ONAP PNF Plug and Play

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

Mar 16, 2018 version 16

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

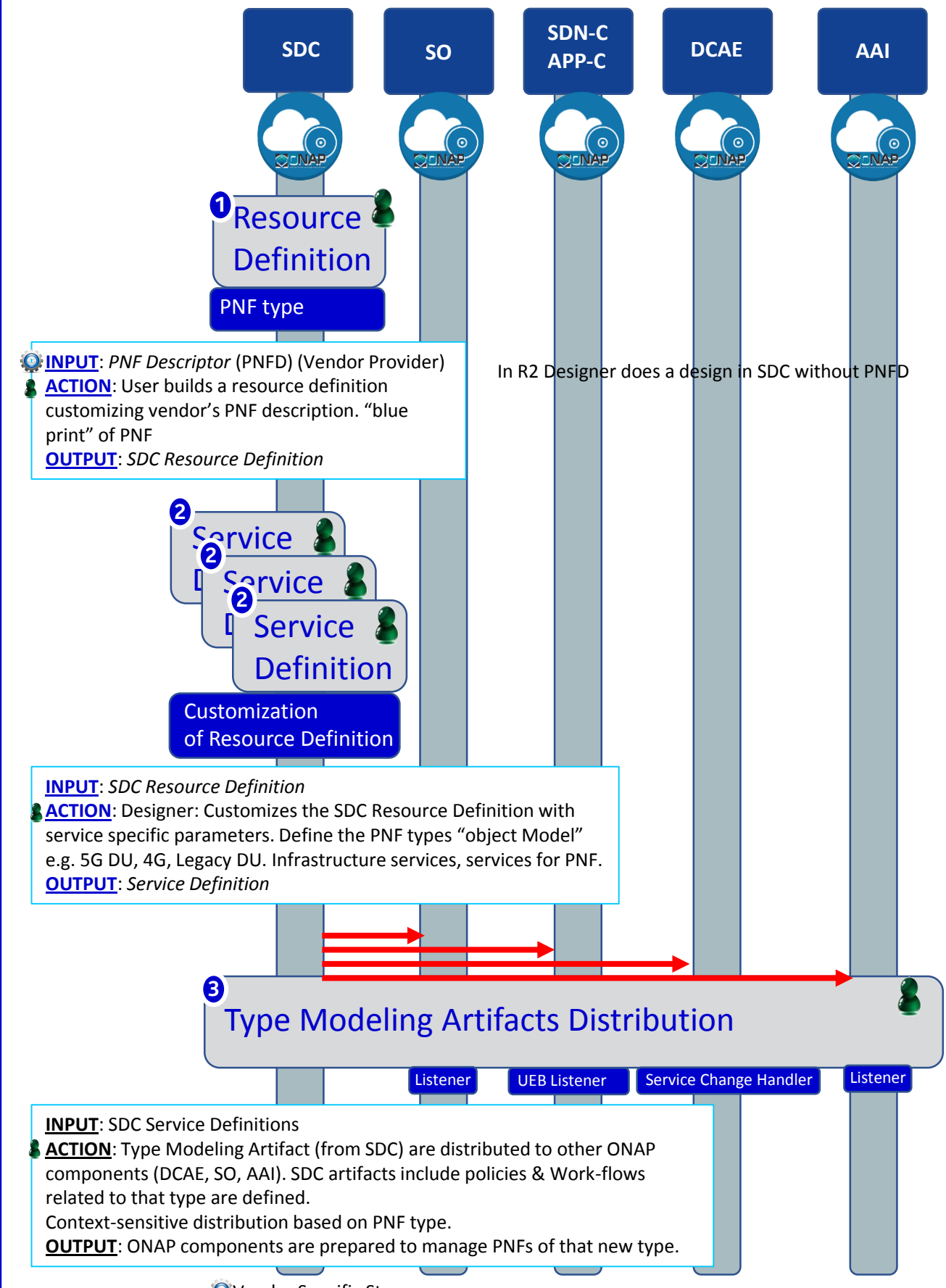
Generic (not vendor proprietary)

E **PNF Activation**

Connection points configured
Second part of PNF service instantiation
Software is downloaded to PNF.
PNF configured and ready to provide service

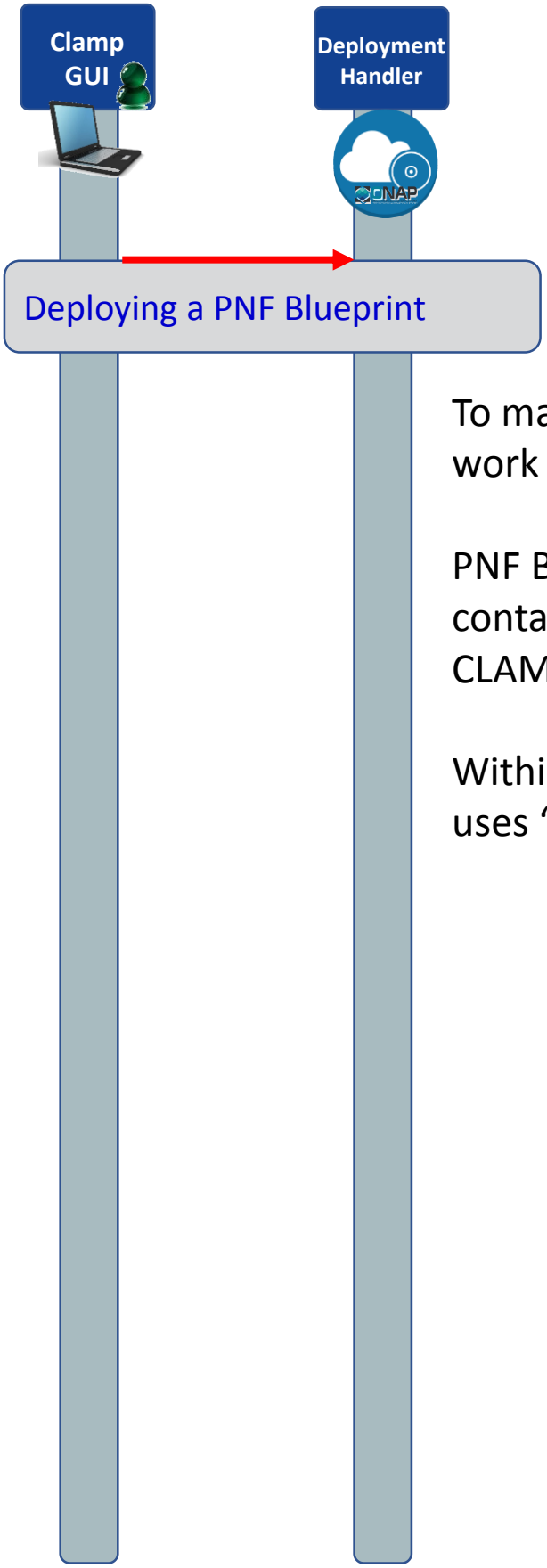
ACTORS	DESCRIPTION
PNF	**PHYSICAL NETWORK FUNCTION (PNF)** – The Distributed Unit (DU) or Network Hardware device that provides service to an end-user.
DHCP	**DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP)** – Protocol to assign IP addresses to a network element (NE). The IP address can be dynamically assigned 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.
vDHCP	**vDHCP** – An entity that exists outside of ONAP, it can assign and manage IP Addresses. Defined in the vCPE Use Case.
vAAA	**vAAA (AUTHENTICATION, AUTHORIZATION, ACCOUNTING)** – Authentication for a PNF to controlling access to the system, enforcing policies, auditing usage. An entity that exists outside of ONAP; defined in the vCPE Use Case.
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** – is a Micro-Service used during the PNF Plug and Play process to receive and process the DMaaP topic (for the PNF VES event)

Design Time


SDC
SO
SDN-C
APP-C
DCAE
AAI
1 Resource Definition
PNF type
INPUT: PNF Descriptor (PNFD) (Vendor Provider)
ACTION: User builds a resource definition customizing vendor's PNF description. "blue print" of PNF
OUTPUT: SDC Resource Definition
In R2 Designer does a design in SDC without PNFD
2 Service Definition
Customization of Resource Definition
INPUT: SDC Resource Definition
ACTION: Designer: Customizes the SDC Resource Definition with service specific parameters. Define the PNF types "object Model" e.g. 5G DU, 4G, Legacy DU. Infrastructure services, services for PNF.
OUTPUT: Service Definition
3 Type Modeling Artifacts Distribution
Listener
UEB Listener
Service Change Handler
Listener
INPUT: SDC Service Definitions
ACTION: Type Modeling Artifact (from SDC) are distributed to other ONAP components (DCAE, SO, AAI). SDC artifacts include policies & Work-flows related to that type are defined.
Context-sensitive distribution based on PNF type.
OUTPUT: ONAP components are prepared to manage PNFs of that new type.
Vendor Specific Step

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	**PNF SERVICE Definition** **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. (?)

Deployment Handler (VES Collector)



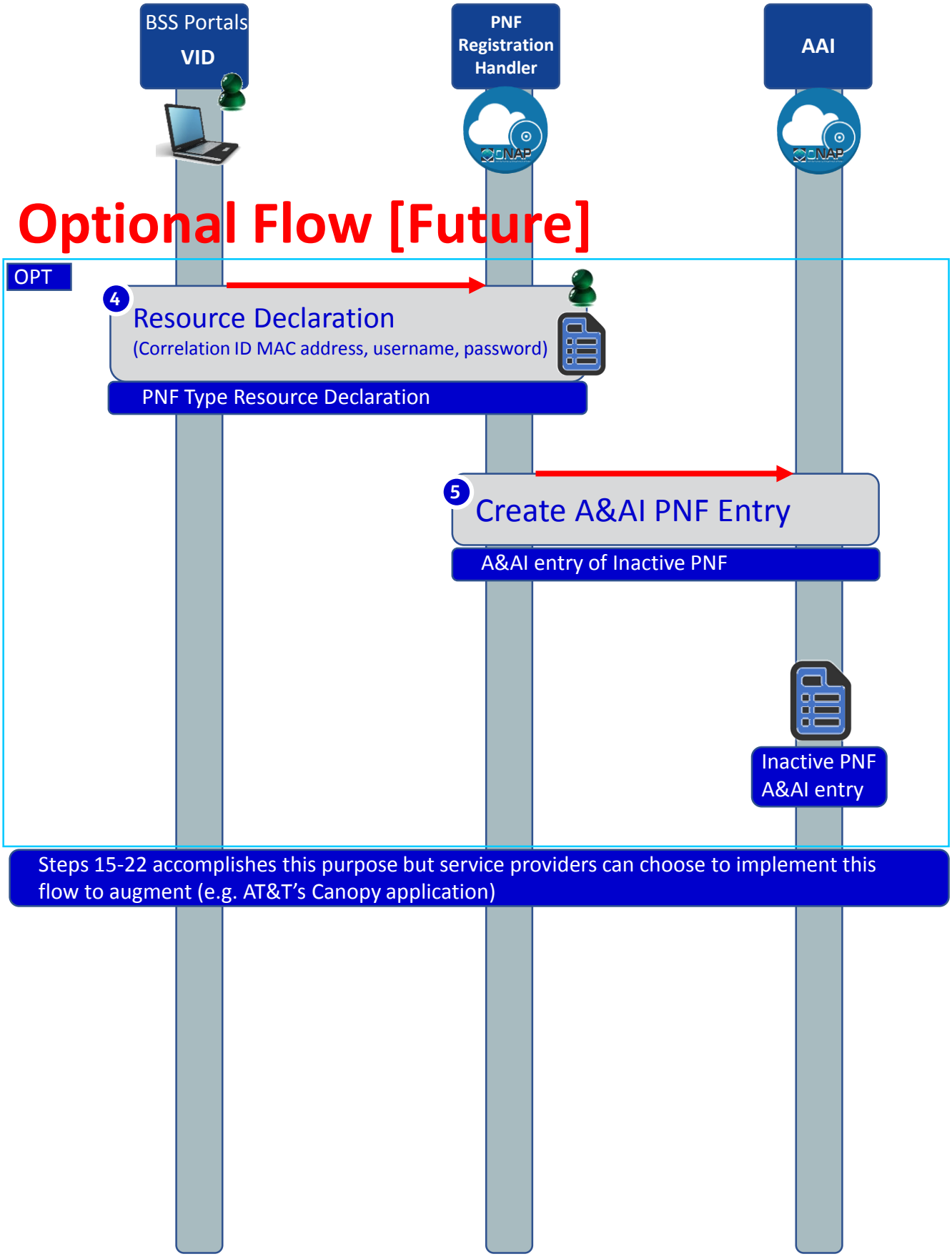
To make a VES Collector in DCAE work properly

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

Within VES Collector schema uses “Adder” (existing)

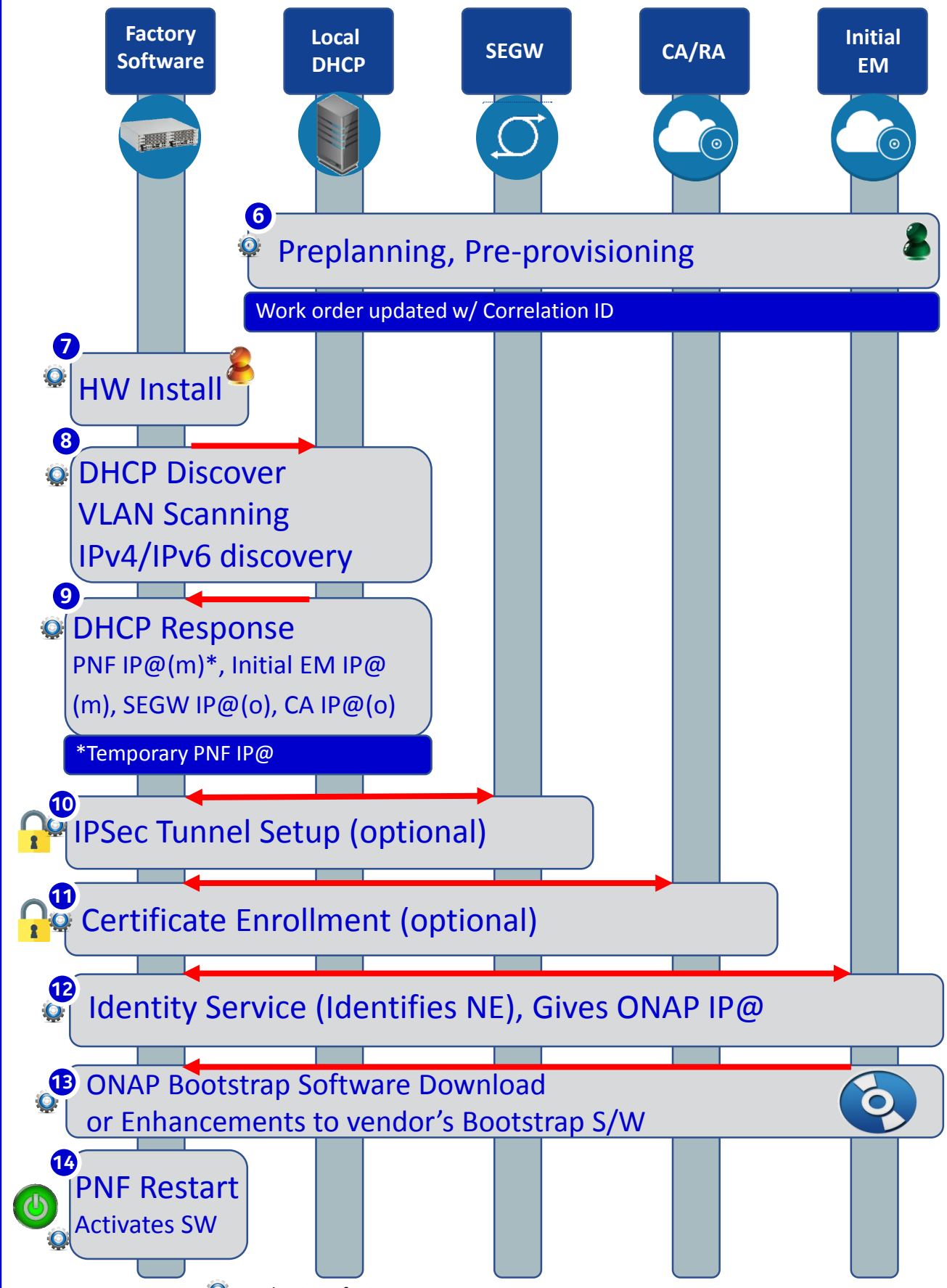
STEP	DESCRIPTION
1	**DEPLOYMENT HANDLER PNF BLUEPRINT** – The Deployment handler is necessary to use, to give it the PNF blueprint so that later on in the Plug and Play flow, DCAE will recognize the PNF. The PNF Blueprint will be docker container. The PNF blueprint May be deployed from CLAMP or Cloudify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

PNF Resource Declaration (future)



STEP	DESCRIPTION
4	**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. .
5	**PNF Registration Handler (PRH) creates an A&AI Entry:** 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.

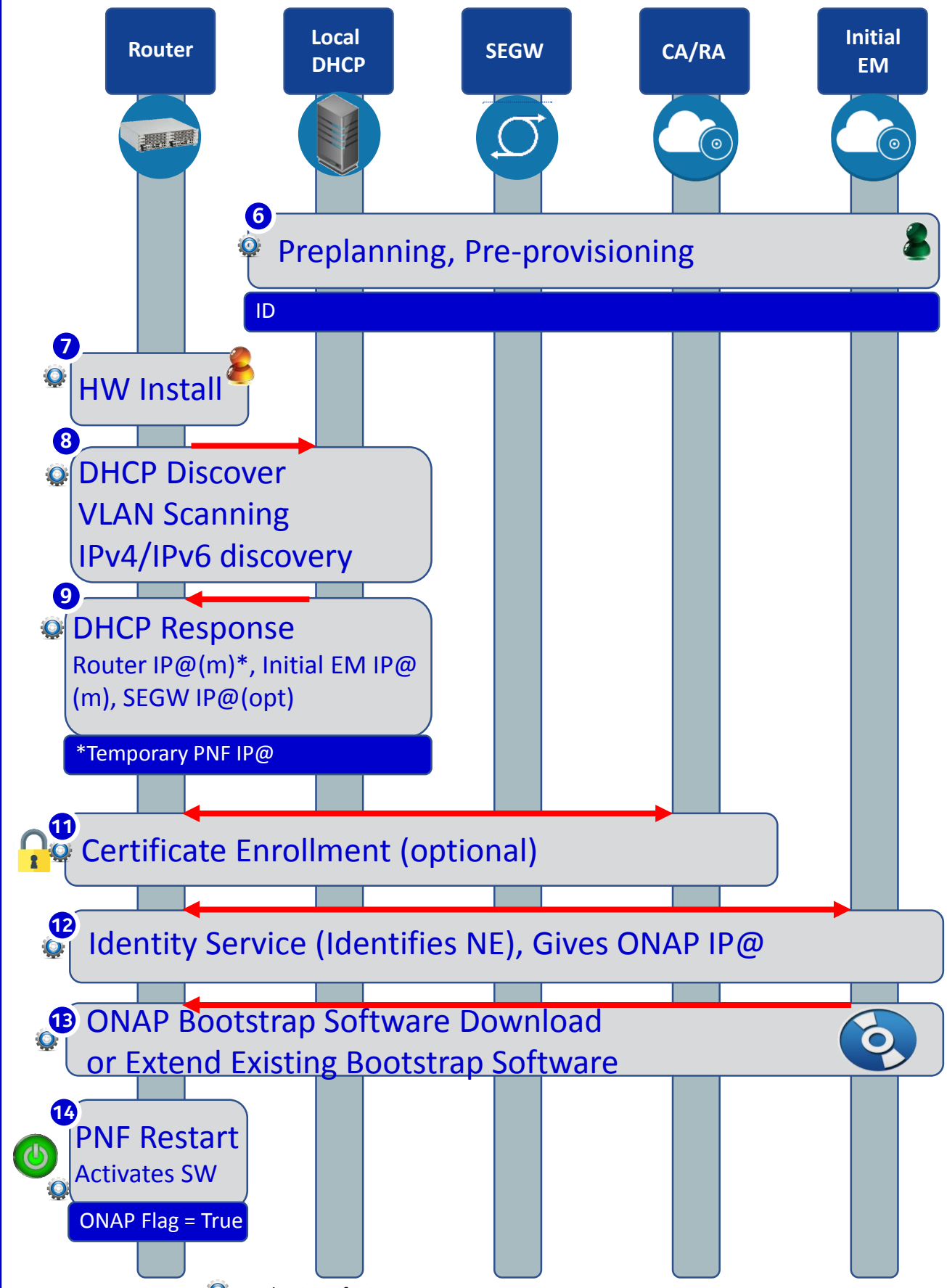
PNF Plug and Play Steps (for 5G DU)



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 BOOTSTRAP 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

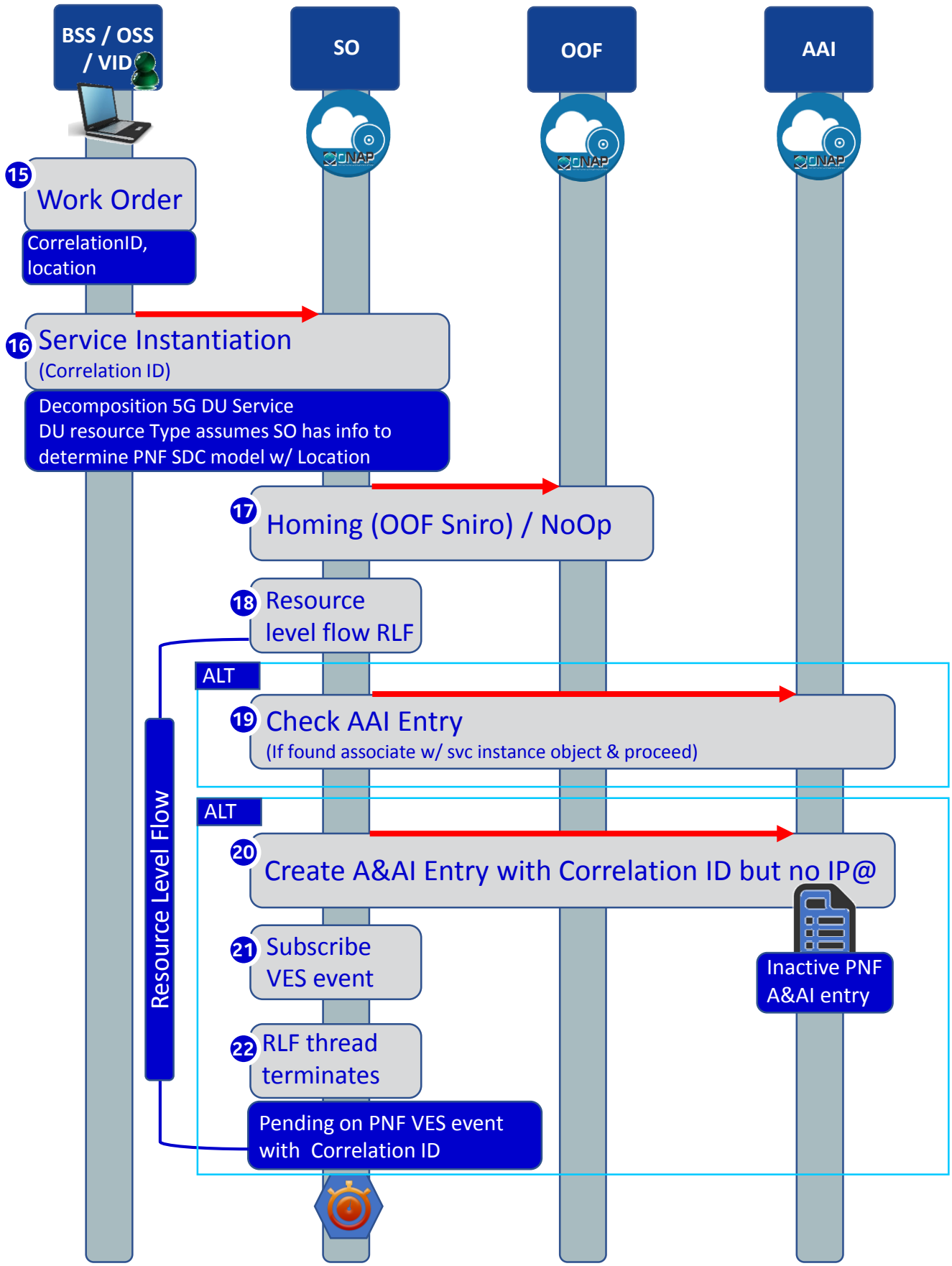
PNF Bootstrapping Steps (for Routers)



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.
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 BOOTSTRAP 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

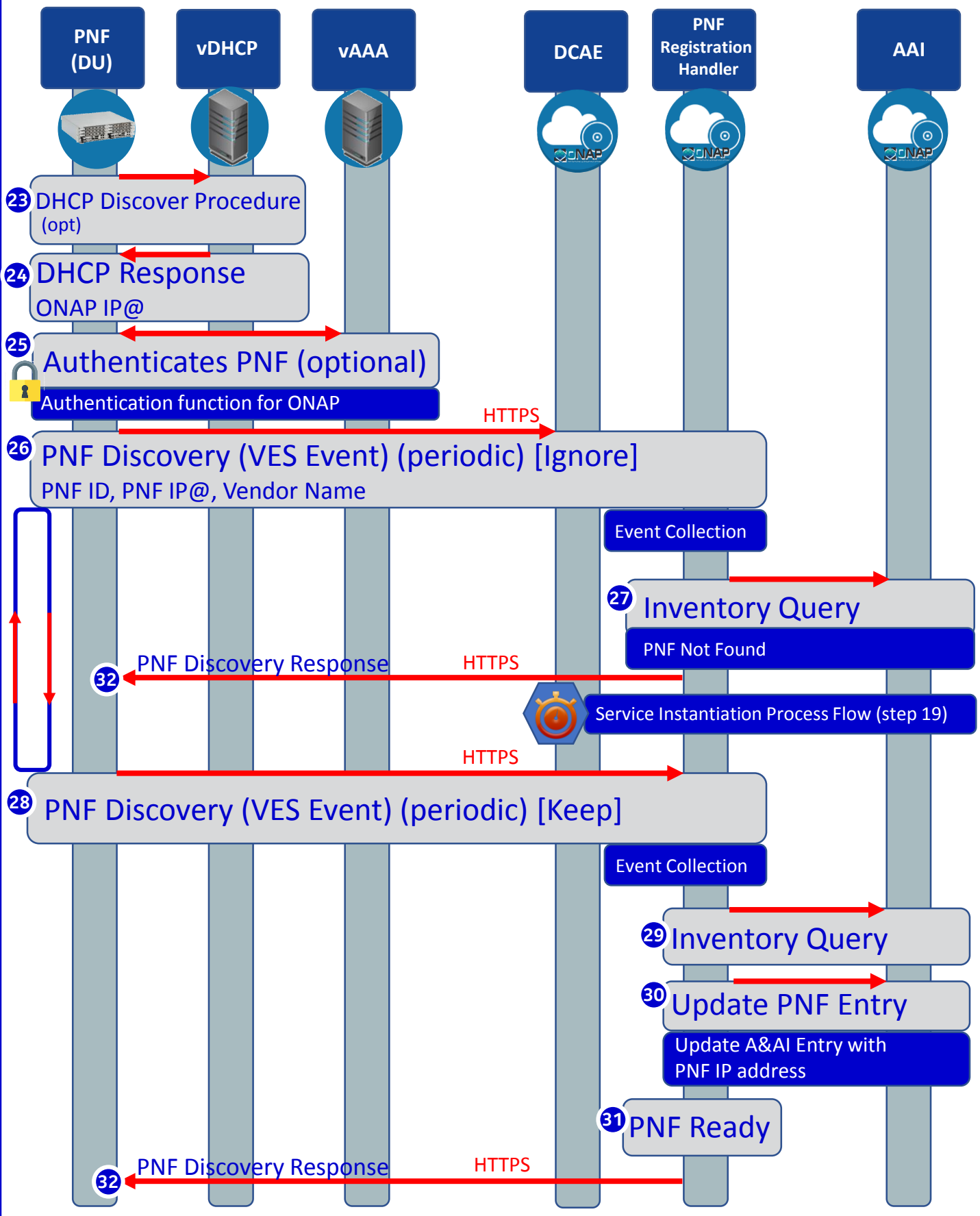
Vendor Specific Step

Service Instantiation Process (Part 1)



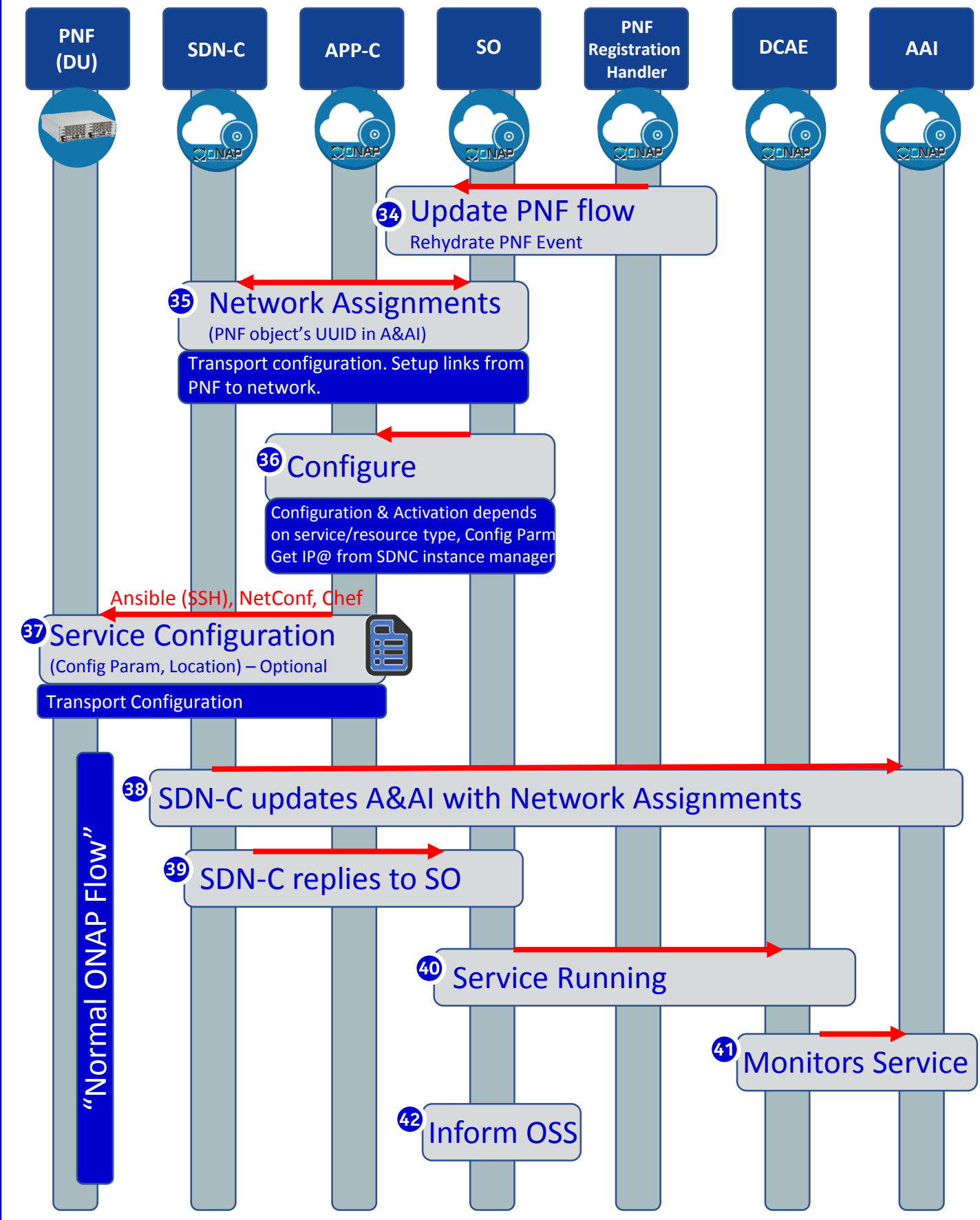
#	DESCRIPTION
15	**WORK ORDER** – The work order (AT&T work order process) determines which PNF to use for this Service/work order. BSS is told the correlation ID. Typically, the PNF will be known before the PNF comes on-line. Orchestrated with a equipment order (to vendor) and location value for the 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



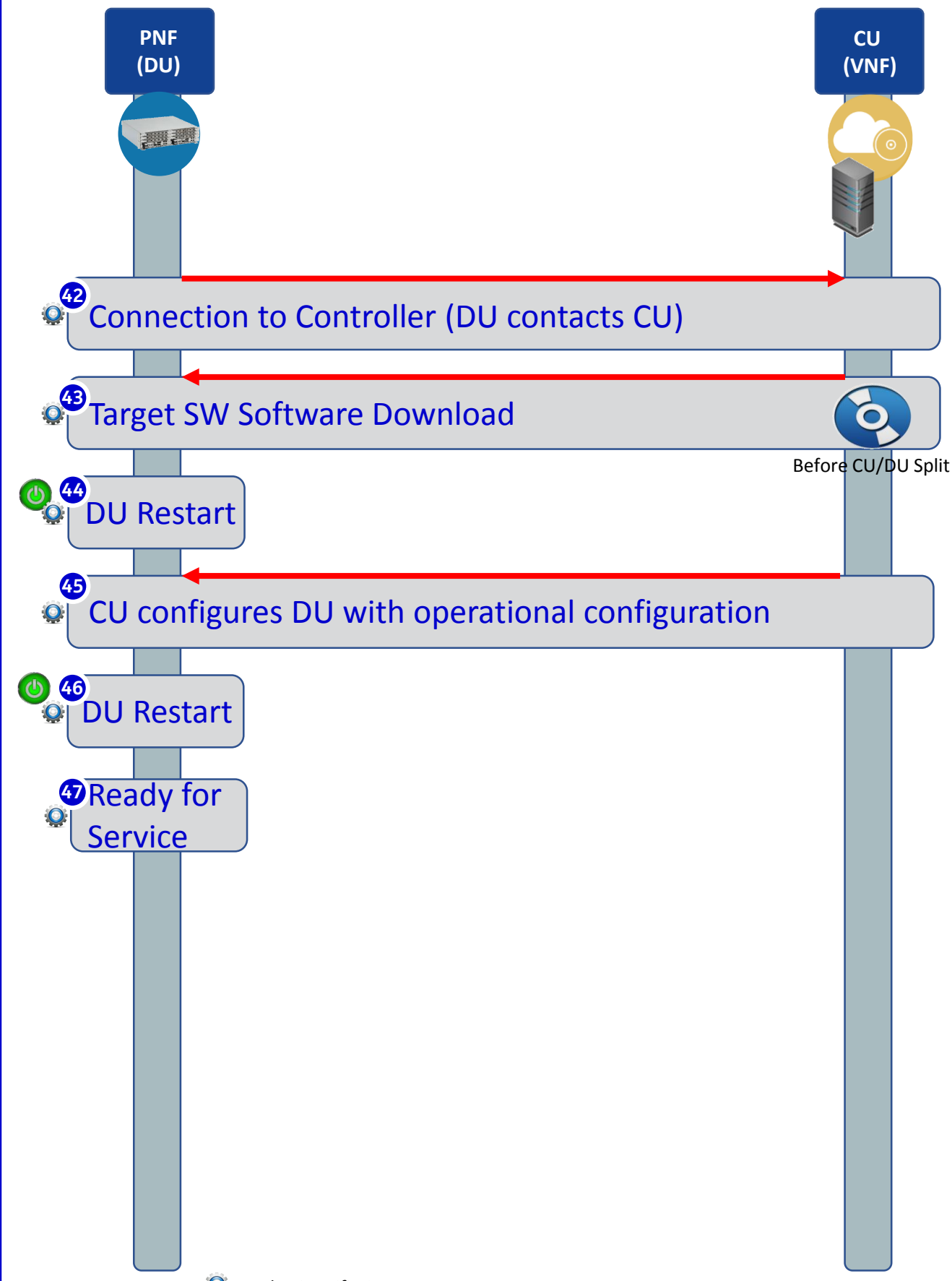
STEP	DESCRIPTION
23	**DHCP Request** –ONAP Onboarding S/W performs a DHCP procedure with vDHCP
24	**DHCP Response** – DHCP response returns a ONAP IP address
25	**Authenticate PNF** – The PNF is authenticated through a vAAA.
26 & 28	**PNF DISCOVERY** – The PNF periodically generates a REST Event (json 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 bootstrapping software. The PNF must natively support or have an adapter to be ONAP capable. Note: The *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** - PIM 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.

PNF Activation Steps (ONAP)



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 SO. 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 (mandatory)** - VF-C/APP-C gives the Controller IP@ to the DU. In R2 for the 5G DU, this will also give a configuration parameter (e.g. CU IP@) which will allow the DU to contact the CU to be configured for service. Eventually when the DU is managed directly from ONAP, this would be the APP-C, SDN-C or VF-C IP@ as appropriate. (2) **OAM IP@ (optional)** - The permanent OAM IP address is given to the PNF. The PNF would receive this IP address and use it. 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** – the Location configuration is given to the PNF. 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

PNF Final Download & Activation (Vendor Specific)



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).
43 ⚙	**TARGET SOFTWARE DOWNLOAD** - The new Target Software is downloaded which is the RAN specific software that will replace the ONAP Bootstrap software.
44 ⚙	**DU RESTART** –After the software successfully reboots, the Target Software becomes activated, and the PNF truly becomes a 5G DU (Distributed Unit).
45 ⚙	**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.
46 ⚙	**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 / Plug and Play	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.
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

PNF Plug and Play Projects Impacts

ONAP Project	IMPACT
Modeling, SDC, VNF-SDK	• (Existing: No Impact) **PNF Update** (if user wants to define a new version of the PNF, w/ additional artifacts, modeled as a wholly new [x] or update [x])
ONAP Controller	• Provide Configuration Parm (CU IP@) to PNF as part of Service Instantiation • Determine the ONAP Controller
VNF Requirements	• **REQUIREMENTS** - Expand VNF requirements to add PNF requirements needed for this use case.
OOF	• (No Impact)
DCAE	• (Step 27 & 31) **SUBSCRIBE** - Subscribe to new PNF Discovery VES event and publish new PNF Discovery DMaaP event • **No Impact**
VID	~~• (Step 19) Create A&AI Entry via VID (removed).~~ **WORK ORDER (CONFIGURATION & DATA ENTRY)** - • (Step 15) How does a user enter parameters (ID, location, config parameters)? What Does technician at step 15 expected to input?
Next Steps	Jira Tasks Functional requirements for each Project Update the ONAP Wiki Pages

PNF REGISTRATION HANDLER IMPACTS

PNF Registration Handler (PRH) Project Impacts	
PNF REGISTRATION HANDLER	• (Steps 27-34 New Plugin/Microservice): PRH is *new DCAE microservice* "plug-in" to be implemented. PRH Developed by Nokia MN (Mobile Networks) ONAP team w/ Lusheng Ji (**1**) **COLLECT PNF REGISTRATION EVENTS** (step 26, 30) - from a PNF sending PNF discovery registration event. [ALT] corruptions in event message. (error handling). PNF directly sends to PRH (without a DMaaP topic). In the future different kinds of PNFs would be supported. PNF Ready (publish event). (**2**) **UPDATE A&AI** – Call A&AI API to query A&AI entry and update the entry. [ALT] A&AI rejects (error handling). The PRH will directly use the A&AI API. (**3**) **CALL SO** - Call "Update PNF Flow" in SO.
PNF to PRH MESSAGING	(**1**) **GET MESSAGE FROM PNF to PRH (step 26, 30)** – *DCAE VES Collector processes messages with valid user name & password (before PNF instance is known). User Name & Password is given for a PNF type. PNF sends VES event with "other" type to a DCAE collector. VES Collector analyzes message & assigns it to a DMaaP topic. PRH subscribe to the topic. VES collector consumes messages from PNF. PRH assigns IP@ in A&AI. Publish another event in Kafka Topic trigger event in SO.* ~~Expecting message to come directly from PNF, Will directly get the message (not using DMaaP) – might come through load-balancer. will know that IP address w/ this MAC-address is approved from PNF. When the PNF contacts PRH it is assumed to be ok (because it is assumed to be pre-authenticated). It was allowed to go to the DHCP server because vetting of vAAA. HTTPS. TLS. LDAP authenticates. "Modern" discovery event mechanism is NetConf. Zero-touch defined for Discovery.~~
DEPLOYING PRH SERVICE IN DCAE PLATFORM	- REST server packaged in Container. Cloudify orchestrator deploys containers. Yaml file defines Ports exports I/Fs. Dcae.gen2/platform/blueprints (yaml examples, VES collector). (Should be a "standard" deployment of a service onto DCAE platform).
DCAE PROJECT PLANNING & INTEGRATION	– Because the PRH is a DCAE sub-project. Integrate & Deploy; Project management aspect DCAE Deployment plan. Wrap in container. Plan to address how to scale requirements from description. Stateless. (DCAE meeting on Feb 15, 2018). - Need new Repository. - [Mar 22, 2018] SDC w/ Modelling, Need SDC blueprint derived from TOSCA model. Onboarding a new Microservice. Go to DCAE designer & build it. R2: Kubernetes > Provide component specification > TOSCA lab > Blueprint template. R2: Hand-craft blueprints. SDC design studio to design w/ manual adjustment. (1) need static Blueprint then DCAE can deploy. Run-time blueprint within DCAE (2) add PRH into SDC catalog. - *DMaaP and AAF integration.*

ACTIVE INVENTORY (A&AI) IMPACTS

ACTIVE & AVAILABLE INVENTORY (A&AI) PROJECT IMPACTS	
INSTANTIATION	• Register PNF Service – may need new registration information in AAA • (Step 20an Instance 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)
ADDRESS UPDATE	(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*).
CORRELATION ID (Open Point)	- what is a correlation-id (?) Needs to be a Unique key. People have suggested PNF ID; A&AI team suggests "pnf-name" others suggested a composite CorrelationID (based on Vendor ID & a unique ID). Note: MAC address and serial number are not unique (only unique within a vendor).
QUERY	(Step 27) A&AI query exists. (no new development) PNF?=PNFID
Add PNF SERVICE FIELDS	*mac-address* & *serial-number,*
	PNF:: proxy IP address

SDN-C and DCAE IMPACTS

SDN-C PROJECT IMPACTS	
NETWORK ASSIGNMENTS	(Step 35) - Assignments for PNF and update AAI. (**1**) Pre-load data (**2**) DHCP used. In TOSCA model specify if DHCP methodology is used. SDN-C knows DHCP will assign. Ent IP@ manager.
SO to SDN-C API for PNF	(Step 35)– what API for transport configuration? Need API or API adaptations will be needed for SDNC (no appropriate API for PNF configuration).
GENERIC RESOURCE API	– Message Extensions { 1…6 – VF-module activate (can reused), Assign, Configure, Deactivate } (1) *Assign* (Generic Resource API) – Try to reuse Generic Resource API for assign with parametric updates to adapt from VNF usage to PNF. SO queries SDN-C for network assignments. What does it return? Return null. *In release 2 we expect PNF IP@ will have already been assigned (and thus the assign query will return null; SO will gracefully accept as valid response*)

APP-C IMPACTS

APP-C PROJECT IMPACTS	
Service Configuration (Open Point) 	(**Step 37**)– How will to send Configuration data (configuration information e.g. CU IP@) to PNF. When send PNF ID (Correlation ID) send configuration data. This will be sent via Ansible. Chef. Could be dependent on PNF. Eventually need to support multiple protocols. Beijing Release Solution: Hardcode the Configuration Data (e.g. CU IP@). Configure action w/ PNF ID. PNF-Type (in SDC then **CDT** uses the same PNF-Type). "Generic flow"; model-driven work-flow; For designer to particular from this PNF this is this data that needs to be sent for this protocol. **CDT** Tool in APP-C. http://onap.readthedocs.io/en/latest/submodules/appc.git/docs/APPC%20LCM%20API%20Guide/APPC%20LCM%20API%20Guide.html [March 1, 2018] from APP-C doesn't care if PNF/VNF same APIs & Same definitions, transparent w/ APP-C. Randa Maher. - (1) Need to create a configuration template (via CDT). - (2) Which protocol to use. NetConf/ Ansible/Chef.  - (3) ONAP interfaces w/ APP-C, VID? - (4) Showcasing: ONAP emulator BLG (vCPE Amsterdam use case) supports NetConf. Or upgrade BLG (add Ansible support) open-source. CDT can create a template that specifies NetConf; APP-C establishes the NetConf connection. QUESTION: Is yang model need to be deployed into APP-C for NetConf to work? NetConf mode where APPC connects to PNF called "Mounting of the Model' ask PNF to give model dynamically to APPC, then APPC mounts into open daylight then talk to PNF , for that to happen, the PNF needs to support its dynamic mounting to APP-C (Arash Hekmat). CDT today supports RESTConf (doesn't require YANG Model) JSON payload.

SERVICE ORCHESTRATOR (SO) IMPACTS

SERVICE ORCHESTRATOR (SO) PROJECT IMPACTS	
SERVICE INSTANTIATION (PART 1)	• Service Instantiation for services on PNFs; implement PNF specific behavior • (New Steps 15-19)– Alternative steps
HOMING/SO & OOF	• (Step 15-17)– SO will add S/W to skip this step. In the [FUTURE] PNF homing may be needed. Interaction between SO & OOF
A&AI ENTRY CREATE	• (Step 20)– "*SO will check & create the A&AI entry*".
SO UPDATE PNF FLOW (Open Point)	 • (Step 34)– PIM notifies SO. SO Subscribe to new PNF Ready DMaaP event. "life long" event (SO gets call from "create instance") for Beijing use "life long" event. User (or PIM) triggers (a new SO instantiation). (?)(Open Point) New interface for "Update PNF Flow" (Seshu to check if can be done).
GENERIC RESOURCE API	• (Step 35)– • **ASSIGN** – S/W change for SO to receive Generic Resource API queries SDN-C for network assignments. When null return SO will accept and proceed. SO can add code to "skip" the SDN-C assign step (as we expect it to have returned "null" anyway).
ACTIVATE (SO -> SDN-C)	• (Step 36) - current flow; for Configuration & Assigning of resources. SDNC w/ A&AI w/ update information. If SDN-C can do this step we proceed that way; otherwise SO puts in the DMaaP hook for APP-C. We expect Step 35 & 36 to happen in one "step" in Beijing Release. L1-L3 bring up; control layer after APP-C.

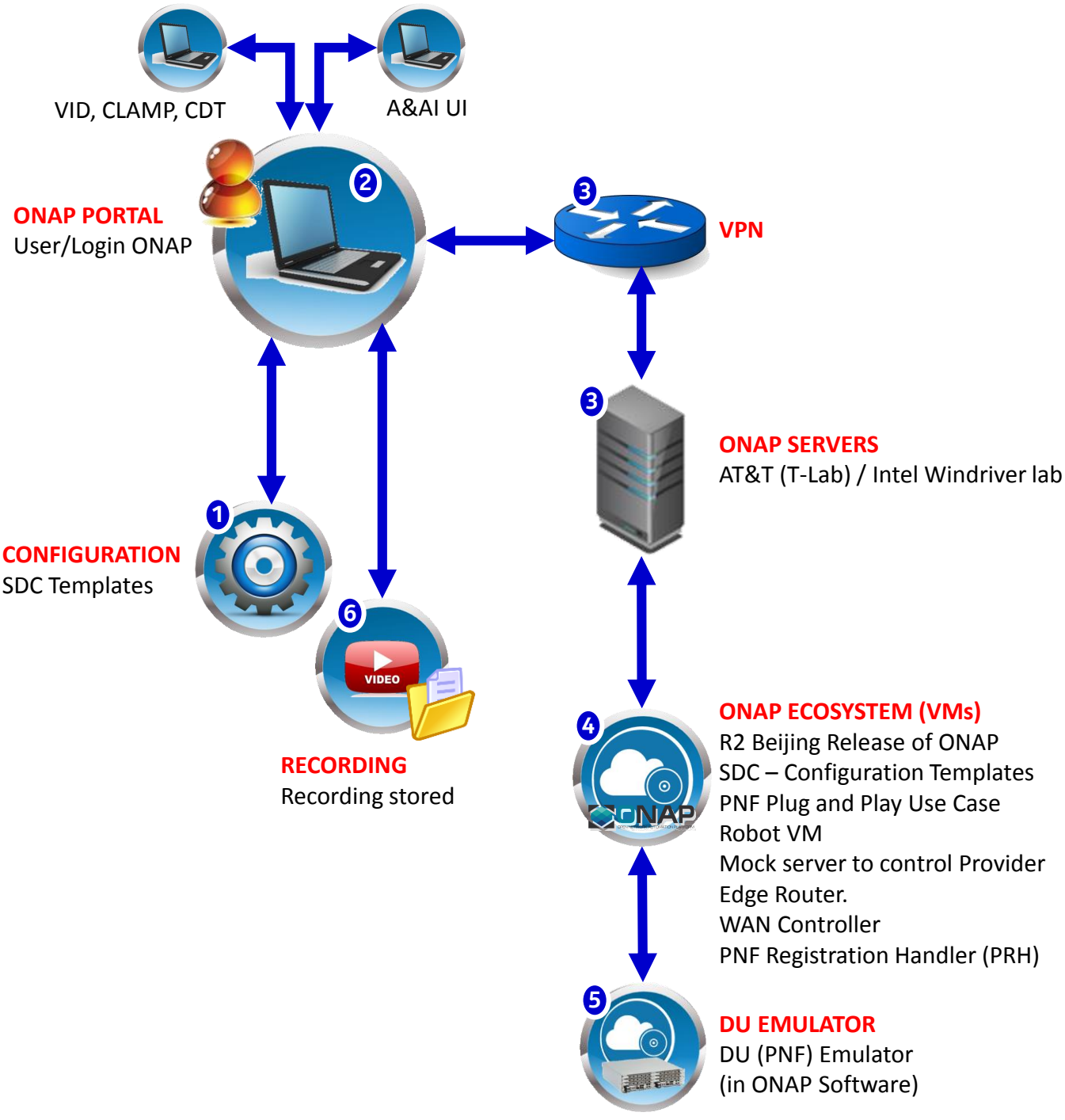
PNF Plug and Play
INTEGRATION & SHOWCASING

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

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).
AUTHENTICATION	**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 CONFIGURATION	**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	**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.
2	**PORTAL & GUIS** – 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.
3	**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) **ONAP SERVERS** – The ONAP Servers that host the ONAP ecosystem are connected to
4	**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. The PNF Registration Handler a new DCAE plug-in are available in this ONAP ecosystem which is used to register the PNF into ONAP.
5	**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.
6	**RECORDING** – A recording is made of the showcase and demo for later upload/download and playback for demonstration purposes.

PNF Demo Steps in Integration Lab

1. On ONAP, install PE simulator in Robot VM
2. Install SDN WAN controller mockserver on Robot VM and register the mockserver as WAN controller on ONAP ESR
3. Design and distribute a service in SDC with only underlay and overlay networks, similar to VoLTE use case just without EPC and IMS. We will have two PEs which are connected by underlay network
4. Check on A&AI UI to see no PE is found by correlation id in A&AI
5. Start PE simulator and verify that NO entry is created in A&AI UI, then stop the PE simulator
6. Instantiate the service from UUI with selected PE correlation ids
7. Check A&AI UI again to see PE are in A&AI but without IP
8. Verify on UUI that service instantiation is started not progressing
9. Start PE simulator again, and verify that the service instantiation progresses and finishes with success. Verify in A&AI UI that the PE has IP info

PNF Plug and Play ROADMAP (Casablanca and onwards)

- ONAP and PNF Plug and Play for 5G RAN

- 5G Use Case Team

Casablanca Release (R3)

FUTURE PROJECT IMPACTS	
Modeling, SDC, VNF-SDK	• **PNF ARTIFACTS DISTRIBUTION** SDN-R adaptation of SDN-C for PNFs (RAN Controllers). Create a single controller (SDN-R vs APP-C) SDN-R and PNF. [Currently supports NetConf-Yang] Support Ansible API to configure PNF Generic PNF PnP; Infrastructure-type PNFs vs Consumer PNFs (RAN/ x). Deploying Radio NEs. Requirement to deploy 5G Network Element (PNF, VNF) • **PNF ARTIFACTS DISTRIBUTION** – (Step 1-3) (Ansible API for SDN-R send CUIP@). For PNF service design template do we need to add a option to deployment artifact, right now SDC doesn't allow you to add this, so is this needed? How would SDN-C receive the ansible API for PNFs. Beijing Solution: Hardcode the CU IP@ (Data). Pass CU IP address based on PNF instantiation Create 5G NodeB service w/ CU & DU The CU IP @ talks to different DUs. In the service needs to get passed to the correct DU. Artifacts to pass real configuration parameter PNF Model Evolution

FUTURE Post-Bejing R2 release

FUTURE PROJECT IMPACTS	
AAF	• (Step 23, 24, 25) **[FUTURE] SECURITY AUTHENTICATION (Open Point)** – What will the long-term PNF plug and play authentication solution look like? (will not be solved in Beijing Release)
SDN-C	• **GENERIC RESOURCE API** – Message Extensions { 1…6 – VF-module activate (can reused), Assign, Configure, Deactivate } (2) *Configure* (Generic Resource API) – Try to reuse Generic Resource API for assign with parametric updates to adapt from VNF usage to PNF. Device spun-up; configure the device (for L1-L3). [Not needed for PNF Plug and Play]. **NOT IN SCOPE OF BEIJING RELEASE.** (3) *Deactivate* (Generic Resource API) – Try to reuse Generic Resource API for assign with parametric updates to adapt from VNF usage to PNF. [Not needed for PNF Plug and Play]. **NOT IN SCOPE OF BEIJING RELEASE.**
SO	• (Step 35) **GENERIC RESOURCE API** – • *Configure* (Generic Resource API) – For PNF configure the device (for L1-L3). [Not needed for PNF Plug and Play]. **NOT IN SCOPE OF BEIJING RELEASE.** • *Deactivate* (Generic Resource API) – For PNF PNP. [Not needed for PNF Plug and Play]. **NOT IN SCOPE OF BEIJING RELEASE.** • ~~(Step 36) **ACTIVATE (SO -> SDN-C)** - current flow; for Configuration & Assigning of resources. SDNC w/ A&AI w/ update information. SO -> APP-C (FUTURE). VF-Scale out. If SDN-C can do this step we proceed that way; otherwise SO puts in the DMaaP hook for APP-C (?). We expect Step 35 & 36 to happen in one "step" in Beijing Release. L1-L3 bring up; control layer after APP-C.~~
VNF SDK	PNF packages, PNF onboarding (VNF SDK)

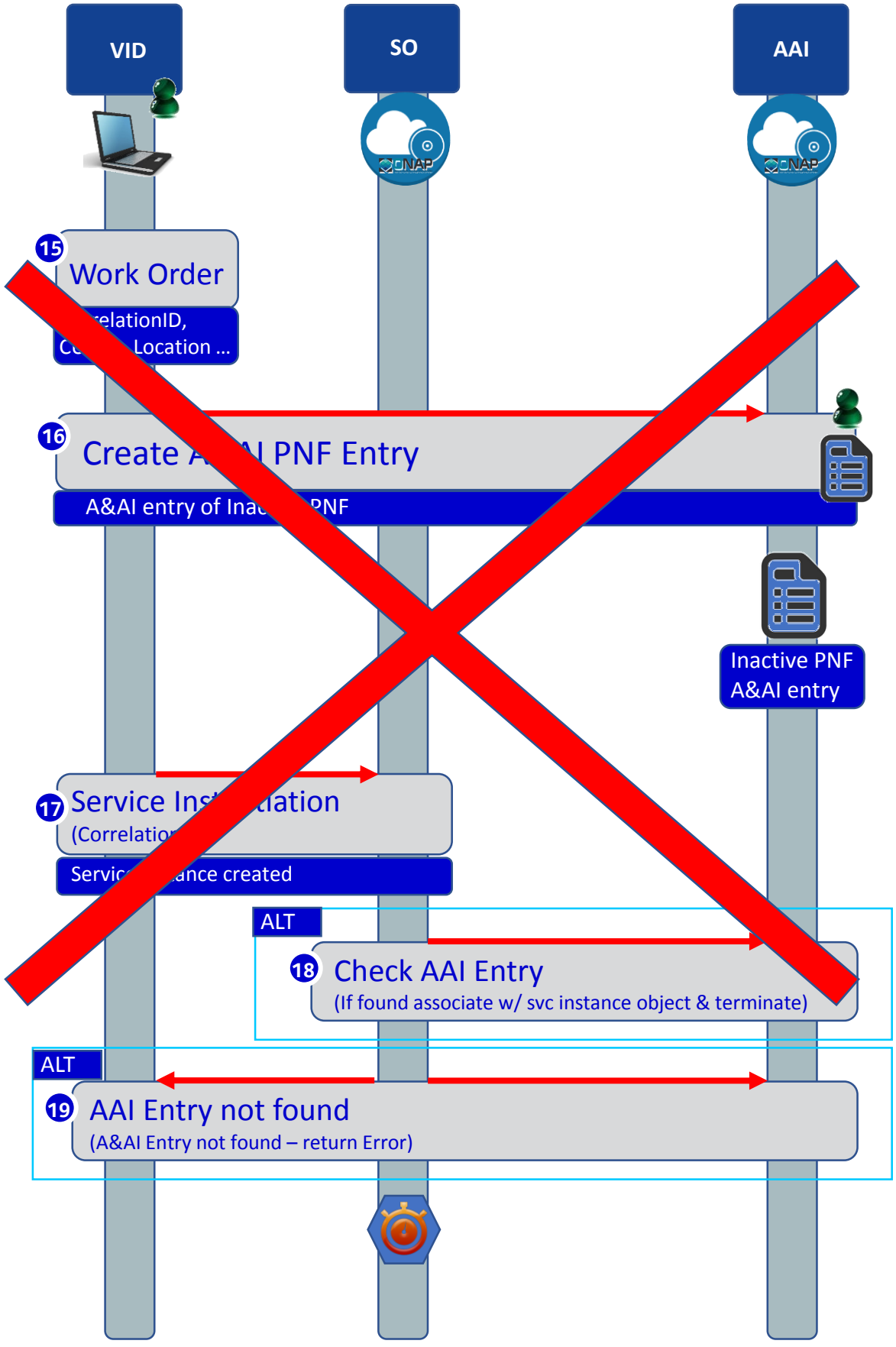
FUTURE Post-Bejing R2 release

FUTURE PROJECT IMPACTS	
PnP Discovery Procedures	Standards Broadband Forum (BBF) TR.069 (discovery for CPE devices), NetConf Call Home (Zero-Touch Draft from IETF). IETFBBF TR-069 CPE. [for Access, IoN, Optical routers, Transport devices]
SDC	Integrate CDT (used by APP-C today) into SDC [General Development] Integrated design tool for configuration design for 5G NEs.
Software Management	Software Upgrade Paradigm & PNF-ONAP. Mechanisms, Protocols, Infrastructure Manager, Packages/Image repositories, Recovery mechanisms (occurs Before Step 37) Software download & Activation of the PNF (DU). [Vimal] do we really need ONAP to manage PNF S/W? [CMCC]: "*Desire to orchestrate S/W mgmt. by operator*"
Multi-Cloud	Multi-cloud edge support Support for Underlay/overlay networks. Orchestrate, instantiate, manage "mini-clouds" on DUs. In 5G single-cloud region manage several data locations.
OOF	PNF choosing between different clouds. Using OOF to home the PNF to different ONAP Clouds vis-à-vis regional area.
"general" PNFs	Plug and Play for other categories of PNFs. Categories of PNFs: - Infrastructure type PNFs - Network type products. Edge & Network infrastructure. E.g. Optical division & Routers. - "Customer" type PNFs - vs customer-based products/Edge - Other "general" PNFs.

ONAP
OPEN NETWORK AUTOMATION PLATFORM

APPENDIX
& Meeting Notes

Service Instantiation Process (Part 1)



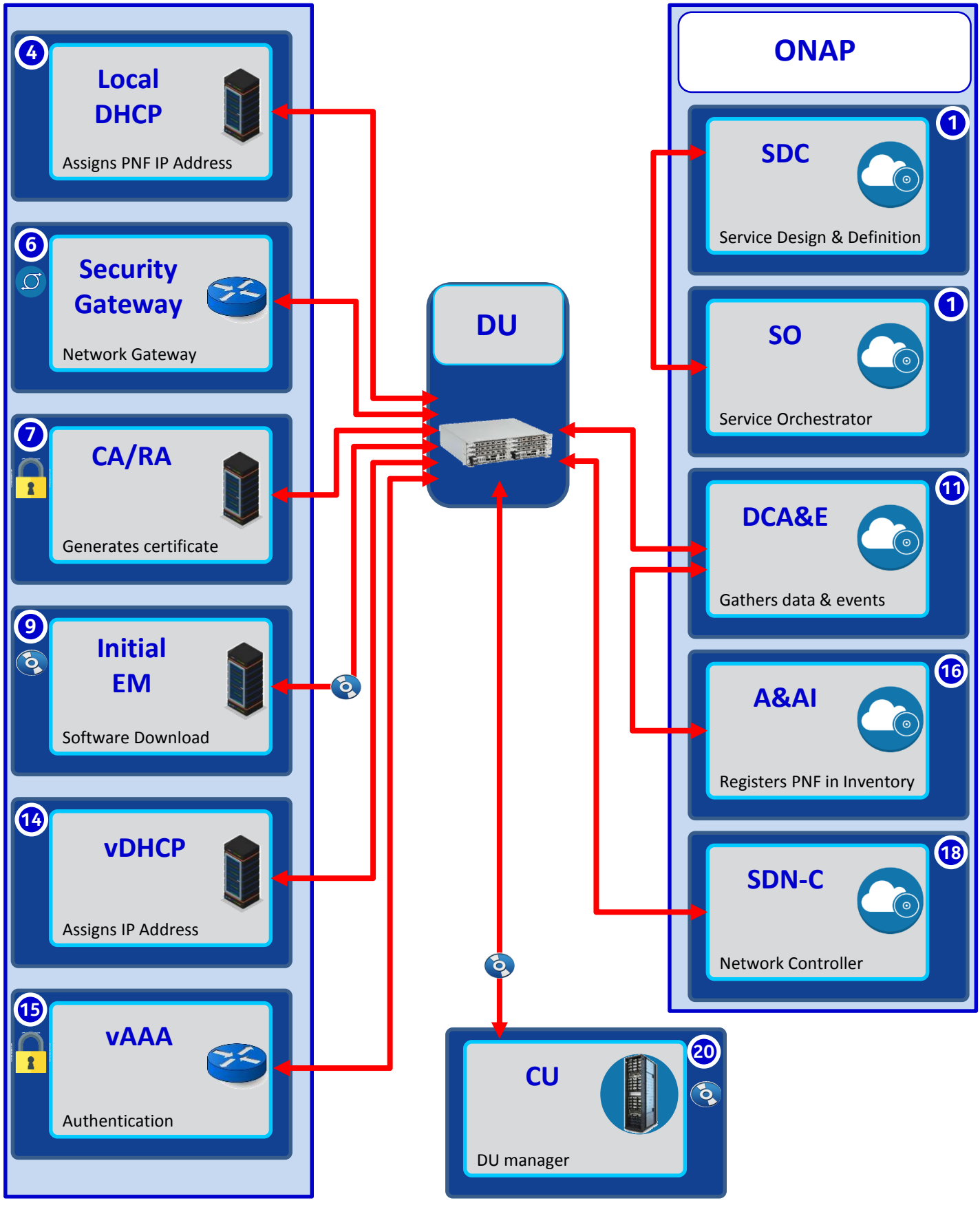
STEP	DESCRIPTION
15	**WORK ORDER** – The work order determines which PNF to use for this Service/work order. BSS is told the correlation ID. Typically, the PNF will be known before the PNF comes on-line. Orchestrated with a equipment order (to vendor) and location value for the PNF.
16	**CREATE A&AI PNF ENTRY** – From the resource declaration information, a A&AI PNF entry is made. The A&AI entry uses the information provided on the VID such as the PNF ID, SW, Config, Username, Password and Event details. This Resource declaration allows for a VES event coming from the PNF later to recognize the PNF and not drop the VES event "on the floor".
17	**SERVICE INSTANTIATION** – The operator on VID creates a service instantiation providing a correlation ID. The service is decomposed for a 5G DU PNF. The DU resource types assumes that the SDC has enough information to determine the PNF SDC model. The CU IP@ is provided manually (as part of service instantiation data).
18	**CHECK A&AI ENTRY** – The BPEL 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.
19	**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.

Agreed on ONAP SO Weekly Sync up on Feb 21, 2018 to use the flow shown on Steps 15-22.

In ATTENDANCE:

Ben Cheung, Marge Hillis, Linda Horn, Sigmar Lust, Damian Nowak, Byung-Woo Jun, DeWayne, John Choma, Rob Daugherty, Arthur Martella, Fred Oliveira, Gil Bullard, Seshu, Abhishek, Azhar Sayyed, Chittars, Ethan Lynn, Marcus Williams, Steve B, Suma, Lukasz Biniek

PNF Plug and Play (PnP) Overview (e.g.)



Feb 16, 2018
ATTENDEES – Ben, Gil, Vimal, Oskar, Shekar, Ken Shi, Linda, Marge, Sigmar, Timo P. Dandrushko, Brian, Dmitriy Andrushko (Mirantis)
AT&T Canopy – preloads A&AI w/ PNFs
But that only works for big PNFs.
Work orders – individual devices are ordered
Canopy is database of physical assets
Can sync up A&AI in advanced
That model doesn't work for consumer.
Because you don't know which instance you will use until it is dispatched
For consumer a technician has many "boxes" PNFs with them.
Pull a "random" box and plug it in.
Don't know until last minute which instance will be used.
It was proposed that (CUTTING OUT) which device to use
Let's have that go to Canopy (CUTTING OUT)
VES event go to canopy, if event repeated outage, wanted event to go DCAE
(CUTTING OUT)
A&AI device to be configured (CUTTING OUT)
Bring your own device so plug in device, go to website (VID-like)
Enter "please activate it"
WORK ORDER/SERVICE ORDER needs to be updated, asset management
Tracking dozen boxes know which box is where (CUTTING OUT)
Assess management tracking systems; service order updated
BSS Systems; for this customer service order; we're using this device.
Could ask technician additionally type in MAC address in VID or
Update VID first. When tech scans box, in addition to update service order (released to ONAP). Have that scan result in a separate (CUTTING OUT) to first inventory the PNF. Then release the service order to ONAP.
STEP 28 could create A&AI; objection any random device connecting; Model
Generic device that can work in 3 contexts; Do I need to know purpose.
PNF model#ABC correlationID = model+MACaddress
Reason why we waited, assumed that needed to have the service context first
Wait for service request (on northbound side)
Device's purpose & context could change over time
Separate as commodity and device [x]
How do we prevent blowing out A&AI (failures, misconfiguration
STORMS of event in Step 26.
Don't want to update A&AI until service I know PNF will serve.
CHURN in A&AI (from many Step 26s)
Distinction between Consumer and Infrastructure (know PNF in advance)
Possible RACE CONDITION for consumer case
For RACE CONDITIONS – if get event ignore it if unknown
Service request/work order update it with instance information
When that service/work order is trigger for ONAP

Feb 19, 2018
ATTENDEES – Ben, Yoav, Oskar, Marge, Sigmar, Damian

NOTES-

(1) **HOW WILL PNF AUTHENTICATION IN THE FUTURE LOOK LIKE?** TR317 authentication. AAA server exchange (authenticating the DHCP request). TLS2.0 w/ certificate. Post of event to PRH. – Added security to access ONAP. Because this opens the question of *how does the PNF actually get the username/password*. Hard Code? (Put into Initial EM)? AAF project could be used for external communications. DSLAM operators (in your home DSL) port on the other end connects to DSLAM. How does it know to trust? DSLAM adds an option on DHCP request it gets "this came on port :[x]" in the network added profile info; when request arrives goes to AAA server & verifies. [FUTURE] Initial EM = VNF. Gets credentials from ONAP. BNG (broadband network gateway) "router". Proxy Un/Pass get to Proxy. Draft (standard) for zero-touch "learning" of devices. How do we know it is good?

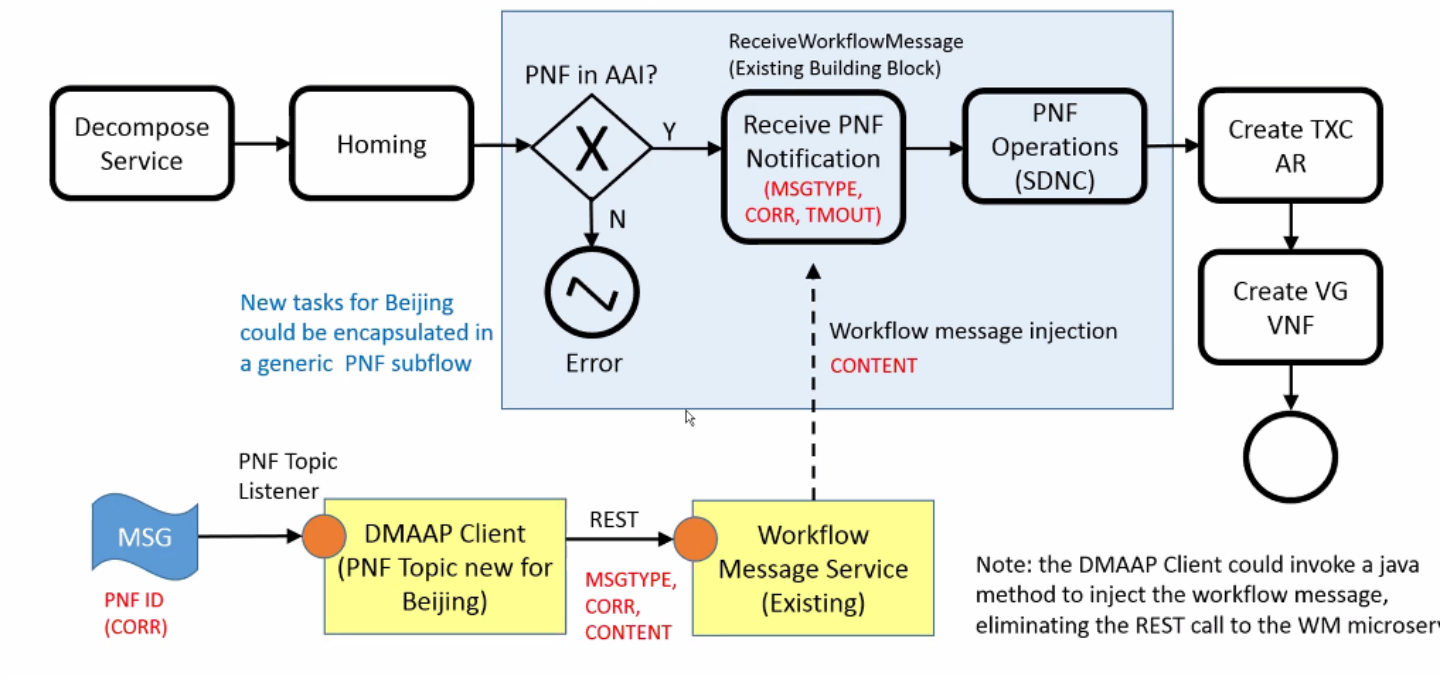
(2) **Where is Username/Password located** – in DHCP server *username & Password (for PNF to access ONAP) .*

(3) **Will AAF Project be involved?** – *Will AAF in the future be involved w/ PNF security solution.*

(4) **LINKS**: https://tools.ietf.org/html/draft-ietf-netconf-zerotouch-19
https://wiki.onap.org/display/DW/vCPE+Use+Case+Tutorial%3A+Design+and+Deploy+based+on+ONAP+Amsterdam+Release

(1) Project Technical Lead (PTL)

CreateVcpeResCust - Proposal "B" for PNF support



APP C Meeting Feb 21 2018—attendees Randa, Scott, Ben, Linda Marge
APP-C does send configure commands to VNFs using Ansible Chef or Netconf. The communication method is selected when the APP-C configure template is built.
The Configure template is a new entity in the Beijing release and they should have more documentation and information after the next Sprint. Paul is the architect for this tool and can give us a demo when he returns from vacation next week. Basically the template is created stand-alone this is not created from SDC in Beijing release. One creates the template from a GUI—the GUI then sends the template to APP-C (its possible Randa and Scott are checking) that the GUI sends the template to SDC and SDC distributes it—they will let us know) The flow should be create the SDC model—this will give us a PNFtype which we have to use for the CDT template—At this time there is not cross checking of data between SDC and the CDT tool. The CDT tool was needed because APP C is not parsing the TOSCA models and needs to have a way of marrying the data sent in a configure request from SO to a format that a PNF/VNF would expect to see. There is one CDT template per PNFtype where a PNFtype might be a Nokia5GDU. SO will send a configure message to APP C. APPC will see the PNFtype in the message and will take the data in the payload and using the template it will create the Ansible/Chef/NetConf appropriate message/command to send the configuration data to the PNF. The SO configure message will include the PNFID and APPC will send the configure directly to the device. (the User Name and Password needed to set up the secure connection will either be in a property file or could get sent in the payload or could be written in the template (maybe for Beijing) Linda asked where the configuration data comes from---Scott has seen it in the payload. This is okay for us in Beijing since we are passing only one parameter. There may be enhancements in later releases where APP-C can go someplace to query for a config file of some sort. The open item for us is if we can use the same API for PNFs as is used for VNFs. Randa pointed us to the API definition We need to study this and send questions.
http://onap.readthedocs.io/en/latest/submodules/appc.git/docs/APPC%20LCM%20API%20Guide/APPC%20LCM%20API%20Guide.html
Next steps
We study LCM API Guide for APPC and ask questions.
Randa sends us some available times for Paul to show us the tool and perhaps a demo and Marge will schedule the meeting.

PnP SECURITY

It is possible to install a certificate into ONAP to be used for authentication in Beijing. Documentation needs to be created so a user would know how to do this.
Open SSL library is used to authenticate certificates and this works in ONAP. Currently, the ONAP component has to call the SSL APIs itself. DCAE may already do this.
Usernames and passwords (for HTTP) need to be manually stored locally (in a /etc/password file?) for Beijing.
AAF is working on security improvements in the Beijing release that would be available for use by other ONAP components in the Casablanca release. CADI (Code Access Data Identity), secret management (storage and protection of secret data like passwords and private keys) and certificate management will provide a common way for ONAP components to store and authentication certificates and passwords.
The people on the call did not have detailed information about how any of this is done right now or how it will work in Casablanca but Amy Zwarico took notes on what functionality and documentation we need and agreed that the Security Subcommittee and AAF should address these needs. It was a very positive meeting.

MARCH 13, 2018
Attendees: Alok, Fari, Gil, Yoav, Oscar, Farideh, Linda, Marge, Damian, Lushing

Very very long meeting. AT&T was not aligned at all and argued about the capabilities of DCAE.

We were told that it is too late to make any API changes (which a new Domain type would be) for Beijing.

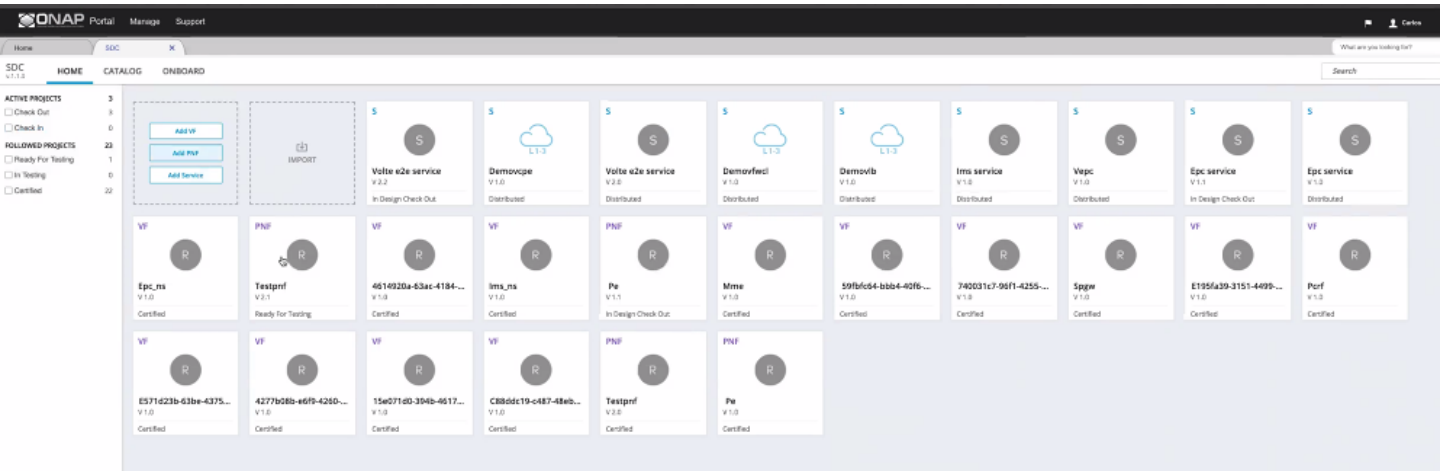
If we want to do anything for Beijing here is the proposal

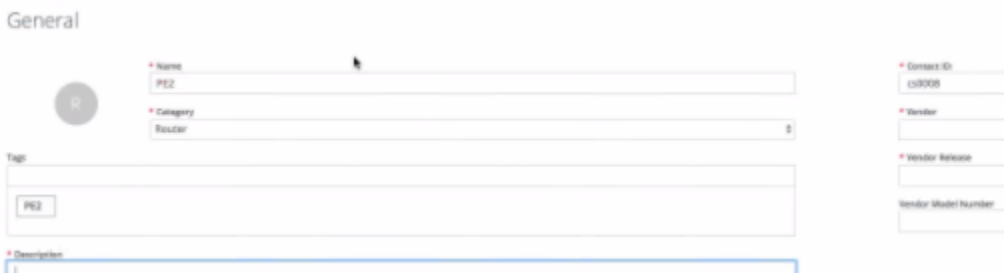
It is believed that DCAE VES Collector can process messages, as long as there is a valid user name and password, before the PNF instance is known in ONAP. What would be done is a User Name and Password would be provided for a PNF type. The PNF would send a VES event of the type "other" to any DCAE collector
The Collector will supposedly be able to analyze that message and assign it to a DMaap topic that the PRH can subscribe to.

Our domain was rejected for many reasons—too much information, not sure all PNFs need, ATT wants to provision etc. However the reason that broke the camel's back is that its too late for Beijing. IT WAS AGREED THAT THIS NEEDS TO BE RE-VISITED FOR CASABLANCA---BEN PLEASE ADD THIS TO THE OPEN POINTS

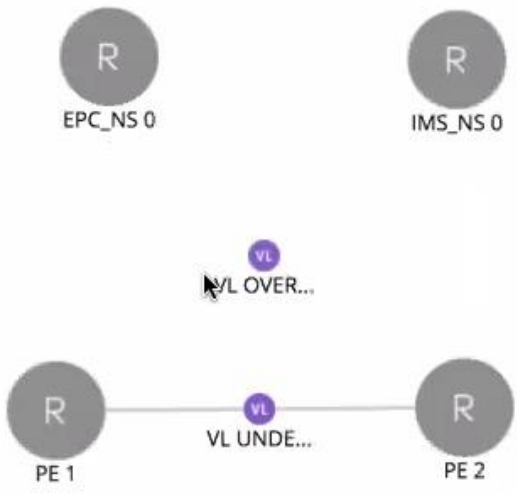
We are concerned about this because Lushing thinks that the VES collector now cannot process the "other" event type but Alok is checking and will send email.
If the collector can process "other" we will use it for Beijing and revisit later.

Damian and Linda—I hope I have this correct there was so much fighting its hard to parse this down to specific things.
I will say Farideh was on the call for most of the time and could well hear the disagreement within ATT and the simplistic support available in DCAE at this time. This can only help our position that ONAP is not ready





Property Name	Type
VL UNDERLAYVPN 0	
serviceType	string
template_author	string
ac2_svlan	integer
ac1_ip	string
ac1_protocol_bgp_as	string
description	string
ac2_route	string
site2_name	string
vendor	string
site1_name	string
ac1_id	string



Property Name	Type
EXTCP	
ip_requirements	list
network_role	string
subnetpoolid	string
mac_requirements	MacRequirements
exCP_naming	Naming
vlan_requirements	list
network_role_tag	string
order	integer

pe1_id	string
id	string
ac1_svlan	integer
ac2_protocol_bgp_as	string
sna2_name	string
ac2_peer_ip	string
topology	string

5G DU (PNFs)
Virtual Link type
Connect 2 PNF w/ connection
Underlay = 1 type of VL

EPC – VOLTE network service provides connectivity for UE to network
IMS – Service if you have connection service for multi-media (voice, video)

```
  PE 2:
    type: org.openecomp.resource.pnf.Pe
    metadata:
      invariantUUID: 14544ac5-c2c5-4b83-9ba3-de4eba0f0f8e
      UUID: 85092b2c-3cdb-48a1-a17b-ac1587fda6a1
      customizationUUID: 4dddd028-b3de-427c-b06c-561846972755
      version: '1.0'
      name: PE
      description: Provider Edge
      type: PNF
      category: Network L2-3
      subcategory: Router
      resourceVendor: ONAP
      resourceVendorRelease: ONAP 2.0
      resourceVendorModelNumber: PE2018
    requirements:
    - port.link:
        capability: virtual_linkable
        node: VL UNDERLAYVPN 0
  IMS_NS 0:
    type: org.openecomp.resource.vf.ImsNs
    metadata:
      invariantUUID: 692d2050-076d-4a92-a36f-d97fdca190e2
      UUID: 06ed37eb-71e9-4ba2-ba7e-8f20eddb6f71
      customizationUUID: 0de4d127-3d77-4c1f-92b6-db9a0fed4f42
      version: '1.0'
      name: IMS_NS
      description: IMS Network Service
      type: VF
      category: Generic
      subcategory: Abstract
      resourceVendor: ONAP
      resourceVendorRelease: ONAP 1.0
      resourceVendorModelNumber: ''
    properties:
      nf_naming:
        ecomp_generated_naming: true
      availability_zone_max_count: 1
      nsd0_providing_service_invariant_uuid: f582235c-c267-4226-9ba8-b0d7e3dcbec8
      nsd0_providing_service_uuid: 64a8e35c-1138-4584-96d6-d44581ed73be
```

```
{
  "resourceName": "VL UNDERLAYVPN",
  "resourceDefId": "4f5d692b-4022-43ab-b878-a93deb5b2061"
  "resourceId": "b977ec47-45b2-41f6-aa03-bf6554dc9620",
  "nsParameters": {
    "locationConstraints": [],
    "additionalParamForNs": {
      "topology": "full-mesh",
      "site2_name": "site2",
      "sna2_name": "site2_sna",
      "description": "underlay",
      "sna1_name": "site1_sna",
      "ac1_route": "3.3.3.12/30:dc84ce88-99f7",
      "ac2_peer_ip": "3.3.3.20/30",
      "technology": "mpls",
      "ac2_route": "3.3.3.20/30:98928302-3287",
      "ac2_id": "84d937a4-b227-375f-a744-2b778f36e04e",
      "ac1_protocol": "STATIC",
      "ac2_svlan": "4004",
      "serviceType": "l3vpn-ipwan",
      "ac2_ip": "3.3.3.21/30",
      "pe2_id": "4412d3f0-c296-314d-9284-b72fc5d485e8",
      "ac1_id": "b4f01ac0-c1e1-3e58-a8be-325e4372c960",
      "af_type": "ipv4",
      "ac1_svlan": "4002",
      "ac1_peer_ip": "3.3.3.12/30",
      "ac1_ip": "3.3.3.13/30",
      "version": "1.0",
      "name": "testunderlay",
      "id": "123124141",
      "pe1_id": "2ef788f0-407c-3070-b756-3a5cd71fde18",
      "ac2_protocol": "STATIC",
      "site1_name": "stie1"
```

```
properties:
  serviceType:
    get_input: vlunderlayvpn0_serviceType
  template_author:
    get_input: vlunderlayvpn0_template_author
  ac2_svlan:
    get_input: vlunderlayvpn0_ac2_svlan
  ac1_ip:
    get_input: vlunderlayvpn0_ac1_ip
  ac1_protocol_bgp_as:
    get_input: vlunderlayvpn0_ac1_protocol_bgp_as
  description:
    get_input: vlunderlayvpn0_description
  ac2_route:
    get_input: vlunderlayvpn0_ac2_route
  site2_name:
    get_input: vlunderlayvpn0_site2_name
  vendor:
    get_input: vlunderlayvpn0_vendor
  site1_name:
    get_input: vlunderlayvpn0_site1_name
  ac1_id:
    get_input: vlunderlayvpn0_ac1_id
  pe1_id:
    get_input: vlunderlayvpn0_pe1_id
  id:
    get_input: vlunderlayvpn0_id
  ac1_svlan:
    get_input: vlunderlayvpn0_ac1_svlan
  ac2_protocol_bgp_as:
    get_input: vlunderlayvpn0_ac2_protocol_bgp_as
  sna2_name:
    get_input: vlunderlayvpn0_sna2_name
  topology:
    get_input: vlunderlayvpn0_topology
  ac2_peer_ip:
    get_input: vlunderlayvpn0_ac2_peer_ip
  ac2_ip:
    get_input: vlunderlayvpn0_ac2_ip
  af_type:
    get_input: vlunderlayvpn0_af_type
  technology:
    get_input: vlunderlayvpn0_technology
```

A: 5G Radio Network Deployment Requirements

Description	Disaggregated 5G RAN may include PNFs and VNFs, in which case cloud infrastructure deployment at the edge is required. Beijing implemented the first phase of PNF discovery and instantiation. Our goal for Casablanca is expand on that work, include VNF deployment at the edge, and fully integrated lifecycle management. Key enhancements needed are: • Support full Application level Configuration (+Ansible), allow various mobile network elements to be controlled from same controller persona created from CC-SDK • Add Lifecycle management functions to controller persona • Support an integrated configuration design tool in SDC that can be used with any controller persona (next gen CDT) • Add support for PNF Software Management and Change management • Edge Cloud Support • Add needed support for deploying Mobility Virtual Network Elements (e.g. CU) at the Edge locations • Further automation of PnP Discovery for PNF
Rationale	Support for deploying and managing 5G mobility network is critically important for most ONAP members.
Impacted ONAP components	**SDC, SO, CC-SDK (SDN-C, APP-C), AAI, DCAE, (V/P)NF-SDK**
Participating Companies	AT&T Amdocs China Mobile Ciena Cisco Ericsson Huawei Intel Nokia VMWare Others

For details regarding the requirements, please see https://wiki.onap.org/display/DW/Missing+Platform+capabilities

From Friday's meeting, we plan to test PNF with VoLTE use case. I expect we can add an PNF(PE router) in SDC, and add properties (like PNF correlation id, etc) and requirements/capabilities (linkable) to the PNF. During service design phase of VoLTE service in SDC, we should be able to pull in two PNFs in composition step and connect them with a underlay network (VL type). Is this doable in current SDC?

After reading the mail I have a number of concerns here:
There is no option to add properties to a PNF itself. You can add different modeling items to the PNF like CP's and they have properties.
the PNF comes with a number of pre-defined properties I have attached an example to this thread.
The correlation id is not a property that is defined in SDC but is populated by VID and used for matching in AA&I
To connect to PNF'S you will need to define on what to connect them this usually means defining a CP in the PNF.
The most important thing is that as far as I know the PNF logic goes through VID and VID is not used at the moment in VOLTE.

We need to align the flow to reflect this and vid needs to be part of this discussion.