

# CCVPN(Cross Domain and Cross Layer VPN) USE CASE

## Use Case Authors:

China Mobile, Huawei, VDF, ZTE, VMWare

[NOTE: More participants are welcome.](#)

## Description:

### Business Driver:

It is the general demand for big Operators such as CMCC and Vodafone to build high-bandwidth, flat and super high-speed OTN (Optical Transport Network) facing with the transition to digital economy and information-based society. They also want to provide a high-speed, flexible and intelligent service for high-value customers, and an instant and flexible VPN service for SMB companies.

Furthermore, Operators want to be able to offer International end-to-end services to their Enterprise Customers. The ability to collaborate and interwork across Carriers is of paramount importance in such scenarios.

The current SOTN has some obvious disadvantages, such as:

- Manual labor is highly needed in service scheduling and resource maintenance which is time-consuming and costly.
- With the high demand for large bandwidth in private line, the expansion to OTN is required. The network needs to be reconstructed under this condition.
- There is no bridge or platform to connect different service providers.

Also, there are urgent demands for:

- Real-time resource update.
- OTN equipment operation and scheduling for different vendors.
- Multi-constrained end-to-end route computation.
- Multi-domain end-to-end service providing.
- Multi-domain network end-to-end survivability.
- Supply SMB companies with VPN service on demand, instantly, flexibly
- Deploy VPN service by overlay mode , untouch carrier network
- "One-click open"and "One-stop", automatically deploy enterprise VPN service
- Self-service order for client-side CPE, self-delivery client-side CPE
- Provide various value-added service on client-side SD-CPE and cloud side

Considering the above aspects, we plan to make a combination of SOTN and ONAP in virtue of the strong orchestration ability of ONAP, which is called CCVPN(Cross Domain and Cross Layer VPN), to realize a unified management and scheduling of resource and services, and also to deploy services automatically. OTN super controller can be realized as a module of ONAP(SDN-C). In this way, multi-domain cooperation is achieved as well as resource and service automatically providing.

In this use case, our focus is not only restricted to resource, but also services from end to end perspective. Scenarios includes 'SOTN only', SD-WAN and end-to-end cross Carrier international private line creation. Priorities are described in the following sections.

### Function specifications include:

1. Physical network onboarding in ONAP
2. Cross-domain orchestration (multiple physical networks) : include route calculation based on abstract topology
3. Cross operator end-to-end service provisioning
4. Closed-loop reroute for Cross-domain service

### Priorities in the whole plan:

- Priority 1: Combine SOTN with ONAP, to manage and orchestrate services automatically.
- Priority 2: Cross-domain E2E Orchestration.
- Priority 3: Create the international private line (ONAP instances interconnection and interwork).
- Priority 4: SD-WAN controller is added to realize cross Layer VPN services.

### Action Phases:

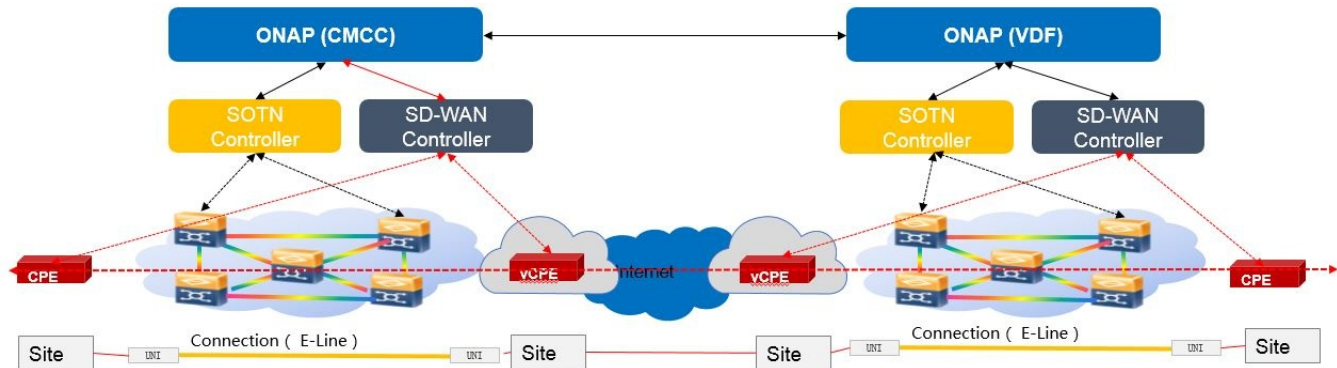
- Phase1: SOTN Orchestration
  - Single Domain
  - Multiple Domains
- Phase2: Cross Carrier Service Creation (ONAP interworking)

- Phase 3: SD-WAN service Creation

## Specific sub-use cases are:

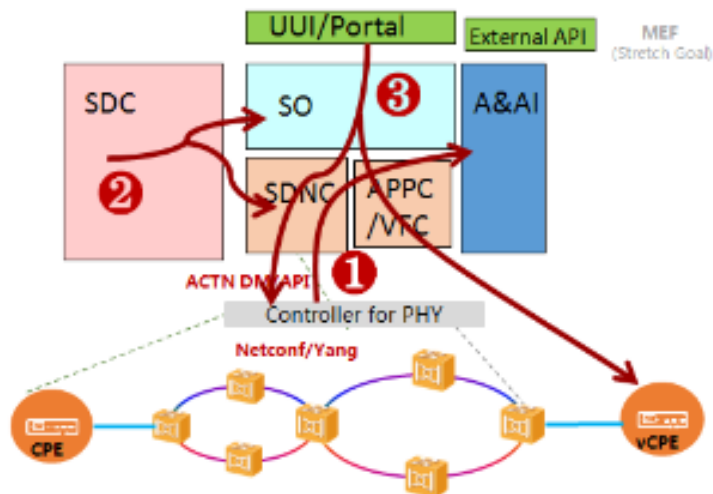
- Service and resource on-boarding
- Service configuration
- Service termination
- Self service adaptation (Bandwidth on demand *to be added*)
- Auto-scaling based on fault and performance (stretch goal)
- fault detection and auto-healing (stretch goal)
- data correlation and analytics (stretch goal)

## Overall Topology Diagram



## Work Flows

### Phase1:



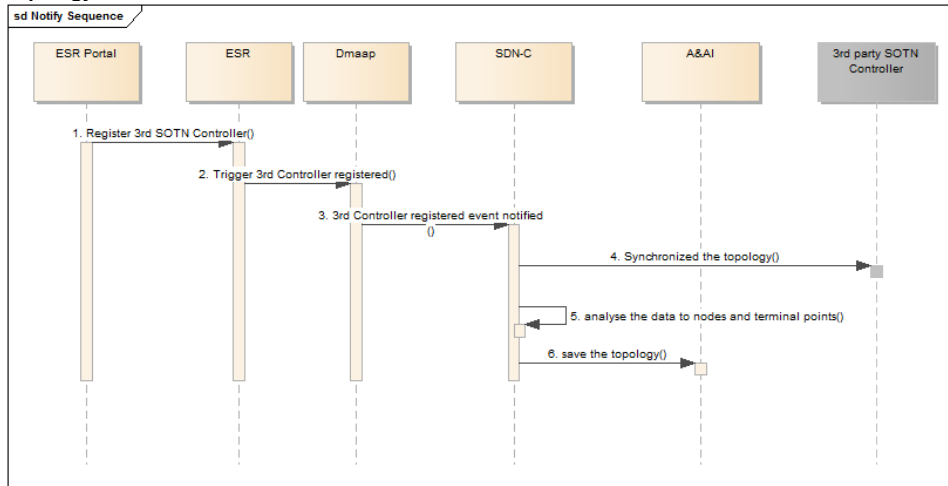
### Short description

Following a successful ONAP deployment, Customers can order CCVPN services via a customer self-service portal. ONAP orchestrator will forward requests to 3<sup>rd</sup> party SOTN Controller upon successful check of service request and OTN resource state. Afterwards, a private channel is built. Domain controller will finish resource configuration on the basis of ONAP request.

For The CCVPN use case, 4 services are designed: SOTN VPN Infra Service, SD-WAN VPN Infra Service, Site DC Service, Site Enterprise Service.

One CCVPN scenario, may contain one SOTN VPN Infra Service, more than one SD-WAN VPN Infra Services, more than one Site DC Services, more than one Site Enterprise Services. Likewise, each SD-WAN VPN Infra Service can attach more than one site.

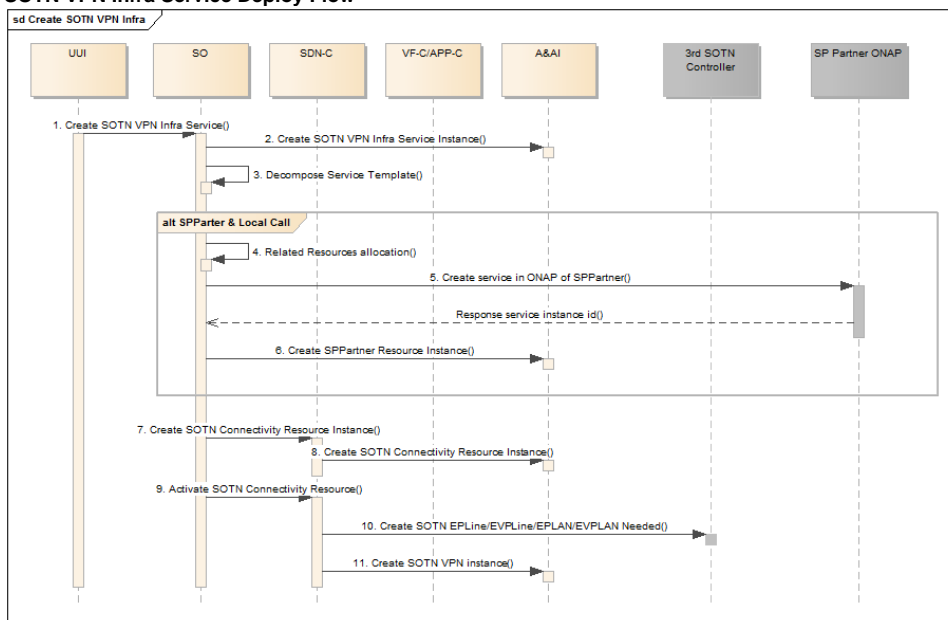
## 1. Topology Notification flow



1. Register the 3rd party SOTN Controller to ESR.
2. ESR trigger a 3rd Controller registered event to Dmaap.
3. SDNC subscribe the event and this event notified .
4. SDNC synchronize the topology from 3rd SOTN controller.
5. SDNC analyse the data from 3rd SDN controller. Get the nodes, links, terminal points of the topology.
6. SDNC call A&AI to create the nodes, links terminal points to save the topology.

Note: For multi 3rd SDN controllers, there will be several topologies notified. The links across the domain topology should be discovered or created by ONAP.

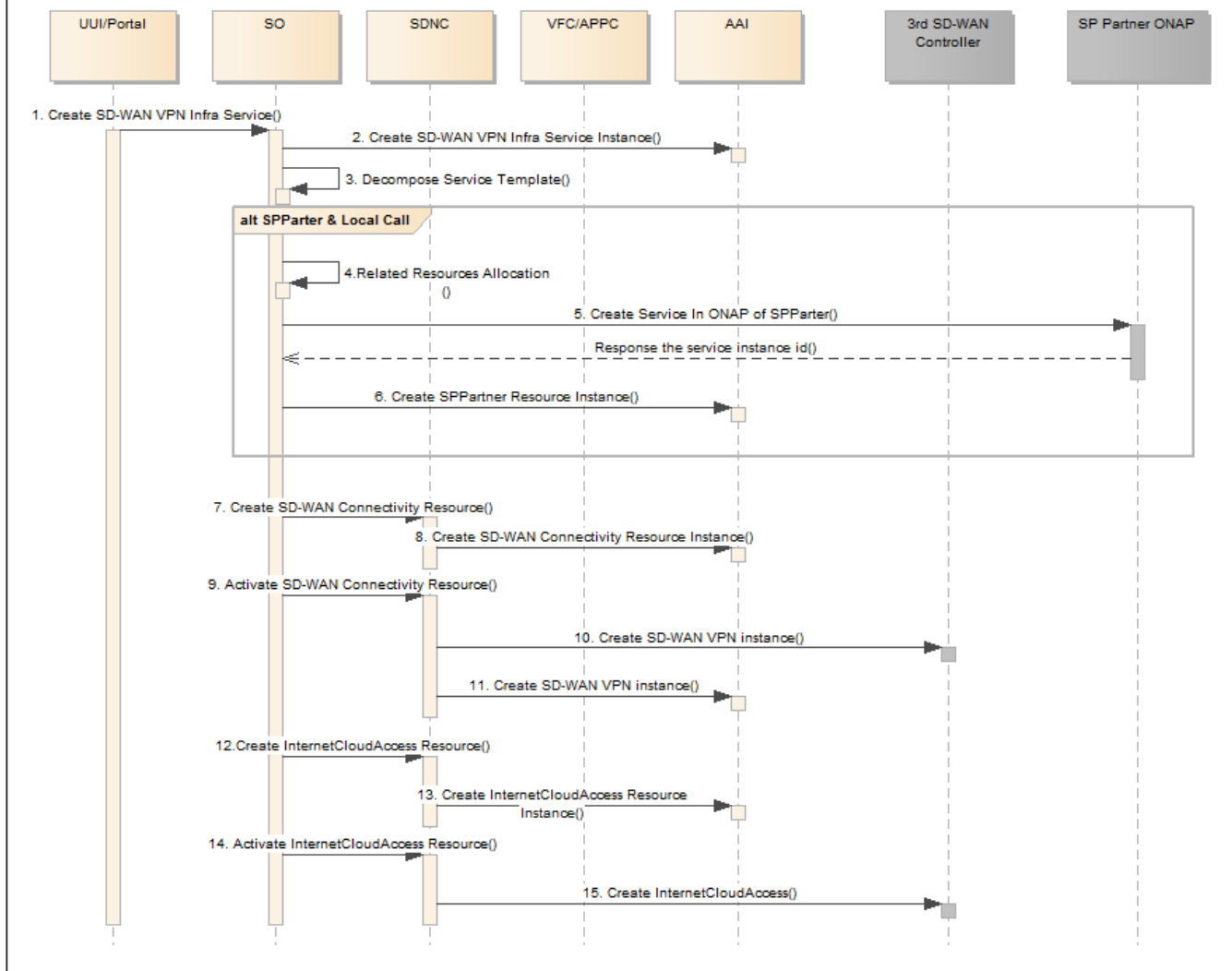
## 2. SOTN VPN Infra Service Deploy Flow



- 1. UII create SOTN VPN Infra Service
- 2. SO create service instance to A&AI
- 3. SO decompose the service template.
- 4. SO allocate the resources needed by cross ONAP deploy.
- 5. SO call the East/West APIs of ONAP of service provider partner, to create the service in the partner side.
- 6. SO create SPPartner resource information in A&AI. this will maintain the service instance uuid from the partner side.
- 7. SO call SDN-C to create SOTN connectivity resource.
- 8. SDN-C create SOTN connectivity resource instance in A&AI.
- 9. SO call SDN-C to activate SOTN connectivity resource.
- 10. SDN-C call 3rd party SOTN controller to create SOTN VPN instance if it is needed. For EPLLine/EVPLLine ,this operation is not needed here. For EPLAN/EVPLAN, it is needed to create a VPN with no UNIs in the 3rd SOTN controller.
- 11. SDN-C call A&AI to create SOTN VPN Instance, the instance will be related to VPN resource instance.

## 3. SD-WAN VPN Infra Service Deploy Flow

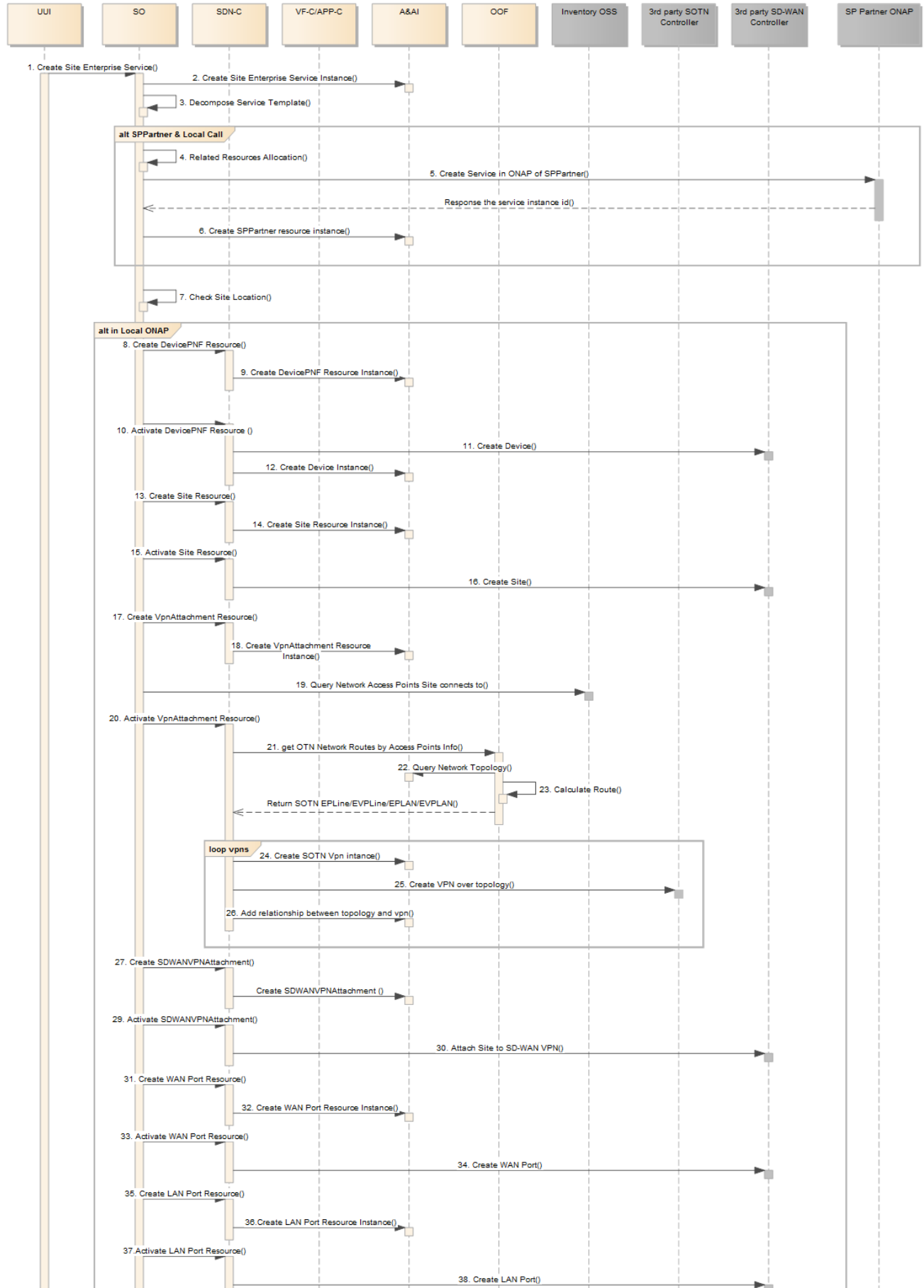
### sd Create SD-WAN VPN Infra



- 1. UUI create SD-WAN VPN Infra Service
- 2. SO create service instance to AAI
- 3. SO decompose the service template.
- 4. SO allocate the resources needed by cross ONAP deploy.
- 5. SO call the East/West APIs of ONAP of service provider partner, to create the service in the partner side.
- 6. SO create SPPartner resource information in A&AI. this will maintain the service instance uuid from the partner side.
- 7. SO call SDN-C to create SD-WAN connectivity resource
- 8. SDN-C call AAI to create SD-WAN connectivity resource instance
- 9. SO call SDN-C to activate the SD-WAN connectivity resource
- 10. SDN-C call 3rd party SD-WAN controller to create the SD-WAN VPN instance.
- 11. SDN-C save the SD-WAN VPN instance information from 3rd party SD-WAN controller to A&AI.
- 12. SO call SDN-C to create internet cloud access resource.
- 13. SDN-C call A&AI to create internet cloud access resource instance.
- 14. SO call SDN-C to activate the internet cloud access resource.
- 15. SDN-C call 3rd SD-WAN controller to create internet cloud access.

### 3. Site Enterprise Service Deploy Flow

# sd Create Site Enterprise

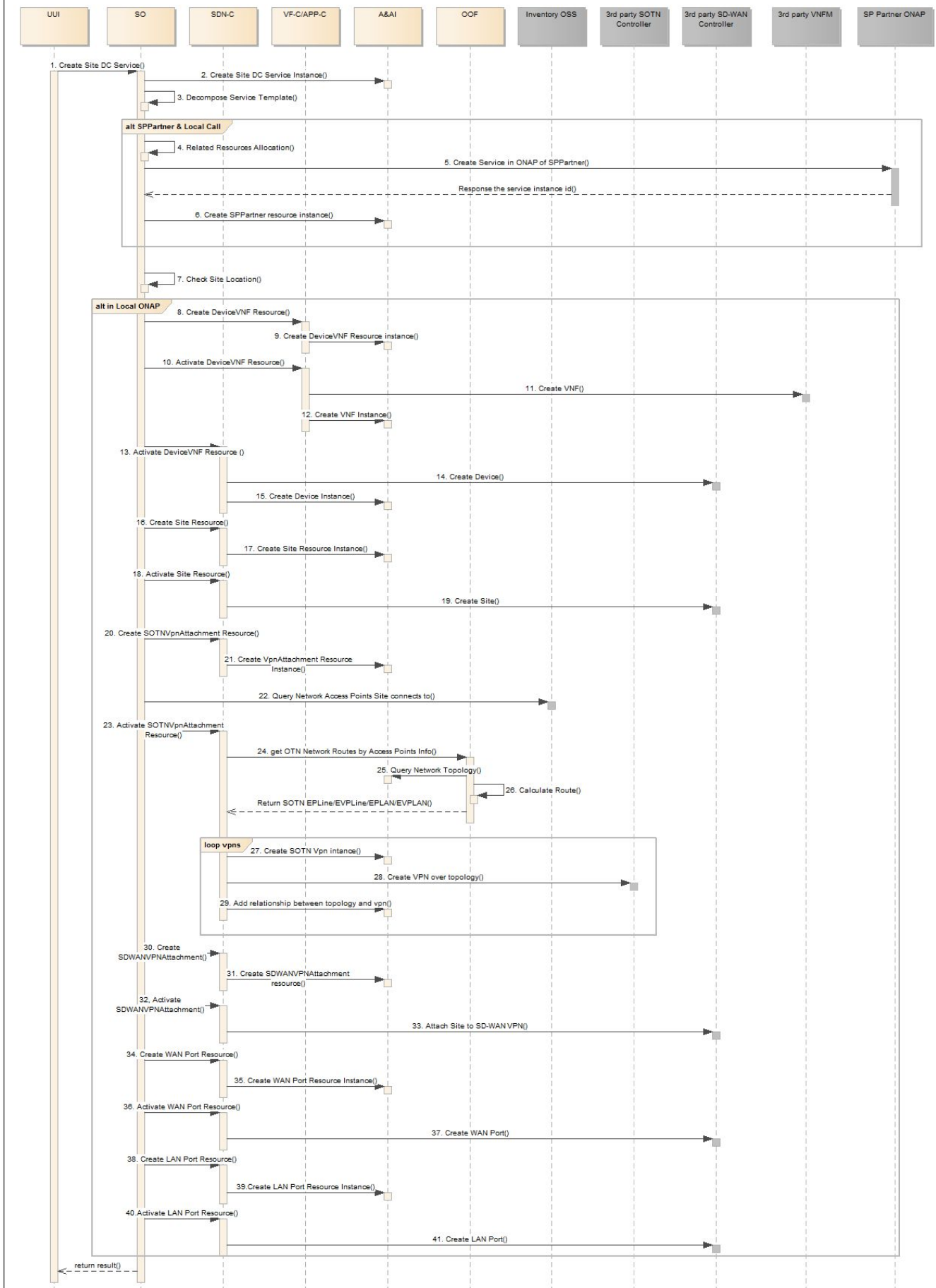




- 1. UI create Site Enterprise Service
- 2. SO create service instance to A&AI
- 3. SO decompose the service template.
- 4. SO allocate the resources needed by cross ONAP deploy.
- 5. SO call the East/West APIs of ONAP of service provider partner, to create the service in the partner side.
- 6. SO create SPPartner resource information in A&AI. this will maintain the service instance uuid from the partner side.
- 7. SO Check the site location to check if it is locate in local ONAP.
- 8. SO call SDN-C to create device PNF resource
- 9. SDN-C call A&AI to create device PNF resource instance
- 10. SO call SDN-C to activate the device PNF resource
- 11. SDN-C call 3rd party SD-WAN controller to create device of the site.
- 12. SDN-C create device instance in A&AI.
- 13. SO call SDN-C to create site resource.
- 14. SDN-C call A&AI to create site resource instance.
- 15. SO call SDN-C to activate the site resource.
- 16. SDN-C call 3rd SD-WAN controller to create site.
- 17. SO call SDN-C to create SOTN VPN attachment resource.
- 18. SDN-C call A&AI to create SOTN VPN attachment resource.
- 19. SO query the network access point information from inventory OSS of SP.
- 20. SO call SDN-C to activate the VPN attachment resource. SDN-C will get the existing VPN Infra Service information and the VPN attachment resource , to get the L1/L2 connectivity needed.
- 21. SDN-C call OOF to do L1/L2 connectivity route calculate between multi 3rd SOTN controller topologies.
- 22. OOF will query AAI for the whole topology notified by multi SOTN controllers.
- 23. OOF do route calculate,OOF return the route informations for L1/L2 connectivity VPNs on each SOTN controller.
- 24. SDN-C will loop the VPNs , and create the SOTN VPN instance to A&AI. This will also update the VPN Infra service instance.
- 25. SDN-C call 3rd SOTN controller to create VPN over topology.
- 26. SDN-C add relationship between the VPN instance and the topology.
- 27. SO call SDN-C to create SD-WAN VPN attachment resource
- 28. SDN-C call A&AI to create SD-WAN VPN attachment resource instance.
- 29. SO call SDN-C to activate the SDN-WAN VPN attachment resource.
- 30. SDN-C call SD-WAN controller to attach the site to the SD-WAN VPN instance.
- 31. SO call SDN-C to create WAN port resource.
- 32. SDN-C call A&AI to create WAN port resource instance.
- 33. SO call SDN-C to activate WAN port resource.
- 34. SDN-C call SD-WAN controller to create WAN port for the Site.
- 35. SO call SDN-C to create LAN port resource.
- 36. SDN-C call A&AI to create LAN port resource instance.
- 37. SO call SDN-C to activate LAN port resource.
- 38. SDN-C call SD-WAN controller to create LAN port for the Site.

#### 4. Site DC Service Deploy Flow

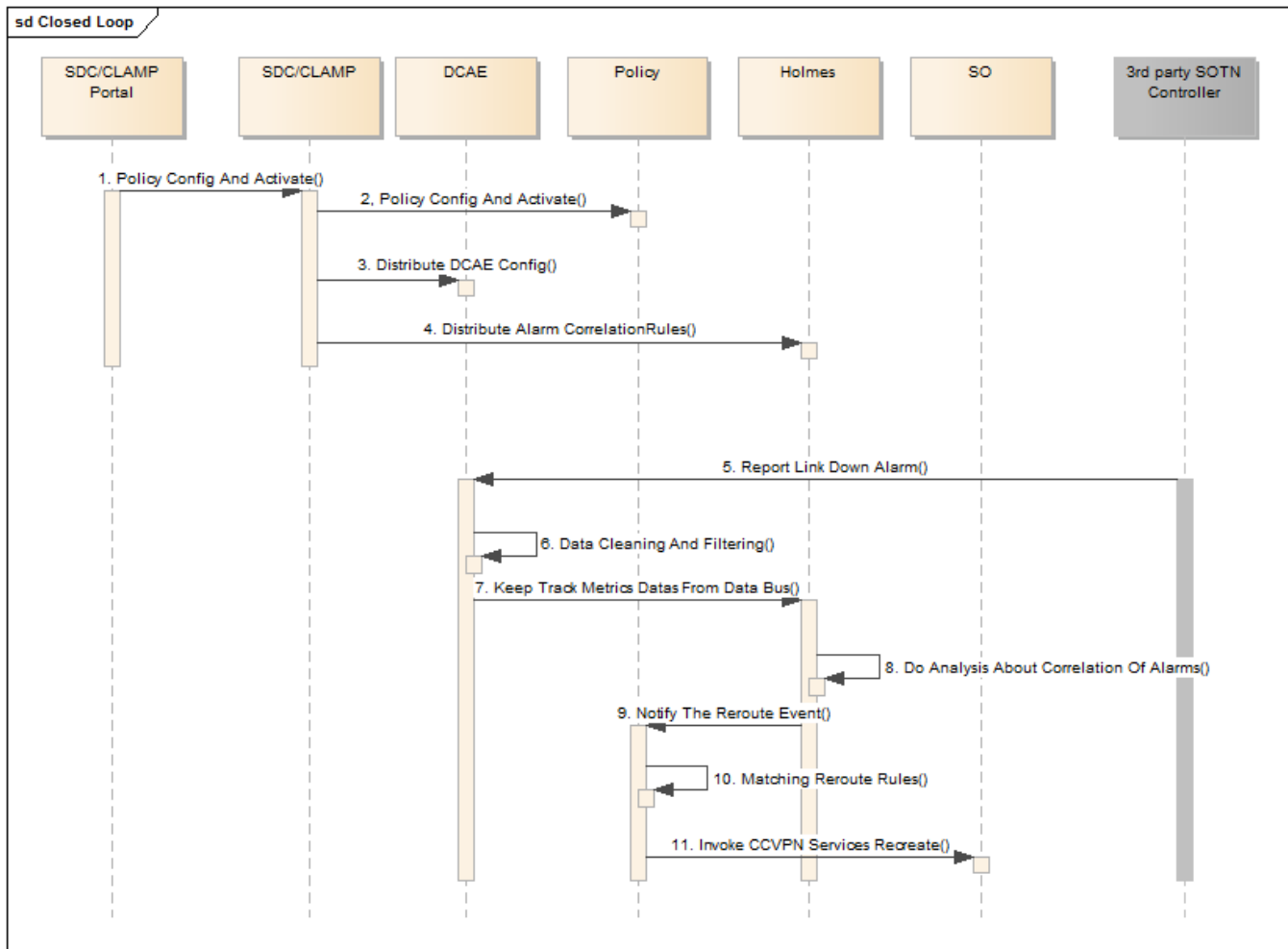
## sd Create Site DC



- 1. UII create Site Enterprise Service
- 2. SO create service instance to A&AI
- 3. SO decompose the service template.
- 4. SO allocate the resources needed by cross ONAP deploy.
- 5. SO call the East/West APIs of ONAP of service provider partner, to create the service in the partner side.
- 6. SO create SPPartner resource information in A&AI. this will maintain the service instance uuid from the partner side.
- 7. SO Check the site location to check if it is locate in local ONAP.
- 8. SO call VF-C/APP-C to create device VNF resource
- 9. VF-C/APP-C call A&AI to create device VNF resource instance
- 10. SO call VF-C/APP-C to activate the device VNF resource.
- 11. VF-C/APP-C call the 3rd party VNFM to deploy VNF.
- 12. VF-C/APP-C call A&AI to create VNF instance.
- 13. SO call SDN-C to activate the device VNF resource
- 14. SDN-C call 3rd party SD-WAN controller to create device of the site.
- 15. SDN-C create device instance in A&AI.
- 16. SO call SDN-C to create site resource.
- 17. SDN-C call A&AI to create site resource instance.
- 18. SO call SDN-C to activate the site resource.
- 19. SDN-C call 3rd SD-WAN controller to create site.
- 20. SO call SDN-C to create SOTN VPN attachment resource.
- 21. SDN-C call AAI to create SOTN VPN attachment resource.
- 22. SO query the network access point information from inventory OSS of SP.
- 23. SO call SDN-C to activate the VPN attachment resource. SDN-C will get the existing VPN Infra Service information and the VPN attachment resource , to get the L1/L2 connectivity needed.
- 24. SDN-C call OOF to do L1/L2 connectivity route calculate between multi 3rd SOTN controller topologies.
- 25. OOF will query AAI for the whole topology notified by multi SOTN controllers.
- 26. OOF do route calculate,OOF return the route informations for L1/L2 connectivity VPNs on each SOTN controller.
- 27. SDN-C will loop the VPNs , and create the SOTN VPN instance to A&AI. This will also update the VPN Infra service instance.
- 28. SDN-C call 3rd SOTN controller to create VPN over topology.
- 29. SDN-C add relationship between the VPN instance and the topology.
- 30. SO call SDN-C to create SD-WAN VPN attachment resource
- 31. SDN-C call A&AI to create SD-WAN VPN attachment resource instance.
- 32. SO call SDN-C to activate the SDN-WAN VPN attachment resource.
- 33. SDN-C call SD-WAN controller to attach the site to the SD-WAN VPN instance.
- 34. SO call SDN-C to create WAN port resource.
- 35. SDN-C call A&AI to create WAN port resource instance.
- 36. SO call SDN-C to activate WAN port resource.
- 37. SDN-C call SD-WAN controller to create WAN port for the Site.
- 38. SO call SDN-C to create LAN port resource.
- 39. SDN-C call A&AI to create LAN port resource instance.
- 40. SO call SDN-C to activate LAN port resource.
- 41. SDN-C call SD-WAN controller to create LAN port for the Site.

## 5. Closed Loop Flow

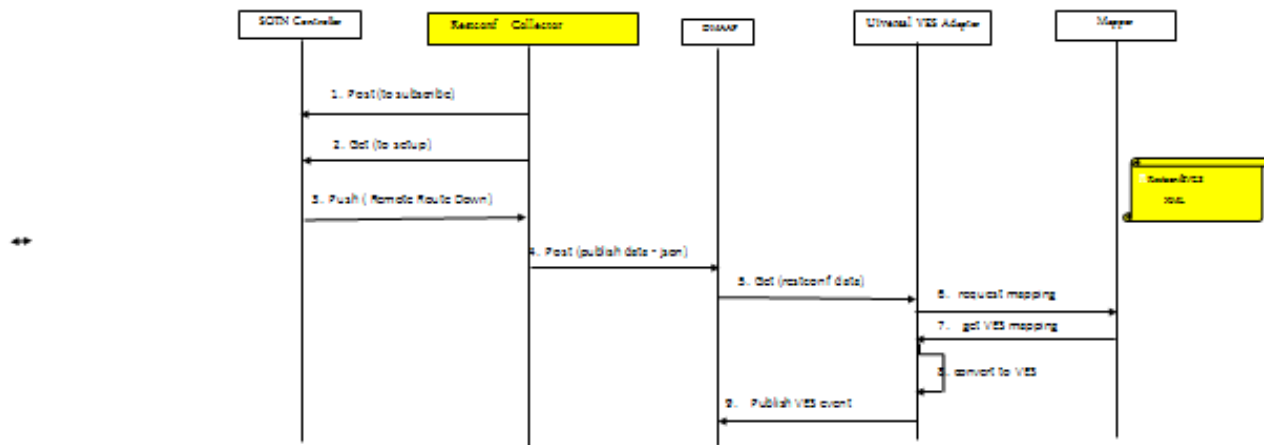




- 1. SDC/CLAMP Portal design and activate policy.
- 2. SDC/CLAMP config and activate the policy.
- 3. SDC/CLAMP distribute the DCAE config.
- 4. SDC/CLAMP distribute the alarm correlation rules to Holmes.
- 5. 3rd party SOTN controller report link down alarm to DCAE
- 6. DCAE will do data cleaning and filtering for the alarms
- 7. DCAE keep track the datas.
- 8. Holmes do analysis for the alarms.
- 9. Holmes notify the reroute event.
- 10. Policy matching the reroute rules.
- 11. Policy call SO to delete the old services and create the new services. For the creation flow, a variable route will be recalculated.

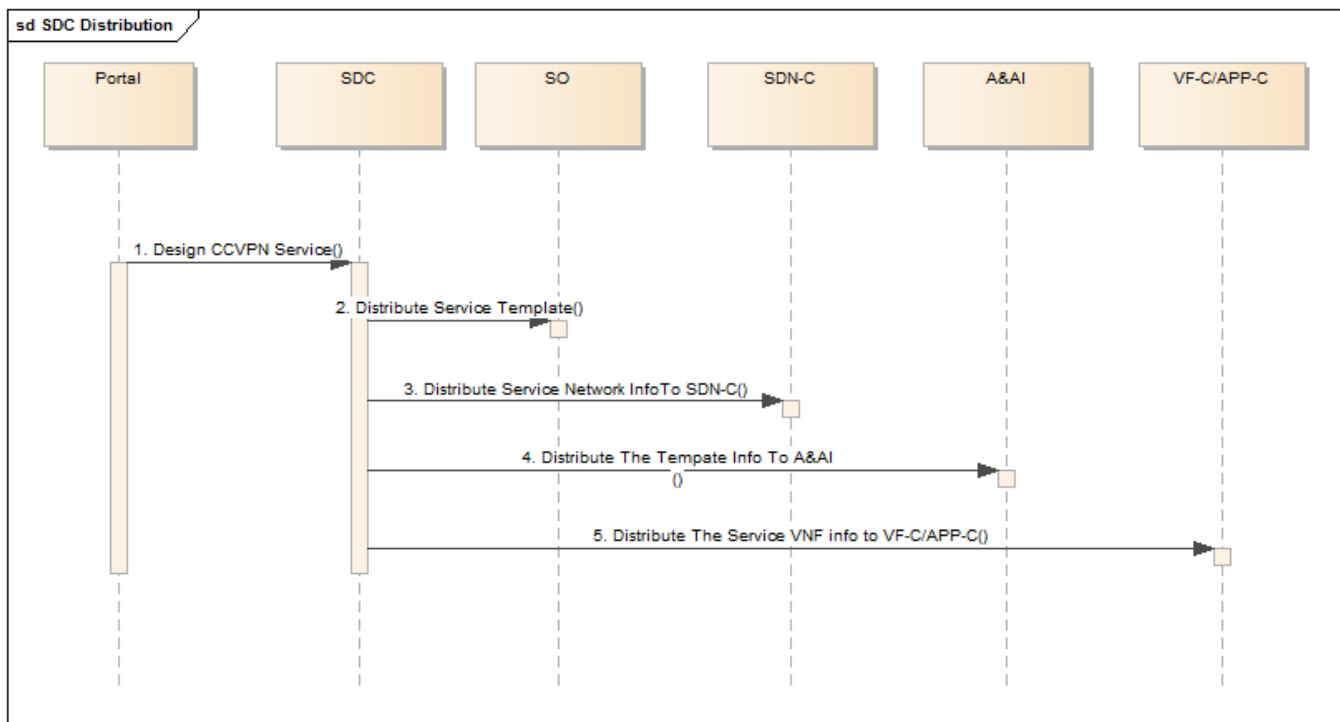
#### 5.1 DCAE Flow in Close Loop (with better diagram later on)

# SOTN Data Collection



1. RestConf Collector (RC) subscribes for remote failure alarm to SOTN Controller (SC)
2. RC requests to set up a long term tunnel with the 3rd party SC
3. SC responds with OK upon successful tunnel setting
4. SC pushes service route status data to the collector
5. RC receives alarm data, converts it into JSON format and publishes on DMAAP with topic of ROUTE\_ALARM\_OUTPUT
6. UVA consumes the alarm message
7. UVA requests the RestConf2VES mapping
8. UVA converts json alarm into VES event
9. UVA publishes the VES event on DMAAP for further correlation

## 6. Service Design Flow



- 1. Design the service in SDC portal
- 2. SDC distribute the service information to SO
- 3. SDC distribute the service network information to SDNC
- 4. SDC distribute the service model information to AAI
- 5. SDC distribute the service VNF information to VFC/APPC.

## Platform Requirements

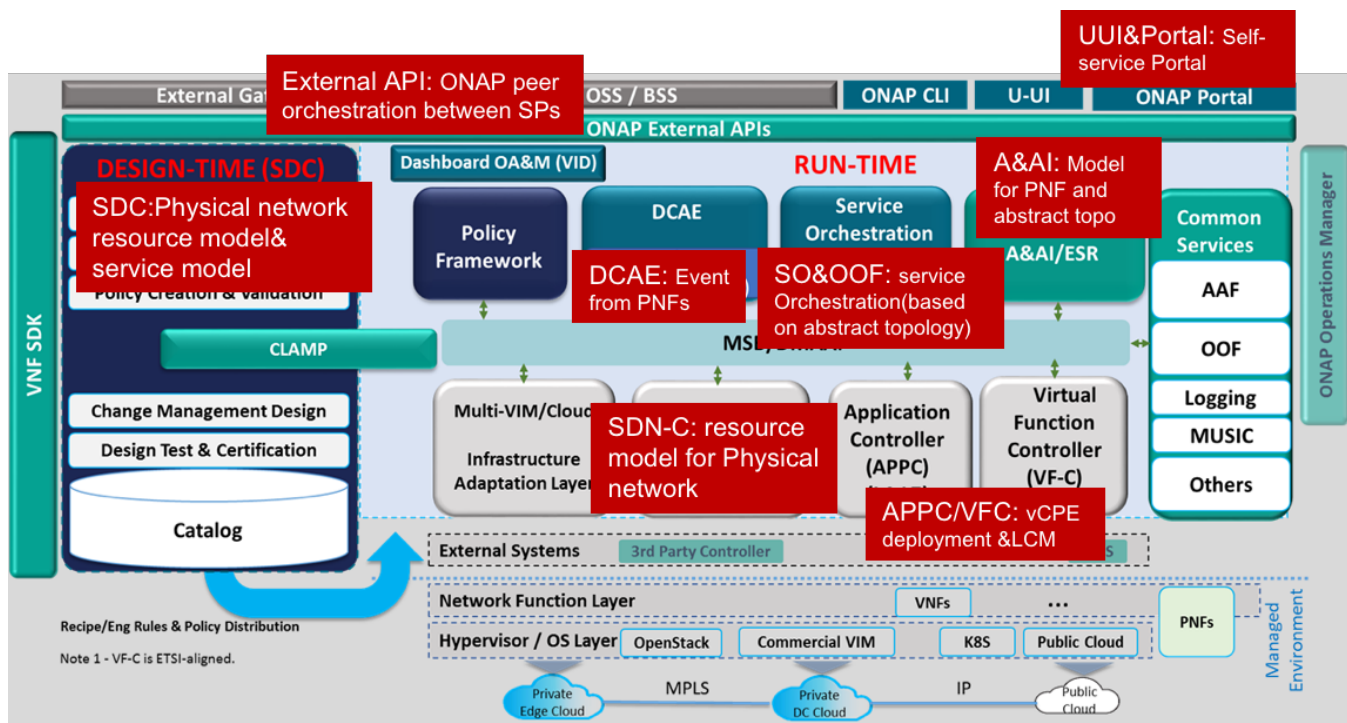
PNF Onboard (abstract topology)

Deploy Artifacts for physical network

Cross-Operators interwork (MEF etc.)

Tenant management

## Project Impact



### PHASE1:

- **SDC** – PNF resource onboarding (include: CPE and physical network which can provide MEF EPL service and can be designed as abstract resource)
- **SO/OOF** – service orchestration & homing based on abstract topology (for the physical network)
- **SDNC** - integrated with 3<sup>rd</sup> controller, New DG for provision to CPE & physical network, sync abstractor topology for the physical network and store it into A&AI
- **UUI** - E2E service provision (need support for tenant & site)
- **A&AI** - DM for PNF, abstract topology of physical network, use travel query for all resource related to special service
- **ESR** - external controller? OTN controller in phase 1?, external inventory OSS to provide reference between physical location information and CPE or UNI/NNI of physical network, or external link between different physical network domain (stretch goal)
- **DCAE** - collect the event data for MEF EPL service or from PNF.
- **VF-C/APPC** – VNF deployment & management when need
- **External APIs** - external controller? OTN controller in phase 1?, external inventory OSS to provide reference between physical location information and CPE or UNI/NNI of physical network, or external link between different physical network domain (stretch goal)
- **Modeling** - the modeling for PNF and abstract topology for physical network

## PHASE2+:

- **ESR** - SD WAN controller & external OSS: inventory/order etc.
- **External API** - cross operator's service interwork
- **Policy** - E2E close-Loop for cross domain service

## Priorities (TBD)

### PNF:

CPE: customer premises equipment, the equipment located at an end-user's premises, can be configure or managed via CLI or controller.

Physical network: a SDN network that can provide E2E MEF EPL service to ONAP, it can be multi-layer network, an 3<sup>rd</sup> controller can separate the control plane and the forward plane, and will handle the instantiation and LCM of EPL under the command from ONAP, and provide abstract topology to ONAP to facility the homing calculation.

Location	PNFs	Intended Provider	PNF CSAR
Site	CPE	Huawei, ZTE	
Physical network	OTN network element	Huawei, ZTE	

### VNF:

VNF: vCPE or similar VNF/APP that need to deploy in site (the enterprise or the Datacenter).

NFVI+VIM: provide infrastructure to run VNF/app.

Location	VNFs	Intended Provider	VNF CSAR
enterprise	vCPE	Huawei?ZTE	
Datacenter			

NFVI+VIM:

Utilize vendors NFVI+VIMs in the ONAP platform.

Location	NFVI+VIMs	Intended Provider	Note
Datacenter		Huaiwei, VMWare	

## Work Commitment

< identify who is committing to work on this use case and on which part>

Work Item	ONAP Member Committed to work on CCVPN
Modeling	CMCC, VDF, Huawei, Verizon
SDC	Huawei
SO	Huawei
OOF	Huawei
SDN-C	CMCC, Huawei

UUI	CMCC, Huawei
DCAE	Huawei
VF-C	Huawei
A&AI	Huawei
External API	Huawei

Attachments:

File	Modified
PNG File sotn use case.png	May 15, 2018 by LIN MENG
PNG File sotn.png	May 15, 2018 by LIN MENG
PNG File phase1workflow.png	May 15, 2018 by LIN MENG
PNG File project impact.png	May 16, 2018 by LIN MENG
PNG File image2018-5-28_17-46-30.png	May 28, 2018 by Chuanyu Chen
PNG File image2018-5-28_18-16-27.png	May 28, 2018 by Chuanyu Chen
PNG File image2018-5-31_17-53-6.png	May 31, 2018 by jianguo zeng
PNG File image2018-5-31_17-54-32.png	May 31, 2018 by jianguo zeng
PNG File image2018-6-4_14-36-9.png	Jun 04, 2018 by Chuanyu Chen
PNG File image2018-6-12_14-12-5.png	Jun 12, 2018 by Chuanyu Chen
PNG File image2018-6-12_14-13-12.png	Jun 12, 2018 by Chuanyu Chen
PNG File image2018-6-12_14-29-25.png	Jun 12, 2018 by Chuanyu Chen
PNG File image2018-6-12_14-44-58.png	Jun 12, 2018 by Chuanyu Chen
PNG File image2018-6-12_14-49-45.png	Jun 12, 2018 by Chuanyu Chen
PNG File image2018-6-12_14-55-59.png	Jun 12, 2018 by Chuanyu Chen
PNG File image2018-6-12_16-15-57.png	Jun 12, 2018 by LIN MENG
PNG File image2018-6-12_16-17-47.png	Jun 12, 2018 by LIN MENG
PNG File image2018-6-28_10-29-16.png	Jun 28, 2018 by Chuanyu Chen
PNG File image2018-6-28_10-40-5.png	Jun 28, 2018 by Chuanyu Chen
PNG File image2018-6-28_10-52-20.png	Jun 28, 2018 by Chuanyu Chen
PNG File image2018-6-28_10-53-48.png	Jun 28, 2018 by Chuanyu Chen
PNG File image2018-6-28_11-0-53.png	Jun 28, 2018 by Chuanyu Chen
PNG File image2018-6-28_11-7-2.png	Jun 28, 2018 by Chuanyu Chen
PNG File image2018-6-28_11-7-19.png	Jun 28, 2018 by Chuanyu Chen
PNG File image2018-6-28_11-7-31.png	Jun 28, 2018 by Chuanyu Chen
PNG File image2018-6-28_11-8-49.png	Jun 28, 2018 by Chuanyu Chen

PNG File image2018-6-28_11-13-30.png	Jun 28, 2018 by Chuanyu Chen
PNG File image2018-6-28_11-21-2.png	Jun 28, 2018 by Chuanyu Chen
PNG File image2018-6-28_11-22-34.png	Jun 28, 2018 by Chuanyu Chen
PNG File image2018-6-28_11-43-44.png	Jun 28, 2018 by Chuanyu Chen
PNG File image2018-6-28_11-50-39.png	Jun 28, 2018 by Chuanyu Chen
PNG File image2018-6-28_11-52-16.png	Jun 28, 2018 by Chuanyu Chen
File Add Personal Space....url	Jul 26, 2018 by Min Sang Yoon
PNG File image2018-7-26_17-39-16.png	Jul 26, 2018 by Xin Miao
PNG File image2018-7-30_23-16-9.png	Jul 31, 2018 by Xin Miao
File DoCreateNetworkInstance.bpmn	Sep 11, 2018 by Zhuoyao Huang
JPEG File topo for CCVPN UseCase.JPG	Dec 09, 2021 by Ahila P

[Download All](#)