|  |
| --- |
| Comment Resolution for CID# Regarding virtual access network instantiation procedure |
| Date: 2016-09-30 |
| **Authors:**  |
| Name  | Affiliation  | Phone  | Email  |
| Yonggang Fang | ZTE TX |  | yfang@ztetx.com |
| Bo Sun | ZTE |  | sun.bo1@zte.com.cn |
| He Huang | ZTE |  | He.huang@zte.com.cn |
| Fumei Liu | ZTE |  | Liu.fumei@zte.com.cn |
| **Notice:**This document does not represent the agreed view of the OmniRAN TG It represents only the views of the participants listed in the ‘Authors:’ field above. It is offered as a basis for discussion. It is not binding on the contributor, who reserve the right to add, amend or withdraw material contained herein.  |
| **Copyright policy:**The contributor is familiar with the IEEE-SA Copyright Policy <<http://standards.ieee.org/IPR/copyrightpolicy.html>>.  |
| **Patent policy:** The contributor is familiar with the IEEE-SA Patent Policy and Procedures:<[http://standards.ieee.org/guides/bylaws/sect6-7.html#6](http://standards.ieee.org/guides/bylaws/sect6-7.html)> and <[http://standards.ieee.org/guides/opman/sect6.html#6.3](http://standards.ieee.org/guides/opman/sect6.html)>. |

Abstract

This document provides the comment resolution for access network setup procedure in Recommended Practice specification of IEEE 802.1CF D0.3 to address the technical comment of omniRAN-16/00xx.

**Proposed Text Changes:**

Instruction to Editor:

Please replace the text of sub-cause of IEEE802.1CF D0.2 omniRAN specification with the following text.

------------- Begin Text Changes ---------------

## Virtual access network Instantiation and release procedure

### Introduction

In dense deployment scenarios, like shopping malls, airports, stations, or office buildings, often multiple ANs are installed to serve various needs for building management, public access, and corporate networking. Coverage areas of these ANs are widely overlapping, which creates challenges due to interference and congestion in the shared radio resource. To make the operational challenges of multiple overlapping ANs more manageable, and to reduce installation and operation cost, access network operators might consider sharing the access networks.

A single IEEE 802 access network infrastructure can be shared among multiple access network operators by creation of virtual access networks for each of the operators. Effectively all functions of multiple access networks can be established through multiple instances on the same hardware, e.g., virtual LANs on bridges or virtual Access Points on IEEE 802.11 hardware.

A virtual access network (VAN) is a software defined access network which is associated with a service provider. A virtual access network is implemented through the virtualized network function modules, which encapsulate physical functions and offer the common software interfaces to other functional modules of the virtual access network. A service provider is expected to operate the virtual access network in the same way as the real dedicated access network.

The virtualized AN approach is different from a roaming scenario in that each access network operator has full access to their virtual slice of the access network infrastructure, instead of allowing users of different service providers to connect to the same AN.

A virtual access network is represented by an instance which is created dynamically by the NFV orchestrator, when there is a need to establish a virtual access network for a service provider.

Before operating such a virtualized AN, the virtual AN has to be instantiated. The access network infrastructure requires an orchestrator with the possibility to create multiple instances of the NMS, the ANC, the NAs, and the backhaul connectivity. The orchestrator has not only to create the virtual network entity instances but also has to establish the connections between the network entities to establish an instance of a virtual AN. In addition, the orchestrator has to set up the connectivity between the virtual AN and its subscription services and access routers.

The virtual access network instantiation defines the procedure of creating a virtual environment for operating the virtual access network, including

* Creation of virtual access network instance: according to the configuration parameters in the V-NMS, the AN orchestrator creates an instance of virtual AN (V-AN) associated with the V-NMS, including one instance of virtual ANC (V-ANC); one or more instances of virtual NA (V-NA); one or more instances of virtual BH (V-BH).
* Initialization of virtual AN instances: once the V-AN is created, the instance of V-NMS communicates with the instance of V-ANC to initialize and configure the V-ANC and the attached virtual network entities, V-NA and V-BH.

The virtual access network instantiation does not include the instantiation of network entities: CIS, SS, and AR as they may be out of the access network depending on the implementation and deployment. If those network entities are virtualized, such instantiation are performed by external means, which is out of scope of this specification. However, the instantiation of such network entities may be managed and controlled by the same NFV orchestrator if they share the same physical computing resources.

The virtual access network instantiation may include the instantiation of NMS if it is a part of access network, depending on the implementation and deployment case. Through the MMI, or pre-configuration, the NFV orchestrator of access network creates an instance of virtual NMS (V-MNS) which is a software entity used to communicate with the service provider and manage the virtual access network operation.

The virtual access network initialization may follow similar procedure described in chapter 7.1.4

### Roles and Identifiers

The virtual access network instantiation involves creation of virtual network functions of access network entities controlled by the NFV orchestrator.



Figure 8.1 virtual access network and network function virtualization

The role of each virtual access network entity is represented and performed through the virtual functions which are described below.

#### NFV Orchestrator

The network function virtualization is managed through NFV management and orchestration (MANO). The MANO orchestrator is responsible for creating a network function packages of new service; lifecycle managing resources; validating and authorizing NFVI resource requests.

#### Virtual Access Network

AN is defined in section 6.5. In a virtualized environment, the entire AN(s) can be modeled as one or multiple logical entities of access networks, i.e. instance(s) of virtual access networks. Each virtual AN may consist one instance of V-ANC, one or more instances of V-NAs, and one or more instances of V-BHs.

The entire virtual AN is under control of the NFV orchestrator, which manages the creation of instance of V-AN on the shared hardware infrastructure. The V-AN instance has its identifier and access network identifiers (e.g. ESSID).

#### Virtual Access Network Control

A physical Access Network Control (ANC) is defined in the section 6.5. The virtual ANC instance represents the functions of physical access network control entity for the service provider in the virtual environment. It has an instance ID for identifying its self in communicating with other instances of virtual access network; a network identifier, and virtual network interfaces towards V-NMS, SS and CIS.

#### Virtual Node of Attachment

A physical Node of Attachment (NA) is defined in the section 6.5. In the virtual access networks, an NA is represented through a software instance of V-NA. A V-NA instance has an instance ID which is used for identifying itself in the communication with other virtual access network entity instances. Like a real NA, a V-NA has its own individual network identifier (SSID) shared with other V-NAs, an unique air interface identifiers (virtual BSSID), Association ID (AID) and/or Color Code (CC) of the virtual access network associated to a service provider.

Multiple instances of V-NAs may be created on the same NA hardware, each of which is associated to one service provider. Therefore multiple service providers are allowed to operate on the same physical infrastructure and air interface through the virtual environment.

In the shared environment, some of the attributes are common to all the virtual NAs. The NFV orchestrator will validate the integrity of shared attributes.

#### Virtual Backhaul Network

A physical Backhaul (BH) is defined in the section 6.5. In the virtual access networks, a BH is represented through a software instance of V-BH which is created by NFV orchestrator. The V-BH may be implemented via VLAN or SDN to provide the virtual network dedicated to the service provider in the shared environment.

A V-BH instance has an instance ID which is used for identifying itself in the communication with other virtual access network entity instances.

### Use Cases

#### Instantiation of a new virtual access network

The instantiation of a new virtual access network for a service provide is under control of NFV orchestrator.

1. The NFV orchestrator creates instance of virtual NMS for a service provider.
2. Based on the configuration information of service provider, the NFV orchestrator creates the instance of virtual access network includes one V-ANC, one or more V-NA, and one or more V-BH, each of which represents the physical entity of access network infrastructure.
3. V-NMS manages and controls the virtual access network initiation and configuration through V-ANC.

#### Dynamically adding instances to the virtual access network

The service provider may add one or more new instances to the virtual access network, such as V-NAs or V-BHs to improve the radio coverage or increase the access network capacity according to the deployment and live traffic demanding. Therefore the virtual access network topology and capacity may dynamically change.

The service provider may add a new instance of V-NA or V-BH through V-NMS. The V-NMS then communicates with the NFV orchestrator to create a new instance of V-NA or V-BH and manage it through the V-ANC.

#### Dynamically removing instances from the virtual access network

The service provider may remove one or more instances such as V-NAs or V-BHs when the radio coverage or access network capacity is not needed according to the deployment and live traffic demanding so as to reduce the power consumption and operation cost.

The service provider can remove an instance of V-NA or V-BH through V-NMS. Once the NFV orchestrator receives the instruction from the V-NMS, it removes the instance of V-NA or V-BH and associated resources in the NFVI.

#### Removal of the entire virtual access network

There are two ways to remove the entire virtual access network:

* The service provider tear down the entire virtual access network through V-NMS.
* The NFV orchestrator autonomously removes the virtual access network when a fatal failure in the virtual access network or physical access network has been detected.

### Functional Requirements

#### Creation of multiple virtual networking entities

In the virtual access network environment, the NFV Orchestrator of access network plays an important role of controlling the virtual access network instantiation.

When the access network is powered up, the AN Orchestrator shall instruct it to search for the operating channel with less congestion or interference in that coverage area for ASA band or unlicensed band using the procedures defined in 7.1.2 and 7.1.3. Once the operating channel is determined, the AN Orchestrator can create an instance of ANC which then controls the instantiation of virtual NAs and BH of the virtual AN for the dedicated service provider over the shared hardware, operating on the selected frequency channel.

The AN Orchestrator first creates the virtual networking instances with default parameters and then establishes the connections between the networking functions to allow the virtual ANC to communicate with the service provider network for configuration information of virtualized access network entities.

#### Virtual AN Configuration

AN configuration is to provision the AN with:

* Air Interface Identifier (e.g. BSSID, AID, or CC)
* Service Network Identifier (SSID)
* Service Identifier or Session Identifier
* Security information
* Radio parameters (operating channel, channel bandwidth, contention window parameters, etc)
* Service parameters, such as QoS information

The virtual AN configuration is performed through virtual ANC created by the AN Orchestrator. Once the virtual AN is instantiated, the service provider can configure the virtual AN through the NMS like configuring the real AN.

In the case of multiple virtual ANs sharing the same infrastructure, each service provider has its own configuration parameters and can figure its virtual AN through its NMS.

If some configuration parameters (like radio interface parameters) are shared by multiple virtual ANs, those parameters should be common and same to all the service providers.

#### Multiple Service Provider support

The access network virtualization allows multiple service providers to share the physical infrastructure and has its own virtual connections to its core network over one or more access routers.

* An virtual AN SHOULD be capable to discover and join its service provider’s network through access routers, to which connectivity exists.
* Multiple virtual ANs each of which is dedicated to a service provider SHOULD be capable to be shared over the same physical access network.
* A V-AN SHOULD maintains its unique air interface identifier and access network identifiers associated with the service provider.
* A V-AN SHOULD be capable to be configured and controlled through the V-ANC by the V-MNS associated to the service provider.
* The V-BH SHOULD be able to forward the user packets of the V-AN over the designated access routers to the service provider’s network, to which the user is subscribed to.
* The NFV orchestrator SHOULD provide fair allocation of radio resources shared among multiple V-ANs which belong to different service providers.

### Detailed Procedure

#### Virtual Access Network Instantiation Procedure

Before an virtual access network instantiation, the V-NMS shall be created either by the NFV orchestrator if the NMS shares the same physical infrastructure or other means which is out of this specification.

The service provider can initiate the V-AN instantiation via issuing a command in V-NMS. Once the NFV orchestrator receive the Create V-AN, it shall validate and verify the command. If the command is verified , the orchestrator shall create an instance of V-ANC, one or more instances of V-NAs and one of more instances of V-BHs according to request. Once the V-ANC instance is created, it will discover and join the associated V-NMS.



Figure 8.2 an example of procedure for V-AN instantiation and initialization

Figure 8.2 shows an example of procedure of V-AN instantiation. The NFV orchestrator receives a Create V-AN from the V-NMS, and add instances of V-AN, including a V-ANC, V-NAs, V-BHs. In the access network shared by multiple service providers, the NFV orchestrator may create multiple V-AN instances, each of which is to associate with a service provider. After the V-ANC instance is created, it shall discover and join the V-NMS of the service provider; and perform the initialization like in the real dedicated access network.

The Create V-AN may include the following information:

* V-NMS ID
* Service Provider Identity
* Time stamp of this message

The V-AN Created message may include the following information:

* V-NMS ID
* Service Provider Identity
* V-AN ID
* Time stamp of this message
* Result code and reason

In V-AN initialization shall follow the procedure defined in 7.1.4.5 Access network setup to discover and join the V-NMS and get the configuration information to provision all the instances attached to the V-AN.

#### Virtual AN Release Procedure

There may be two ways to release the virtual AN.

* NFV orchestrator initiated V-AN release: the orchestrator autonomously requests to remove the virtual access network instances.
* Service provider initiated the V-AN release: the service provider network starts the termination of V-AN through the V-NMS.

Figure 8.3 shows an example of release procedure of virtual access network. Figure 8.3 (a) shows the procedure of virtual access network release initiated by the orchestrator. In some case like fatal failure, the NFV orchestrator initiates releasing of the entire V-AN and remove the instances of V-NAs, V-BHs and V-ANC. It then sends a Release Notification message to the V-NMS to notify the service provider.

The Release Notification message for NFV orchestrator initiated V-AN release may include

* V-AN ID
* Released V-ANC, V-NAs and V-BH IDs
* Air interface ID,
* Time stamp of this message
* Result code and reason



(a)



(b)

Figure 8.3 an example of virtual access release procedure:

(a) Orchestrator initiated V-AN release; (b) Service provider initiated V-AN release

Figure 8.3 (b) shows another example of the procedure of V-AN release initiated by the service provider. In some case, the service provider may need to release the V-AN for maintenance, upgrade, etc. The service provider can initiate a command in V-NMS to instruct the NFV orchestrator to remove the instances of V-NAs, V-BHs and V-ANC, and their associated resources for the V-AN. When receiving a Release Request message from the V-NMS, the NFV orchestrator validates the message and verifies that the request matches completely with an instance of a V-AN. Only when complete match is determined, the NFV orchestrator will remove all the instances associated to the V-AN and send the Release Response to the V-NMS.

The Release Request for Service Provider network initiated release should include

* V-AN ID
* Time stamp of this message

The Release Response for Service Provider initiated release may include

* V-AN ID
* Timestamp of this message
* Result code

#### Adding a New Instance to the V-AN Procedure



 Figure 8.4 an example of adding a new instance to V-AN

Figure 8.4 shows an example of the procedure of adding an instance to V-AN by the service provider through V-NMS. In some case, the service provider may need to add a new instance of V-NA to increase the radio coverage or air link capacity. The service provider initiates a command in V-NMS to instruct the orchestrator to add the requested instance of V-NA (or V-BH) and associated resources to the V-AN. When receiving the Add Request message from the V-NMS, the NFV orchestrator validates the message and verifies that the request matches completely with an instance of the V-AN. Only if complete match is determined and the requested instance do not collide with the operation of other V-ANs of the same access network infrastructure, the NFV orchestrator will add the instances of V-NA (or V-BH) and associated resources to the V-AN. The new added instance of V-NA (or V-BH) then sends the V-NA Added message V-ANC and the V-NMS.

#### Removal of an Instance from the V-AN Procedure



Figure 8.5 an example of removal of an instance from V-AN

Figure 8.5 shows an example of the procedure of removal of an instance from the V-AN by the service provider through its V-NMS. In some case, the service provider may need to remove an instance of V-NA to reduce the radio coverage or air link capacity when it is not needed. The service provider initiates a command in V-NMS to instruct the orchestrator to remove the requested instance of V-NA (or V-BH) and associated resources from the V-AN. When receiving the Remove Request message from the V-NMS, the NFV orchestrator validates the message and verifies that the request matches completely with an instance of a virtual AN. Only if complete match is determined, the NFV orchestrator will removes the requested instances of V-NA (or V-BH) and associated resources from the V-AN. Meanwhile the V-ANC removes the V-NA from its attachment list and indicates to the V-NMS via V-NA Removed message.

#### Update Virtual AN Configuration Procedure

After instantiation of a V-AN, the service provider may re-configure the V-AN through V-NMS to change the operation.



Figure 8.6 an example of virtual AN configuration update procedure

Figure 8.6 shows an example of procedure for V-AN re-configuration. During the normal operation of V-AN, the service provider may reconfigure the V-AN through its V-NMS. Only when the re-configuration do not collide with the operation of other V-ANs of the same access network infrastructure, the NFV orchestrator will change the configuration of the requested instances in the V-AN according to the wishes of the service provider. Otherwise the NFV orchestrator will respond with an alternative proposal to best match the required reconfiguration.

-------------- End Text Changes ----------------