|  |
| --- |
| Comment Resolution for CID#7 Regarding AN setup procedure |
| Date: 2016-06-17 |
| **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 D0.0 to address the technical comment of #7 of omniRAN-16/0006.

**Comments on D0.0:**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| CID | Category | Page | Sub-Cause | Line# | Comment | Proposed Change | Resolution |
| 7 | Technical | 25 | 7.1.4.5 | 665 | The discovery request should be sent by the AN (not the Service Provider) during the AN setup and initialization. After receiving the Discovery Request message, the Service Provider responds with the Discover response to include the information that AN needs to establish the network connection to the Service Provider network.  | Suggest to change to the original text. See a separate contribution for the change. | Revised.See detail below. |

**Discussion:**

The section 7.1.4 is to provide the setup procedure of access network (AN) over the unlicensed spectrum, including establishing the connection between the AN and Service Provider's Network, acquiring the configuration parameters of AN from the Service Provider network, and initializing the AN according to the received configuration parameters.

The comment #7 of omniRAN-16/0006 indicates that the Discovery Request message flow in 7.1.4.5.1 regarding the AN setup procedure is incorrect. We agree with this comment as for following reasons

* In the current D0.0 version, the Discovery Request message in FIG. 12 is sent by the Service Provider network to the AN Orchestrator. As the Discovery Request message is used for the AN to indicate its appearances and find the Service Provider network, it does not make sense for the Service Provider to send such message to the AN.
* The AN may be powered on at any time and the Service Provider may not know the status of AN before the basic connection is established. If the Service Provider blindly and constantly broadcasts the Discovery Request message, it would waste the network capacity and reduce the transmission efficiency. In the real deployment, it is not aware of a network implementing in such as way.
* The omniRAN as a Recommended Practice specification should reflect the real implementation and deployment scenario.

The correct message flow for Discovery Request and Response messages should be

1. The ANC is powered and sends a Discovery Request message on behalf of AN to the Service Provider network.
2. The Service Provider network sends a Discovery Response message with service network information and configuration parameters for the ANC to provision the access network.
3. After receiving the Discovery Response(s) with the configuration parameters, the ANC then can select a service provider's network and provision the network.

Based on above analysis, we agree the comments with revised resolution.

* In order to make consistent between the title of this chapter and content, the title of 7.1.4 is suggested to change to “Access network setup and release procedure”. Therefore, the access network setup procedure could be able to use the result from the radio channel allocation defined in 7.1.2 and 7.1.3.
* Add a new section 7.1.5 “Virtual access network instantiation and release procedure”. As the network virtualization and virtualized network functions are introduced in the recent proposals, it would be necessary to distinguish the basic access network setup and virtual access network instantiation, and reflect such new topic in the corresponding section. The virtual access network instantiation procedure could also be based on the result from the previous procedure of radio channel allocation defined in 7.1.2 and 7.1.3.
* The network manage system (NMS) is also discussed and added in the network reference model recently to support fault diagnosis, detection and report, and network configuration as well. As the AN setup is under control of NMS typically, it is necessary to refine the text to reflect such changes in the NRM.

**Proposed Text Changes:**

Instruction to Editor:

Please replace the text of sub-cause 7.1.4 of IEEE802.1CF D0.0 omniRAN specification with the following text.

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

### Access network setup and release procedure

#### Introduction

An IEEE 802 access network infrastructure can be operated by an access network operator over ASA spectrum or unlicensed spectrum. When the access network is powered up, it may need to search for a radio frequency channel with less congestion or interference over one or more channels in ASA or unlicensed bands using the procedures defined in 7.1.2 and 7.1.3 respectively. Once the operating channel is found, the access network shall be initialized with the configuration parameters retrieved through the NMS of service provider.

#### Roles and Identifiers

##### Node of Attachment

NA is defined in the section 6.5. NAs may consist of one or more radio interfaces for an access network operator in the basic network service model. Each NA in the basic service model has its own air interface identity (like BSSID) and the same network identifier in the AN.

##### Access Network

AN is defined in section 6.5. In the basic network service model, the AN consists of one or more NAs, one Access Network Controller (ANC) and Backhaul network (BH).

#### Use Cases

##### Access network infrastructure

In the basic network service model, an access network operator manages and operates the access network with the configuration parameters retrieved through the NMS of service provider.

#### Functional Requirements

##### Basic access network setup

The access network needs to establish the connections with the service provider network to acquire the configuration parameters for the configuration of access networks including NA backhaul network.

##### Access Network Configuration

AN configuration is the provisioning of the AN with:

* Air Interface Identity
* Service Network Identity
* Service Identity or Session Identity
* Security information
* Radio parameters.
* Service parameters, such as QoS information

The AN configuration is under the control of ANC. After the AN is powered up, the ANC communicates with the NMS of service provider network to get the configuration information and then provision the AN.

#### Detailed Procedure

##### Access Network Setup Procedure

The access network setup procedure includes

* Service network discovery
* Joining the service network

The procedure of service network discovery is used for the powered up AN to find the service provider’s network and get the service provider information and configuration parameters for the access network setup. Once the service network is found and provides the configuration parameter, the ANC would setup the access network with the configuration information retrieved from the service provider for operating the AN over the unlicensed spectrum or ASA spectrum.

The Figure 12 shows an example of procedure of access network setup. When the access network is powered up, the ANC on behalf of NAs sends a Discovery Request message to the NMS which is a part of service provider network. After receiving the Discovery Request message, the NMS sends the Discovery Response message with the service network information for the ANC to select and provision the access network.

 Figure 12 An example of access network setup procedure

The Discovery Request message may contain following information:

* ANC/NA Identity
* The Service Network to be associated
* Time stamp of this message
* Discovery type which provides the information how the AN gets the service provider’s network address, such as manual configuration, DNS server, etc.
* The capability information of physical NAs attached to the AN
* The physical backhaul capabilities

The Discovery Response message should include the following information:

* Service Provider Identity
* ANC Identifier
* Time stamp
* Access Router Interface ID
* Subscription Service Interface ID and Identity
* Radio configuration information for the required area
* Backhaul parameters to the Service Provider’s subscription service and access router such as multiple ports and addresses of the network and the load information of each port.
* Service Provider Network descriptor, such as capability (max NA number, max user number…), security information, etc.
* Service Provider’s network address list which helps NA to choose a proper port for the following communication

The Join Request message should include the following information:

* ANC or NA Identity
* The Service Network Identifier
* Time stamp of this message
* ANC or NAs location information. This helps the service provider’s network to determine whether to accept the join request
* NA descriptor, such as capability, encryption information, etc.

The Join Response message should include

* Service Provider Identifier
* ANC Identifier
* Time stamp of this message
* Result code: indicating whether the Join Request is admitted or not. If not, it lists the reason of the rejection.
* Service Provider Network descriptor, such as capability (max NA number, max user number…), security information, etc.
* Service Provider’s network address list which helps NA to choose a proper port for the following communication

##### Access Network Release Procedure

There are two ways to release the access network: access network is released by itself, or released by the service provider through the NMS.

(a)

 (b)

Figure 13 an example of access network release procedure

Figure 13a and 13b shows an example of access network release procedure. The access network could be released by the ANC (Figure 13a), or by the Service Provider through NMS (Figure 13b). In some particular case like at certain abnormal condition, the access network may have to initiate access network release under the control of ANC (Figure 13a). In such case, the ANC will notify the Service Provider through the NMS that the access network will be shut down. Either the Service Provider network responds the notification or not, the access network will release itself.

The Release Notification message may contain following information:

* ANC/NA Identity
* Service Network identifier
* Time stamp of this message

The Release Response message should include

* Service Provider Network Identity
* ANC Identifier
* Time stamp of this message
* Result code

In normal case, the access network release should be controlled by the Service Provider through the NMS. When the Service Provider needs to release the access network for maintenance, power saving, or major software/hardware upgrade, it could initiate the access network release through the NMS (Figure13b). When the ANC receives the Release Request message from the NMS, it will verify the command and start the access network release according to the requirement. The ANC will send the Release Response to the NMS about the result of access network release.

The Release Request message may contain following information:

* Service Network identifier
* ANC/NA Identity
* Time stamp of this message

The Release Response message should include

* ANC Identifier
* Service Provider Network Identity
* Time stamp of this message
* Result code

### Virtual access network Instantiation and release procedure

#### Introduction

An IEEE 802 access network infrastructure can be shared among multiple operators by the creation of virtual access networks in which each virtual access network is operating for an individual service provider. In the shared access networks, some or all functions in the access network can be established through multiple network function instances on the same hardware, e.g. Virtual LANs in bridges or virtual Access Points on IEEE 802.11 hardware.

The virtual access networks could be operated in ASA spectrum or unlicensed spectrum. When the access network is powered up, it needs to find the operating channel with less congestion or interference using the procedures defined in 7.1.2 or 7.1.3, and then perform the virtual access network establishment.

#### Roles and Identifiers

##### Virtual Node of Attachment

NA is defined in the section 6.5. In the shared network service model, a physical NA may support multiple instances of virtual NAs on the same hardware. Some of the attributes are common to all the virtual NAs, while each virtual NA has an individual network identity with its own air interface identifiers (for example, virtual BSSID) and own network identifiers.

##### 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, virtual access networks. Each virtual AN may consist one or more virtualized NAs with its own virtual ANC and BH. The entire AN(s) is under the control of the AN Orchestrator, which manages the creation of instance of virtual AN on the shared hardware infrastructure. Each virtual AN instance has its own radio network identifiers (e.g. virtual BSSID), its own ANC identifier, and its own network interfaces towards subscription services and access routers.

#### Use Cases

##### Access network infrastructure sharing

In high dense deployment scenarios, like shopping malls, airports, stations or office buildings, often multiple physical ANs are installed to serve the various needs for public, corporate and offloading usage. Coverage areas of these particular ANs are widely overlapping which creates challenges due to interference and congestion in the shared radio environment. To make the operational challenges manageable and to reduce installation and operation cost, service providers might consider sharing the access networks, which means that a single physical access network infrastructure can create multiple virtual ANs, each of which is for a service provider with dedicated connections to the service provider’s networks over the access router. The virtualized AN approach is different to a roaming scenario, which allows the each service provider share the entire access network virtually without switching network service identifier when a terminal is roaming among access networks. In order to be able to operate in such a virtualized AN environment, the virtual AN instance has to be created with virtual NAs and related backhaul connectivity over the physical access network infrastructure.

#### Functional Requirements

##### Creation of multiple virtual networking entities

In the virtual access network environment, the AN Orchestrator plays an important role of controlling the virtual access network initialization and configuration.

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 is determined, the AN Orchestrator can create an instance of ANC which then controls the operation of virtual NAs and backhaul 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 virtualized ANC to communicate with the service provider network for configuration information of virtualized access network entities.

##### Virtual AN Configuration

AN configuration is the provisioning of the AN with:

* Air Interface Identity
* Service Network Identity
* Service Identity or Session Identity
* Security information
* Radio parameters.
* Service parameters, such as QoS information

In the virtual access network, the AN configuration is performed through virtual ANC created by the AN Orchestrator. Configuration parameters for the virtual AN setup should be acquired from NMS of the service providers. In the case of multiple instances of virtual ANs on an infrastructure shared by multiple service providers, each service provider may have its own configuration parameters through its NMS. The virtualized ANs would share the common configuration of radio interface parameters and provide the same radio coverage for all the service providers.

##### Multiple Service Provider support

In the shared access network environment, a virtualized AN may be interconnected to the service provider network over one or more access routers, and multiple virtualized AN share the same physical access network infrastructure hardware. Therefore the virtual ANs SHOULD be able to provide a sharing mechanism amongst different service providers.

* An virtualized AN SHOULD be capable to discover and join its service provider’s network through access routers, to which connectivity exists.
* Multiple virtualized ANs SHOULD be capable to be shared over the physical access network by multiple service providers.
* A virtualized AN SHOULD maintains its unique air interface identifier and access network identifiers associated with the service provider.
* A virtualized AN SHOULD be capable to be configured and controlled via the virtual ANC associated to the service provider.
* The virtualized backhaul SHOULD be able to forward the user packets over the designated access routers to the service provider’s network, to which the user is subscribed to.
* The virtualized ANs SHOULD provide fair allocation of radio resource sharing among terminals belonging to different service providers.

#### Detailed Procedure

##### Virtual Access Network Setup Procedure

In the virtualized access network case, the AN Orchestrator needs to create a virtual AN instance first using default setting. Once the virtual ANC instance is initiated, the virtual ANC is then responsible for the virtual AN setup.

Figure 14 an example of procedure for the virtual AN setup

Figure 14 shows an example of setup procedure for virtual AN. The AN Orchestrator is responsible to create a virtual AN instance including virtual ANC, virtual NA(s), and virtual BH first. In shared access network model, multiple virtual AN instances may be created to associate with different service providers. After the virtual ANC instance is created, the virtual ANC takes over the virtual AN setup and sends a Discovery Request message to the NMS which is associated to a Service Provider.

The joining procedure in the virtual AN setup is to provide the virtual AN to join the service provider network, which is similar to the joining procedure in the basic AN setup procedure. Once the virtual ANC receives the Discovery Response from the NMS, it then select the proper service provider network and configure the virtual AN to join with the service provider network. After the virtual access network setup is completed, the virtual ANC will send a Creation Response to the AN Orchestrator to notify the virtual AN setup result.

The Discovery Request message for the virtual AN setup may contain following information:

* Virtual ANC Identity
* Service Provider Identifier
* Time stamp of this message
* Discovery type
* The capability information of physical NAs attached to the virtual AN
* The physical backhaul capabilities

The Discovery Response message for the virtual AN setup should include the following information:

* Service Provider Identity
* Virtual ANC Identifier
* Time stamp of this message
* Access Router Interface ID
* Subscription Service Interface ID and Identity
* Security configuration information
* Radio configuration information for the required area
* Backhaul parameters to the Service Provider’s subscription service and access router such as multiple ports and addresses of the network and the load information of each port.
* Service Provider Network descriptor, such as capability (max NA number, max user number…), security information, etc.
* Service Provider’s network address list which helps NA to choose a proper port for the following communication
* Operational capabilities of the virtual AN

The Creation Request message for virtual AN setup should include the following information:

* Virtual AN Identity
* Service Provider Identity
* Time stamp of this message

The Creation Response message for the virtual AN setup should include the following information:

* Service Provider Identity
* ANC Identifier
* Time stamp of this message
* Result code and reason

##### Virtual AN Release Procedure

There may be two ways to release the virtual AN.

* AN Orchestrator initiated the virtual AN release: the AN Orchestrator sends a request to the virtual AN to initiate the virtual AN release.
* Service Provider initiated the virtual AN release: the service provider network starts the termination of virtual AN through the NMS via sending the Release Request message.

Figure 15 shows an example of release procedure of virtual access network. Figure 15a show the procedure of virtual access network release initiated by the AN-Orchestrator. In some case, when the AN Orchestrator needs to release the virtual AN, it will instruct the virtual ANC to send a Release Notification message to the NMS of the service provider. Once the virtual ANC receives the Release Response, it passes to the AN Orchestrator. The AN Orchestrator will then release the instance of virtual AN including virtual NAs, virtual BH and finally virtual ANC.

The Release Notification message for AN-Orchestrator initiated virtual AN release should include

* Virtual AN Identity
* Service Provider Identity
* Time stamp of this message
* Subscription Service Interface ID and Identity
* Access Router Interface ID and Identity

The Release Response message for AN-Orchestrator initiated virtual AN release may include

* Service Provide Identity
* Virtual AN Identity
* Time stamp of this message
* Result code and reason



(a)



(b)

Figure 15 an example of virtual access release:

(a) AN-Orchestrator initiated virtual AN release; (b) Service Provider initiated virtual AN release

Figure 15b shows another example of the procedure of virtual AN release initiated by the Service Provider network. In some case, the Service Provider may need to release the virtual access network for maintenance, upgrade, etc. When receiving a Release Request message from the NMS, the virtual ANC passes the request to the AN Orchestrator to evaluate the message and verifies that the request matches completely with an instance of a virtualized AN. Only when complete match is determined, the AN Orchestrator will instruct the virtual ANC to send the Release Response to the NMS. The AN Orchestrator will then release the instance of virtual AN including virtual NAs, virtual BH and finally virtual ANC.

The Release Request message for Service Provider network initiated release should include

* Service Provider Identity
* Virtual AN Identity
* Time stamp of this message
* Subscription Service Interface ID and Identity
* Access Router Interface ID and Identity

The Release Response message for Service Provider initiated release may include

* Virtual AN Identity
* Service Provide Identity
* Timestamp of this message
* Result code and reason

##### Update Virtual AN Configuration Procedure

After successful instantiation of a virtual AN, the operation of the virtual AN can commence following the functional behavior and messaging described in the following chapters.



Figure 16 an example of virtual AN configuration update procedure

Figure 16 shows an example of procedure for virtual AN configuration update. During normal operation of the virtual AN, the NMS of Service Provider may request to re-configure the virtual AN. Only when the re-configuration do not collide with the operation of other virtual ANs of the same access network infrastructure, the virtual ANC will change the configuration of the virtual AN according to the wishes of the Service Provider. Otherwise the virtual ANC will respond with an alternative proposal to best match the required reconfiguration.

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