|  |  |  |  |
| --- | --- | --- | --- |
| OmniRAN SDN Use Cases and Requirements | | | |
| Date: [2014-05-15] | | | |
| **Authors:** | | | |
| Name | Affiliation | Phone | Email |
| Antonio de la Oliva | UC3M |  | [aoliva@it.uc3m.es](mailto:aoliva@it.uc3m.es) |
| Juan Carlos Zuniga | InterDigital |  | [j.c.zuniga@ieee.org](mailto:j.c.zuniga@ieee.org) |
| Paul Congdon | Tallac Networks |  | [paul.congdon@tallac.com](mailto:paul.congdon@tallac.com) |
| **Notice:**  This document does not represent the agreed view of the 802.1 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 a summary of some possible use cases for Software-Defined Networking (SDN) concepts in 802 technologies. It provides a high level description of the use cases and it derives the requirements that are applicable to OmniRAN SDN.

OMNIRAN SDN Use cases

# This document presents an aggregated view of the different SDN-based use cases being discussed in OmniRAN. It is based on several contributions which are listed in the following:

* <https://mentor.ieee.org/omniran/dcn/14/omniran-14-0009-00-0000-onf-wireless-and-mobile-wg-status-update.pptx>
* <https://mentor.ieee.org/omniran/dcn/14/omniran-14-0029-00-0000-sdn-based-use-cases-for-bof.pptx>
* <https://mentor.ieee.org/omniran/dcn/14/omniran-14-0002-00-0000-sdn-based-control-plane-and-data-plane-separation-in-omniran-network-reference-model.pptx>

The use cases currently identified of interest to the OMNIRAN TG are the following:

* Functional Split of IEEE 802 technologies
* Large Scale Access Management
* Virtualization and sharing of IEEE 802 technologies
* Unified Access Control

# Functional Split of IEEE 802 technologies

A common trend nowadays is to split wireless solution functionality amongst different physical locations in order to provide enhanced operation (i.e. through centralization of several functions) and management. This trend can be observed for example in IEEE 802.11 technologies which are commonly deployed following a model based on the centralization of several functions such as access control or channel configuration and the deployment of transparent access points in charge of forwarding the data plane. This mode of deployment follows the so-called controller-based deployment and its present in the portfolio of major vendors of IEEE 802.11 hardware solutions.

This model of functionally splitting the different operations of the wireless technologies can be applied to the different wireless technologies in general, providing centralized configuration/management and control interfaces in charge of the control plane, while deploying a disjoint and optimized data-path.

# Deployment Domain

The functional split of control and data planes can be applied to any IEEE 802 technology in the access area (similarly to what is already done in technologies such as IEEE 802.11) and backhaul area (like IEEE 802.16). In wired technologies, such as IEEE 802.3, recent advances in SDN protocols such as OpenFlow enable the control- and data-planes split.

# Use Case Description

In order to apply SDN concepts to IEEE 802 technologies, mechanisms enabling the split between the control/configuration of the network and the actual data forwarding must be provided. The functional split can be implemented following different models:

* Data, control and configuration mechanisms are integrated in the same entity. This is the most common model of operation and the most widely deployed. For example this is the case of an AP working in standalone mode, with all MAC and PHY layers included in the same box.
* Configuration mechanisms are performed through external API. This is the case of technologies controlled by, e.g., SNMP. A separate management system configures the network elements, e.g., channel, Tx power, etc. by generating remote primitives and messages and running an external configuration protocol.
* Different levels of control mechanisms are deployed in an external entity. This is the case of technologies relying on external controllers running parts of the control plane. There are multiple levels of splitting possible, from cases where just some functions such as the association of users are controlled (but the MAC layer runs on the point of attachment) to cases where the complete MAC runs in a separate box. In this last case, the points of attachment act as simple radio heads or transparent APs forwarding all frames to the central controller. This configuration can take the form of the extreme case of C-RAN (Cloud-RAN [1]) concepts where the complete MAC and higher layer control functions are located in a cloud or data center.

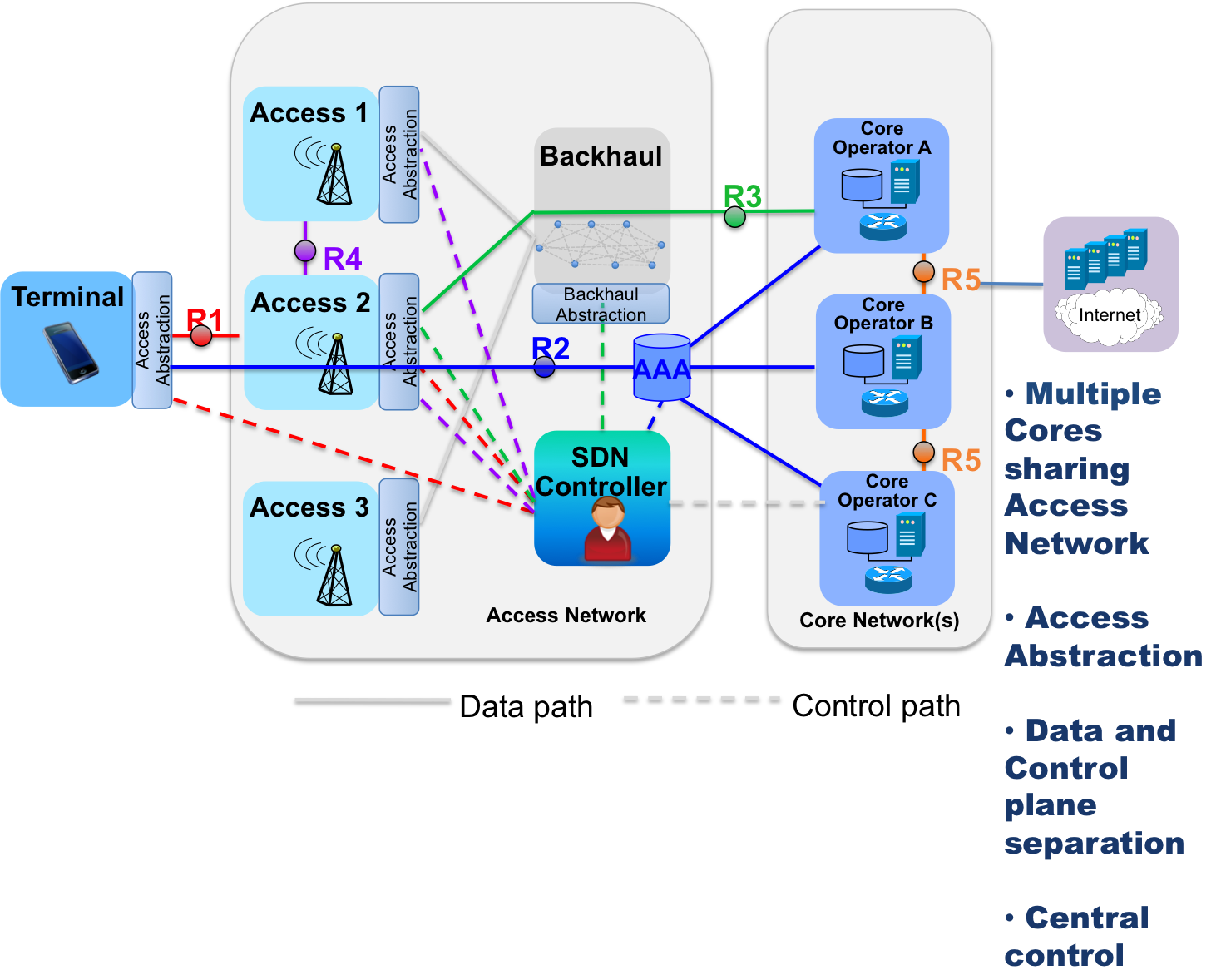
In the same way, the data-path can also take different forms:

* The data-path goes through the central controller which forwards data frames to the appropriate AP.
* The data-path is completely disjoint from the control path and goes directly to the point of attachment were the user is located. This solution requires other mechanisms to control the data-path configuration that may or may not be co-located with the control plane.

In summary, this use case considers three different layers that can be separated: data-plane, control-plane and management-plane.

It is worth noting that the functional split forms the basis for the sharing and virtualization of the IEEE 802 technologies. These mechanism enable an IEEE 802 based network were different elements are shared and different data-paths and control-planes are deployed and orchestrated in order to achieve coherent operation.

# OmniRAN Architecture Mapping



Following previous discussion in <https://mentor.ieee.org/omniran/dcn/14/omniran-14-0002-00-0000-sdn-based-control-plane-and-data-plane-separation-in-omniran-network-reference-model.pptx>, the functional split will impact the R2 and R3 interfaces that will need to be separated into control and data-plane variants. In addition, R4 is also involved since depending on the level of control split, R4 control part will be included in the R3 control path while R4 data path will remain an interface between the different RAN networks.

In addition, for the sharing of the different RANs by several operators, a new interface for the orchestration of mechanisms might need to be put in place. This functionality can be included in R5, hence is out of the scope of OmniRAN.

Regarding the configuration interface, R3 needs to include some kind of general interface enabling the configuration of the different IEEE 802 technologies, in order to create a common configuration interface running in the controller entity.

# Requirements for OmniRAN

* Interception of MAC control/management frames and forwarding them to the assigned controller
* Actions based on wireless frames parameters and on control/management frames
* Common configuration interface for IEEE 802 technologies
* etc

# Large Scale Access Management

Service providers and network operators commonly have network infrastructure comprised of several 802 technologies. Hence, there is a need to perform coherent control and management functions on the whole network, regardless of the underlying network technology being used.

# Deployment Domain

Access management of heterogeneous networks can be applied to any wired and wireless IEEE 802 technology in the access (similarly to what is already done in technologies such as IEEE 802.11) and backhaul (like IEEE 802.16 and IEEE 802.3).

# Use Case Description

In order to implement a coherent management of 802-based heterogeneous networks, some SDN-based mechanisms need to be supported:

* Data path control protocol to handle the setup of data flows paths.
* Control/management protocol to handle configuration of radio properties and MAC features

# OmniRAN Architecture Mapping

(See previous figure)

# Requirements for OmniRAN

* + SDN abstraction functionality / layer
  + Radio configuration capabilities
  + MAC properties configuration

# Virtualization and sharing of IEEE 802 technologies

One of the main advantages of SDN-base deployments is that it allows virtualizing and sharing network resources dynamically. These features permit differentiating the traffic associated to each virtual network, while still maintaining a single point of control and management for the whole network.

# Deployment Domain

In this case, user devices can get access to a single point of attachment running several dynamically created networks, where each network can have differentiated services, such as QoS, isolated access/backhaul/fronthaul network instances, etc.

# Use Case Description

Network operators can share resources with different service providers, allowing hence multi-tenancy features.

# OmniRAN Architecture Mapping

Virtualization.pdf

# Requirements for OmniRAN

* + Interception of MAC layer frames (e.g., portal issues)
  + Actions based on wireless frame parameters
  + Dynamic association of virtual networks to data paths
  + Management of QoS/queues properties and fine-grain QoS measurements
  + Dynamic creation of virtual points of attachment in single hardware instance

# Unified Access Control

It is common for users of 802 technologies to incorporate multiple access technologies in their computing devices. It is desirable to allow and control user access to network resources based on user identity, the device in use, the location of access and which applications are desired, no matter which 802 medium the user is connected to. Such policy control is typically dynamically deployed to the access layer based upon authentication processes including common technologies such as IEEE 802.1X. In addition, cryptographic key distribution may also be included as part of this access control process.

# Deployment Domain

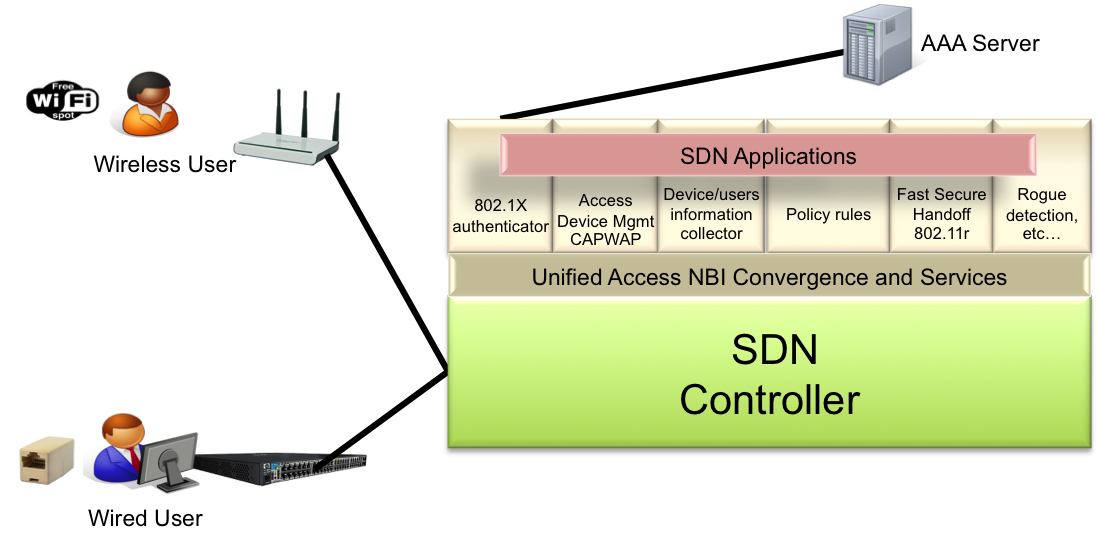
In this case, a user and/or user device is authenticated against common authentication repositories over multiple IEEE 802 medium (e.g. IEEE 802.11 and IEEE 802.3). Access control policies are specified using a common high-level description, but are translated into access technology specific controls and functionalities. Means for specifying common data path control elements, such as flow tables and forwarding databases, should be exploited.

# Use Case Description

In order to facilitate access security and common user role/location based policy, centrally defined policy is defined and deployed across all IEEE 802 access layer technologies. Common end-user authentication, authorization and accounting (AAA) is enabled by a common access control framework. IEEE 802.1X provides this framework for IEEE 802 networks. It is desirable to centralize the IEEE 802.1X authenticator using SDN approaches to ensure consistent policy enforcement can be achieved across all mediums. High-level policy definition is, perhaps, out of scope for IEEE 802 technologies, however, the enforcement mechanisms are typically part of the infrastructure forwarding devices and are within scope.

Example policy enforcement mechanisms that should be common across 802 mediums are the ability to associate the end-user/station with a particular virtual network instance, associate security restrictions and QoS parameters with an end-user/station session and provide transient encryption key material as the result of successful authentication.

# OmniRAN Architecture Mapping



# Requirements for OmniRAN

* Intercept MAC layer authentication/association frames
* Intercept EAPOL authentication frames
* Relay this frames or its information to access control servers (e.g., use centralized captive portal with different authentication mechanisms such as Google, use a common AAA authentication server, etc..)
* Configure network/access security, in-line policy enforcement functions and associate a data-path
* Push credentials to terminal and point of attachment (e.g., interface with 802.11r)

**REFERENCES**

1. China Mobile Research Institute, "C-RAN - Road Towards Green Radio Access Networks," in WWRF Meeting, Dusseldorf (Germany), October 2011.