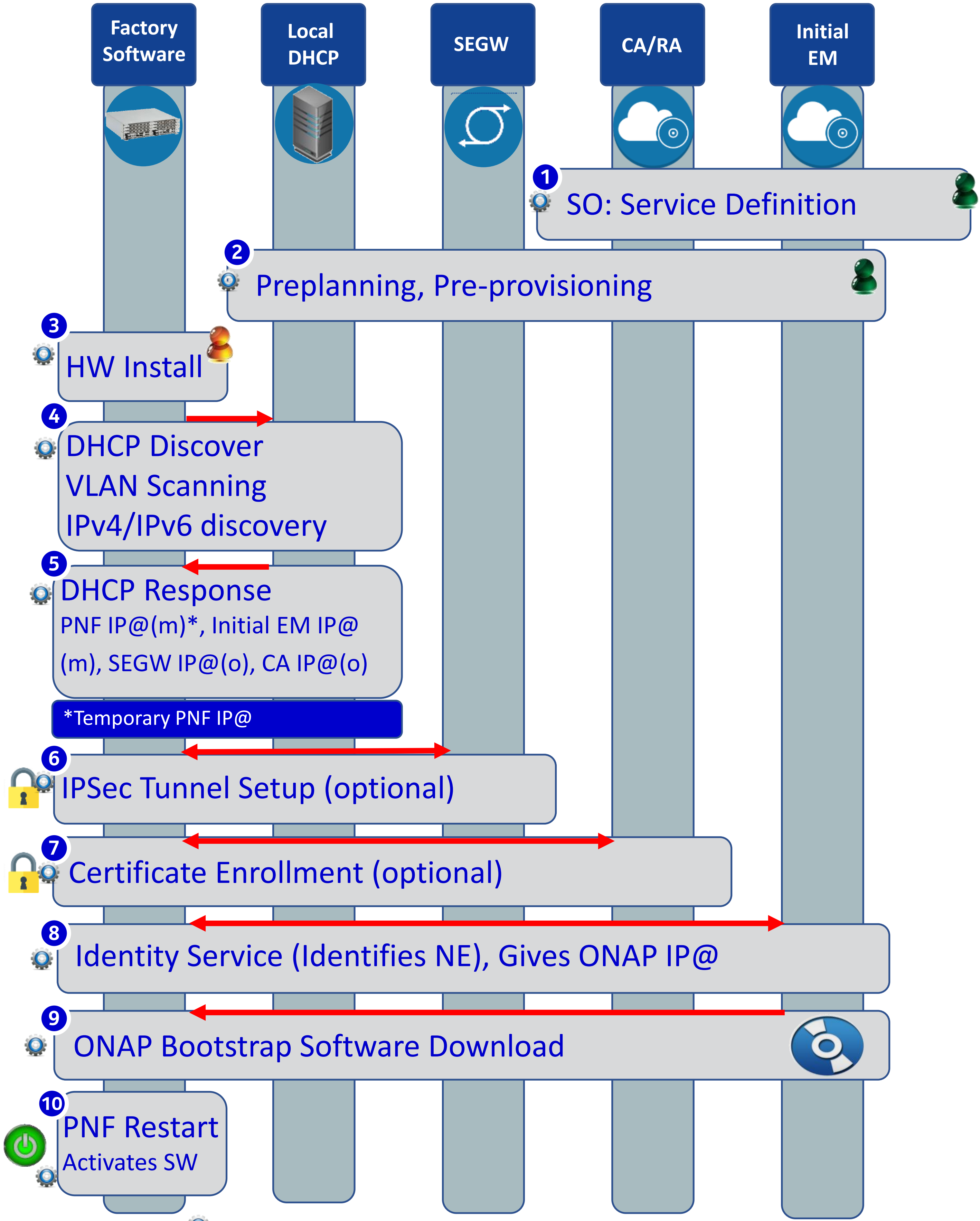
| ACTORS | DESCRIPTION |
|---|---|
| PNF | **PHYSICAL NETWORK FUNCTION (PNF)** – The Distributed Unit (DU) or Network Hardware device that provides service to an end-user. |
| DHCP | **DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP)** – Protocol to assign IP addresses to a network element (NE). The IP address 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, reponsible 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)** – The network controller manages messages, DMaap Events, Inventory queries. A controller for Layer 0 to 3 devices and to manage 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 onboarding can potentially perform analytics on the onboarding 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)** - Manages the life cycle of virtual applications, virtual network functions (VNFs), and components. A controller for “applications”. App-C manages the 5G DU & 4G DU. |

# PNF Bootstrapping Steps



Factory Software

Local DHCP

SEGW

CA/RA

Initial EM

1 SO: Service Definition

2 Preplanning, Pre-provisioning

3 HW Install

4 DHCP Discover
VLAN Scanning
IPv4/IPv6 discovery

5 DHCP Response
PNF IP@(m)*, Initial EM IP@(m), SEGW IP@(o), CA IP@(o)

*Temporary PNF IP@

6 IPSec Tunnel Setup (optional)

7 Certificate Enrollment (optional)

8 Identity Service (Identifies NE), Gives ONAP IP@

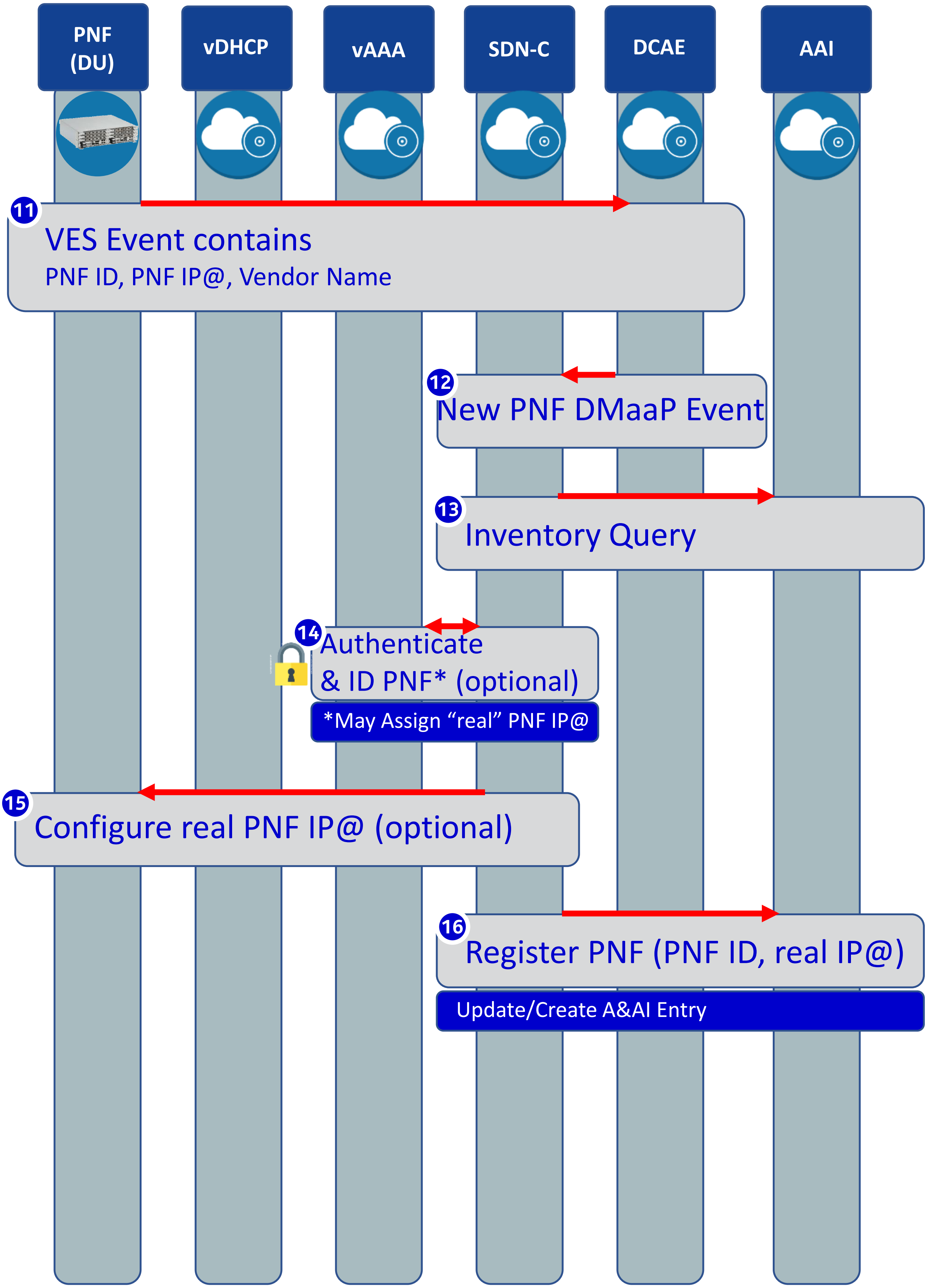
9 ONAP Bootstrap Software Download

10 PNF Restart
Activates SW

⚙ Vendor Specific Step

| STEP | DESCRIPTION |
|---|---|
| 1 | **SO: SERVICE DEFINITION** - A technician will provision the Service Definition which describes the type of VNF & PNF (CU & DU) units that will be instantiated. These are models that describe the type of units that we expect to support. Later, a correlation key (of the PNF ID) on the VID GUI is used to fetch what type of PNF to use based on the PNF ID. service template ID/name and a PNF ID/key shall be provided via VID (or other API) for service definitions containing PNF |
| 2 | **PRE-PLANNING, PRE-PROVISIONING** – There is data which is programmed into the system for the PNF onboarding 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. |
| 3 | **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. |
| 4 | **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. |
| 5 | **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. |
| 6 | **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. |
| 7 | **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. |
| 8 | **IDENTITY SERVICE** – The identity service is there to identify the PNF. It also returns the ONAP IP address |
| 9 | **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 |
| 10 | **PNF RESET** – The PNF is reset so that the downloaded ONAP Bootstrap software becomes activated and is then ready to continue to PNF registration |

# PNF Registration Steps



PNF (DU)

vDHCP

vAAA

SDN-C

DCAE

AAI

11 VES Event contains

PNF ID, PNF IP@, Vendor Name

12 New PNF DMaaP Event

13 Inventory Query

14 Authenticate & ID PNF* (optional)

*May Assign “real” PNF IP@

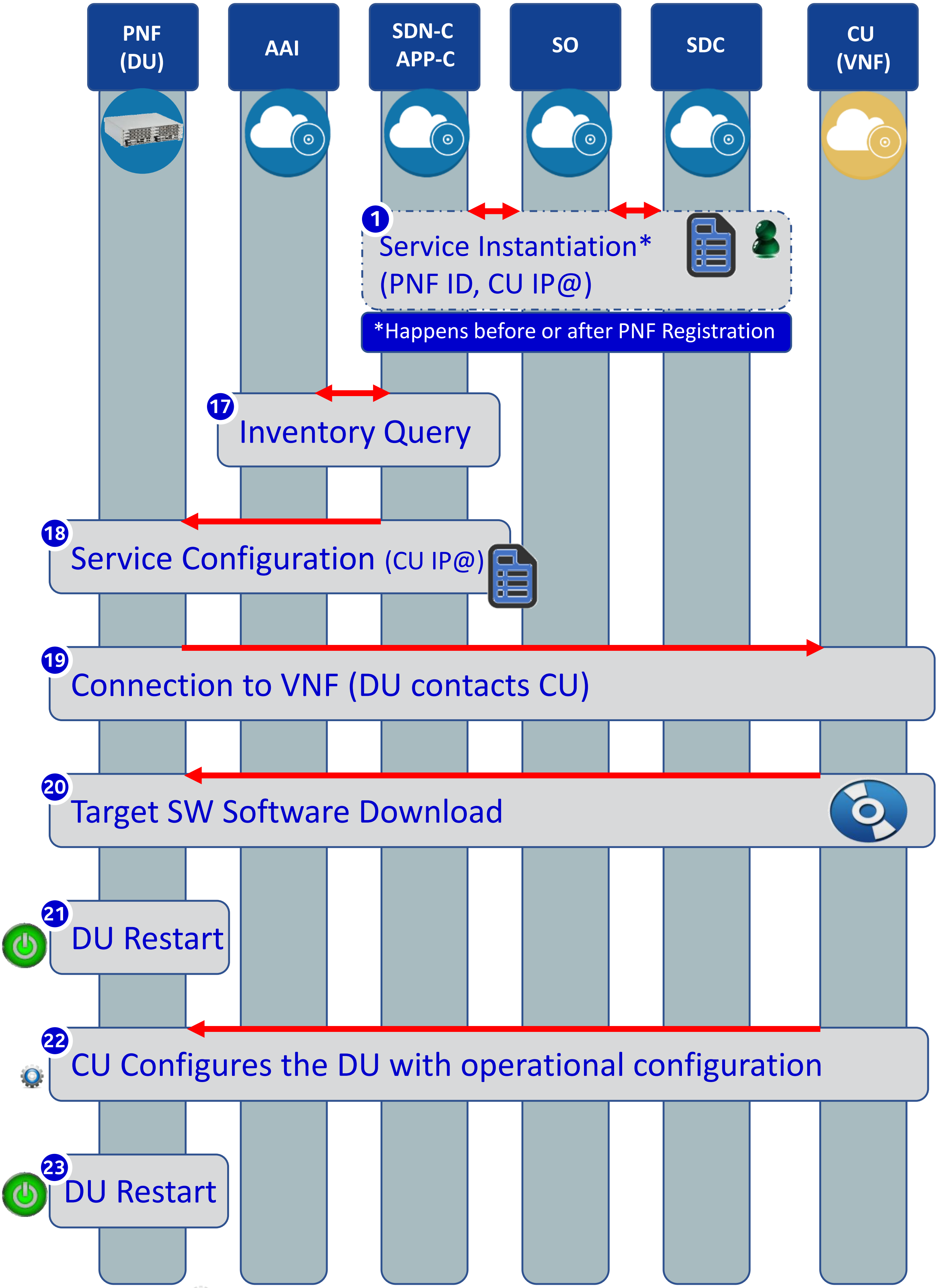
15 Configure real PNF IP@ (optional)

16 Register PNF (PNF ID, real IP@)

Update/Create A&AI Entry

| STEP | DESCRIPTION |
|---|---|
| 11 | **VES EVENT** – The PNF generates a VES Event to DCAE which is the “triggering” event that tells ONAP that the PNF is trying to register. This VES event contains the PNF ID, which will serve as an identifying key within A&AI to seek for that particular PNF. The VES event also contains the PNF IP address and the vendor name amongst other things. |
| 12 | **DMaaP EVENT** – When DCAE receives the VES event, DCAE generates a DMaaP event. This then publishes the VES event into the proper Kafka topic. SDN-C subscribes for these types of events and so is notified when one is published. This VEST event indicates that a new PNF has been identified. |
| 13 | **INVENTORY QUERY** - SDN-C performs an inventory Query to A&AI. It might have been the case that the instance of this PNF has already been created; and thus, already exists within A&AI. It performs this query using the PNF ID as a key. |
| 14 | **AUTHENTICATION** - SDC uploads the serial# and MAC address into A&AI so that in this step SDN-C knows to expect a particular PNF hardware. This step is optional and is vendor dependent. Also, the PNF doesn’t need this step; it is a security measure for ONAP. Note that SDC would need a custom DG for PNF-based SDC data. |
| 15 | **CONFIGURE PNF IP @** - If so desired, a permanent IP address can be provided to the PNF in this step. The PNF would receive this IP address and use it starting at this point in the onboarding process. 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 step is optional and is not necessarily executed. |
| 16 | **REGISTER PNF IN A&AI** – The PNF is registered into A&AI using the PNF ID as a key. SDN-C has already performed an inventory query, and it might be the case that the PNF already exists, it might be the case that the PNF information needs to be updated, or lastly it might be the case that the PNF A&AI entry needs to be created. After this step, the PNF is considered to be registered into the ONAP and with an entry into A&AI becomes available as an network element to fulfil service requests. |

# PNF Activation Steps



PNF (DU)

AAI

SDN-C APP-C

SO

SDC

CU (VNF)

1 Service Instantiation* (PNF ID, CU IP@)

*Happens before or after PNF Registration

17 Inventory Query

18 Service Configuration (CU IP@)

19 Connection to VNF (DU contacts CU)

20 Target SW Software Download

21 DU Restart

22 CU Configures the DU with operational configuration

23 DU Restart

Vendor Specific Step

| STEP | DESCRIPTION |
|---|---|
| 1 | **SERVICE INSTANTIATION** – The PNF is instantiated from the Service Definition. The service instantiation may occur before or after PNF registration. It is noted as step 1 because it might also happen during step 1, for pre-provisioning. The PNF ID is used as a key, and the CU IP @ is provisioned. The 5G DU application is an instantiation on the PNF. |
| 17 | **INVENTORY QUERY** – SDN-C performs an A&AI query using the PNF ID as a key. |
| 18 | **SERVICE CONFIGURATION** - The SDN-C provides the CU IP @ to the DU, which will allow the DU to contact the CU. |
| 19 | **CONNECTION TO VNF** – 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. |
| 20 | **TARGET SOFTWARE DOWNLOAD** - The new Target Software is downloaded which is the RAN specific software that will replace the ONAP Bootstrap software. |
| 21 | **DU RESTART** –After the software successfully reboots, the Target Software becomes activated, and the PNF truly becomes a DU (Distributed Unit). |
| 22 | **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. |
| 23 | **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. |

# Backup Slides

TOPIC For Discussion (Oskar Malm)

Processing of incoming DMaaP events (possibly converted from VES events by DCAE) related to PnP

Support resource assignment request from SO during service instantiation if service description includes a PNF. I don’t know if today this would mean SO selecting the controller, or if SO simply posts a message expecting a controller to pick up that message. Either way multiple controllers cannot handle the same request.

Additional configuration of PNF as requested by SO, e g using NETCONF.

mailto:oskar.malm@ericsson.com

- (page 1) Do we agree that SDNC will host the specific logic needed to support PNFs in the controller layer? Will SDNC handle all PNFs, regardless if they provide “L0-3” or “L4+” functions? Does this mean that SDNC also will handle application level configuration of network functions and not just IP/Ethernet/forwarding etc? Will APPC be involved at all for any PNFs?

**FREEMAN, BRIAN D <bf1936@att.com>**

SDNC would not likely be the configuration entity for all PNFs.

Particularly Mobility VNFs would either be APPC or the existing Service Provider OSS’s since likely the PNFs are exactly the same for the service provider.

I think (to be confirmed) the goal of the PNF discovery is partly to make hybrid solutions where we have both a VNF and a PNF work with the data going into ONAP for the PNF to support the E2E service flows that can combine the two. A service provider may chose to use SDNC, APPC, or their existing OSSs to configure the PNFs.

I think the self discovery mechanism should support “triggering” of the service provider selected mechanism (and I think that is supported in the flow at the SO interface) . When its APPC or SDNC that trigger can be routed to the ONAP component based on the SO Model/workflow etc.

It is also possible that ONAP workflow would simply notify the OSS that the configuration is required and wait for notification that configuration is complete in the SO workflow.

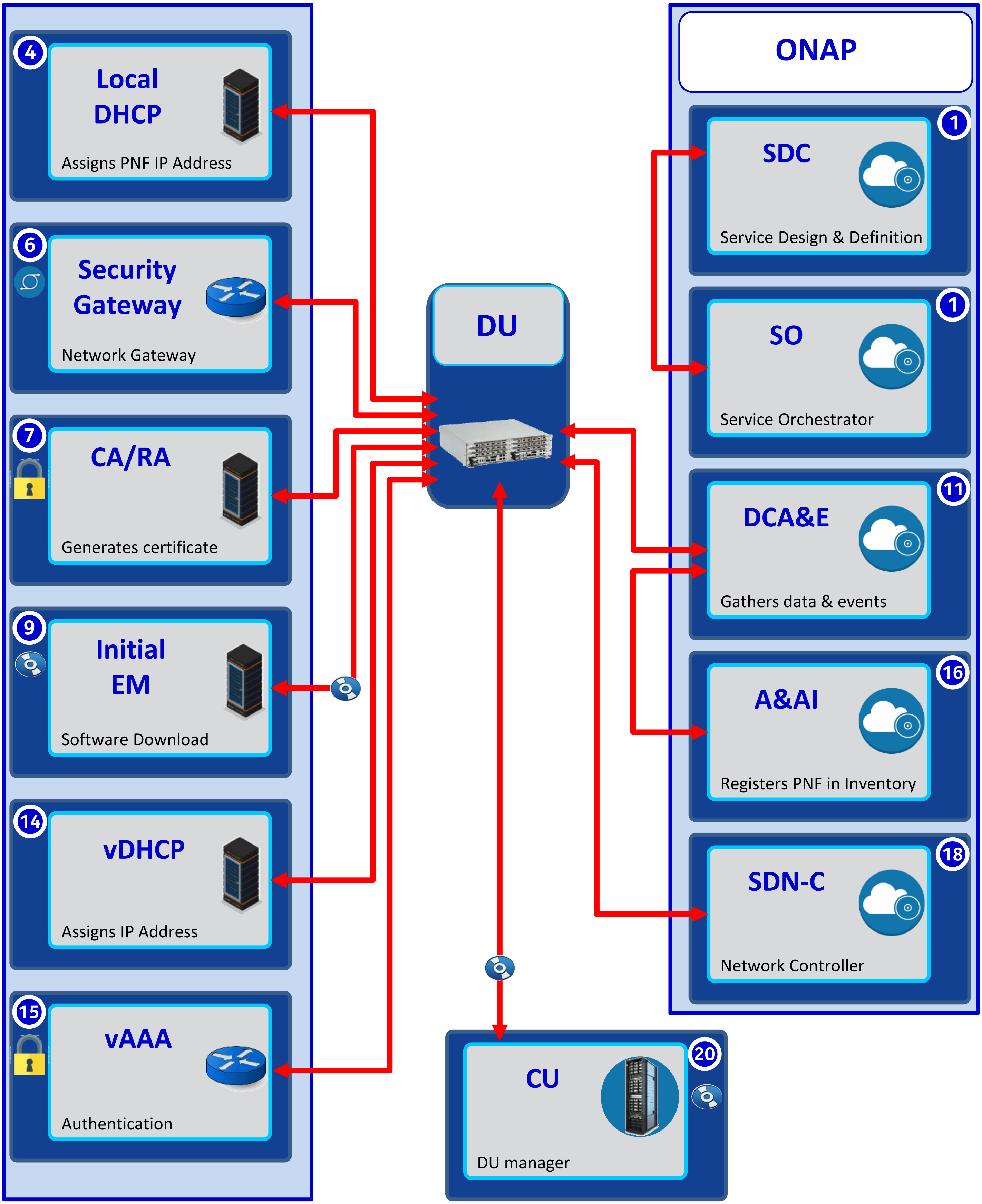
We should keep in mind that consumer PNF self discovery can flow differently since many times the new PNF is brought up in a “walled garden” with temporary IP address / configuration until terms and conditions are agreed to and the actual account data is pushed.

Sometimes that account data i tied by MAC address of the device.

Sometimes that account data is tied to the layer 2 device that the PNF is attached (DHCP Option 82 data with “subscriber vlan” information )

Sometimes that account data is tied to DATA entered by the user in self service while in the walled garden and then pushed to the PNF only after terms and conditions are agreed to (and reboot as necessary to remove the walled garden) – DOCSIS has used this method on occasion.

# PNF Onboarding (PnP) Overview (e.g.)


4
Local DHCP
Assigns PNF IP Address
6
Security Gateway
Network Gateway
7
CA/RA
Generates certificate
9
Initial EM
Software Download
14
vDHCP
Assigns IP Address
15
vAAA
Authentication
DU
ONAP
1
SDC
Service Design & Definition
1
SO
Service Orchestrator
11
DCA&E
Gathers data & events
16
A&AI
Registers PNF in Inventory
18
SDN-C
Network Controller
20
CU
DU manager