the Measurement. Typical unit values include: watt (power), dB, bits/s (throughput), PRB, Packets, Sequence.
Meas Range	Numerical Value Range for the measurement in the units given by the meas units.
Meas Family	Family or grouping of measurements.
Meas SubFamily	Subgrouping for the measurement.
Meas Description	This field provides a textual description of the measurement. This is intended for an operator to understand the meaning of the measurement.
Meas Condition	Provides the Measure Conditions.
COUNTER FIELDS	
COUNTER FIELD	**DESCRIPTION**
Criteria	Criteria to determine which counter to peg (same for all counters associated with the measurement. If there are no criteria there will also not be counters associated with the meas.
Counter ID	Gives the identifier of the Counter
Counter Name	This is the name of the counter
Counter Description	This field provides a textual description of the counter. This is intended for an operator to understand the meaning of the counter.
Counter Suffix 3GPP	The 3GPP standardized Suffix. The suffix value is defined in the 3GPP TS32.425 standard.
Counter Condition	This field describes the trigger condition that trips the counter. Triggering events are specific exchanges that happen in the flow of call management

ALARM DEFINITIONS

Field	Type	Required ?	Description
alarmAdditional Information	hashMap	No	Additional alarm information (note: for SNMP mapping to VES, for hash key use OID of varbind, for value use incoming data for that varbind)
alarmCondition	string	Yes	Short name of the alarm condition/problem, such as a trap name. Should not have white space (e.g., tpLgCgiNotInConfig, BfdSessionDown, linkDown, etc…)
alarmInterfaceA	string	No	Card, port, channel or interface name of the device generating the alarm
eventCategory	string	No	Event category, for example: 'license', 'link', 'routing', 'security', 'signaling '
eventSeverity	string	Yes	Event severity enumeration: 'CRITICAL', 'MAJOR', 'MINOR', 'WARNING', 'NORMAL '
eventSourceType	string	Yes	Examples: 'card', 'host', 'other', 'port', 'portThreshold', 'router', 'slotThreshold', 'switch', 'virtualMachine', 'virtualNetworkFunction'
faultFieldsVersion	number	Yes	Version of the faultFields block
specificProblem	string	Yes	Description of the alarm or problem (e.g., 'This event is sent when the LG is asked to perform a location for a CGI that is not in its configuration')
vfStatus	string	Yes	Virtual function status enumeration: 'Active', 'Idle', 'Preparing to terminate ', 'Ready to terminate', 'Requesting Termination'

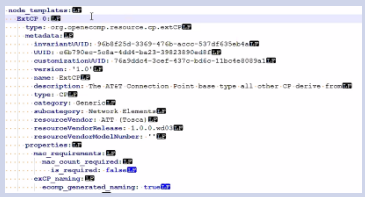
SDC MODELING (Design Time)





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

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.

- **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

From Potential PNF template for PNF S/W management & change mgmt. (Lixiang,YaoguangWang, ChangMing Bai Hwawei)

ACTIVE INVENTORY (A&AI) IMPACTS

ACTIVE & AVAILABLE INVENTORY (A&AI) PROJECT IMPACTS	
New A&AI PNF Parameters	**PNF GEOLOCATION** - provides information about the geographical location (e.g. geographic coordinates or address of the building, etc.) of the PNF. Latitude/Longitude
Software Version	**DETECTED SOFTWARE PNF VERSION(S) –** during Run-Time when the PNF registers with ONAP it can report its (list) of PNF Software that is currently has installed. And this could be kept track of in the A&AI entry for that PNF. Entry will also have *Active/Passive* • **Content of PNF software version List** **Contents** / **Description** **softwareList** – **description**: Describes the main feature of the this software version **softwareList** – **swVersion**: Software version
	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]

PNF A&AI ENTRY (From Beijing)

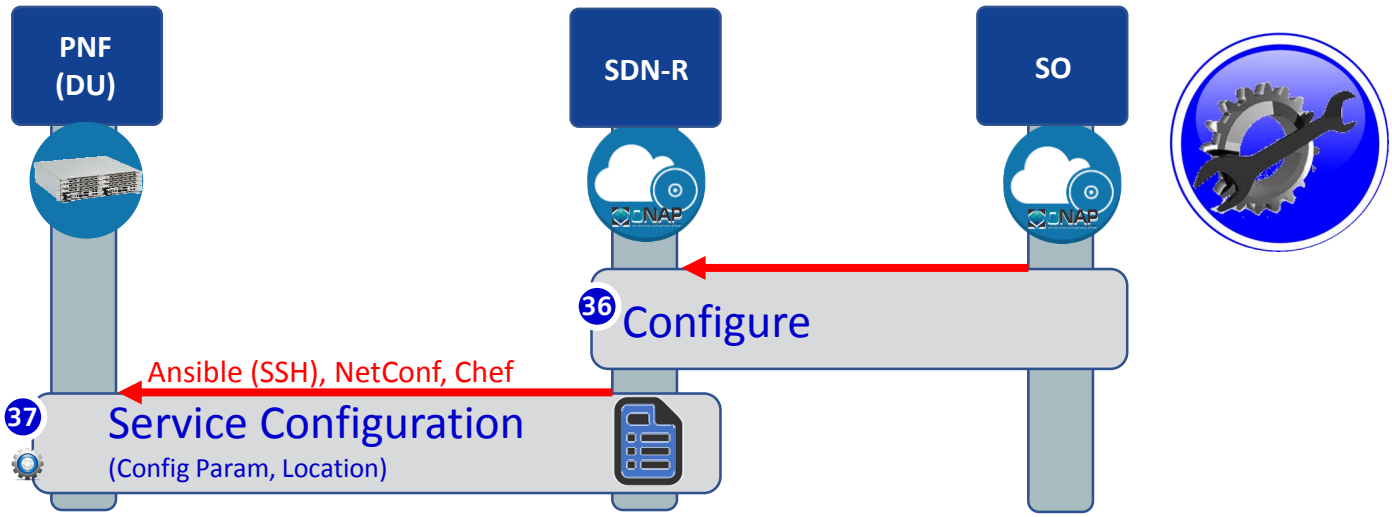
Register PNF Service – may need new registration information in AAA

• PNF has a "*pnf-name*" = Key in AAI. Could change it to the ID. E.g. "Name" = "abcd""ID#""#Code" (automated, NF naming code); *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. ; (FYI/ *ipaddress-v4-loopback-0*).

mac-address & *serial-number,*

PNF:: proxy IP address

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	(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 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 *optional*. (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)** – The expected PNF Software Version(s).

Vendor Specific Step

SDN-R w/ PnP in R3

SDN-R FUNCTIONS	DESCRIPTION
PROTOCOL SPECIFIED	PNF onboarding package defines of PNF (protocol). PNF info model (SDC) will have (1) protocol (2) controller: **(1)** **Protocols Supported** – PNF package. CM Protocol is in PNF onboarding package. **(2)** **Controller type** – defined in design time. Controller type is specified in design time. Design time designer specifies which controller is used. Distributed in PNF Modeling artifacts
MODEL DRIVEN DESIGN	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.
VENDOR SPECIFIC ADAPTOR	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.
UPDATING PNF & CONTROLLER RELATION INFO	Updating the controller/protocol (“lifecycle management”).
ERROR LEGS (ERROR FLOWS)	Errors when SDN-R interacts w/ a PNF

Vendor Specific Step