|  |
| --- |
| SDN Functional Decomposition |
| Date: 2015-01-13 |
| **Authors:**  |
| Name  | Affiliation  | Phone  | Email  |
| Antonio de la Oliva | UC3M | +34657079687 | aoliva@it.uc3m.es |
| **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 proposes initial draft text for the SDN chapter of IEEE 802.1cf

1 SDN Functional Decomposition 3

1.1 Introduction 3

1.2 Acronyms 3

1.3 Roles and identifiers 3

1.4 Use Cases 3

1.4.1 Setup of interfaces and nodes 3

1.4.2 Detection of terminal attachment 4

1.4.3 Data Path Establishment 4

1.4.4 Data Path Teardown 5

1.4.5 Data-Path Maintenance 5

1.4.6 Control-Path Maintenance 5

1.4.7 Path relocation 5

1.4.8 Affecting the behavior of Coordination and Information System 5

1.4.9 Configuration of connection between the Core Network and the Access Network 5

1.4.10 Event Handling 5

1.4.11 Statistic gathering 5

1.5 Functional requirements 6

1.5.1 Support of a control connection between the different data path elements and the controller 6

1.5.2 Support for data path elements with heterogeneous technology interfaces 6

1.5.3 Support of communication mechanisms between the terminal and the controller 6

1.5.4 Support of per packet matching, forwarding rules and actions in the data path element 6

1.5.5 Support of state recording in the data path elements 6

1.5.6 Support of security associations between the controller and the data path elements (including terminal) 6

1.5.7 Support of security associations between controllers belonging to the AN and CN, which communicate 6

1.5.8 Support of security associations between AN controllers and CIS servers 6

1.6 SDN specific attributes 6

1.6.1 Abstract parameters 6

1.6.2 Terminal Configuration 7

1.6.3 Access Network Configuration 7

1.6.4 Data path Establishment 7

1.6.5 Triggering technology specific features 7

1.6.6 Interacting with CIS 8

1.6.7 Communication between CN and AN 8

1.6.8 Event handling 8

1.6.9 Statistic gathering 8

1.7 SDN basic functions 8

1.7.1 Configuration of interfaces 8

1.7.2 Data path establishment/modification 8

1.7.3 Data path teardown 9

1.7.4 CIS communication and controller as proxy for CIS 9

1.7.5 Triggering technology specific functionality from the controller 9

1.7.6 Event Handling 9

1.7.7 Statistics Gathering 9

1.8 Detailed procedures 9

# SDN Functional Decomposition

## Introduction

Over the last few years, the Software Defined Networking (SDN) paradigm has gained a lot of popularity. SDN decouples the system that makes decisions about where traffic is sent (i.e., control plane) from the underlying system that forwards traffic to the selected destination (i.e., data plane). With SDN, network administrators can program the behaviour of the network in a centralised way, without requiring to access and configure each of the hardware devices independently, which greatly simplifies overall network management.

It is important to highlight that SDN is merely a tool that enables innovation in network control. SDN neither dictates how that control should be designed nor solves any particular problem, this means that the actual protocol or control state machine is left for the application developer to design and implement, leaving the door open to innovation and differentiation in the market.

SDN has two defining characteristics:

* SDN separates the control plane (which decides how to handle the traffic) from the data plane (which forwards traffic according to decisions that the control plane makes).
* SDN consolidates the control plane, so that a single software control program controls multiple data-plane elements. The SDN control plane exercises direct control over the state in the network’s data-plane elements (i.e., routers, switches, and other middleboxes) via a well-defined Application Programming Interface (API).

The SDN concept relies on two well defined interfaces, the Southbound (also known as D-CPI) and the Northbound (also known as A-CPI). The Southbound interface is used by the controller to interact with the data path elements (e.g., switches) while the Northbound interface is used by applications to interact with the controller and implement the application logic. Southbound interfaces fall in the scope of IEEE 802, while Northbound interfaces are presumable out of its scope.

Among the different protocols that can be used to realise the SDN concept, OpenFlow [REF] is the one most widely adopted by the telecommunications industry. OpenFlow design is based on 5 characteristics (known as the 5C):

* Plane separation
	+ Forwarding functionality, including the logic and tables for choosing how to deal with incoming packets based on characteristics such as MAC address, IP address, and VLAN ID, resides in the forwarding plane.
	+ The protocols, logic, and algorithms that are used to program the forwarding plane reside in the control plane.
* Simplified devices & Centralised Control
	+ Instead of hundreds of thousands of lines of complicated control plane software running on the device and allowing the device to behave autonomously, that software is removed from the device and placed in a centralized controller.
* Network automation and virtualization
	+ SDN can be derived precisely from the abstractions of distributed state, forwarding, and configuration
	+ They are derived from decomposing into simplifying abstractions the actual complex problem of network control faced by networks today.
* Openness
	+ SDN interfaces should remain standard, well documented, and not proprietary.
	+ The premise is that keeping open both the northbound and southbound interfaces to the SDN controller will allow for research into new and innovative methods of network operation.

It is also important to highlight that SDN mandates that the control functionality is implemented in a centralized node (the controller), hence implementations relying on distributed control processes on data-path elements do not adhere to the SDN definition. This rules out distributed approaches using protocols such as SPB and/or MMRP protocols which work by exchanging information between data path elements and reaching a consensus state in the network, without the intervention of a central controller taking the decisions.

Some other protocols are also used as Southbound protocols, and some of them are already used within IEEE 802 networks, such as SNMP. Some other Southbound protocols such as CAPWAP rely on the interface with the MIB on each technology to define how it behaves.

While so far SDN efforts have been mostly focused on wired networks, and comparatively little attention has been paid to applying it to wireless, the potential benefits of this technology extended to adequately support mobile networks are much higher than with wired networks, for the following reasons:

* It allows to manage all the heterogeneous technologies (such as cellular or WLAN) in a transparent way, hiding the specificities of the technologies to the TE tool.
* It allows to integrate in a single decision point different types of communication that have traditionally been handled separately, such as device-to-device and infrastructure communications.
* It can also be used to address new functions that are not needed in wired networks, such as switching off those points of access that are not needed at a given point in time, and thus reduce energy consumption.
* Finally, using an adequate abstraction of wireless resources, handling the complex capacity calculations in heterogeneous deployments could be as simple as in wired networks

Within the IEEE 802 set of technologies, there are multiple functionalities which can be designed based on the SDN paradigm. This document presents several use cases showcasing these functionalities:

* Setup of interfaces and nodes
* Detection of node attachment
* Path Establishment
* Path Tear Down
* Path Maintenance
* Path relocation
* Affecting the behavior of Coordination and Information System
* Configuration of connection between the Core Network and the Access Network
* Event handling
* Statistic gathering

Another important point raised within the SDN community has been the need of a common and extensible protocol allowing the configuration of devices in a centralized way. One of the major problems faced now in the management of large networks is the lack of a secure protocol enabling the common configuration of all devices in the network. One may argue that the use of MIBs and the SNMP protocol solves this issue but in reality the use of this protocol is not exempt of problems. In addition, the MIBs are difficult to maintain and their definition lacks of clarity, and the administrators of large networks usually have to use vendor locked tools and specific scripts to configure their networks. The networking community is looking at other recent tools to overcome these issues being the champion of this approach the NETCONF protocol, that uses YANG models as data representation tool. This document also presents an overview of this protocol and data representation model.

## Acronyms

CIS Coordination and Information System

CN Core Network

AN Access Network

## Roles and identifiers

* Controller: Application that manages different behaviors (e.g., flow control) in a Software Defined Networking environment.
* Data path element: Hardware/Software entity in charge of executing the orders from the controller, affecting the path through which data is forwarded.

## NETCONF protocol and YANG modelling

As explained in the introduction, managing a communication network is a costly and difficult operation that currently is not performed in a programmatic way:

* A huge number of human resources are employed on maintaining network configuration, performance and security.
* Configuration errors are the main cause of network failures. Usually these errors came from erroneous human intervention and they cost millions in downtime and recovery.
* Current techniques are based on custom, locked-in CLI procedures, error prone.

There is a clear need for a programmatic mechanism for the management of configuration data and standard mechanisms for the management of heterogeneous, multiple-vendors network equipment. This is the hole that NETCONF tries to fill in.

NETCONF is a new transaction-based protocol for programmatic management of network configurations which builds on top of well-known protocols (SSH, XML, SOAP) to provide secure configuration of heterogeneous devices.

The key characteristics of the NETCONF protocol are listed in the following:

* It supports partial device configuration to the most fine-grain level.
* It supports full device configuration with a single operation and network wide device configuration.
* It supports support reporting error codes for partially or completely failed configuration requests.
* It supports sending configuration requests independent of the completion of previous requests. Requests may be queued or processed concurrently at a device. Each request has a request ID. Success or failure indications can be sent independently of other requests individually for each request ID.
* It is extensible. New operations can be added and its support can be checked by capability retrieval.
* Configurations of a device or for portions of it are encoded in XML
* UML XML Schema is also provided
* For each of the next elements the specification provides UML class description and XML example

One of the key points on any management protocol is the security. In order to assure correct security for its operations, NETCONF supports TLS as communication transport protocol that can be used for providing integrity, privacy, and mutual authentication. All specified transport mappings for NETCONF use TLS or TCP as underlying transport protocol and thus provide reliable transport.

A data model is a consistent and complete definition of the structure, syntax and semantics of data. NETCONF uses YANG data modeling language to model both configuration data as well as state data of network elements.

YANG is a modular language representing data structures in an XML tree format, making it very appropriate for the definition of the NETCONF structures. The data modeling language comes with a number of builtin data types, from which additional data types can be derived if needed. A YANG module defines a hierarchy of data that can be used for NETCONF-based operations, including configuration, state data, Remote Procedure Calls (RPCs), and notifications. This allows a complete description of all data sent between a NETCONF client and server. The hierarchy of data is organized as a tree, in which each node has a name and either a value or a set of childs. The language defines the nodes and their interaction.

The YANG data model is structured in modules, which can be formed by submodules. Any module can import data from external modules and even modify the hierarchy defined in other module by adding nodes to that module. This can be done conditionally only if certain conditions are met. In addition, through YANG, constraints can be enforced on the data, restricting the value of appearance of nodes based on the presence or value of other nodes.

To the extent possible, YANG maintains compatibility with Simple Network Management Protocol's (SNMP's) SMIv2 (Structure of Management Information version 2 [[RFC2578](https://tools.ietf.org/html/rfc2578)], [[RFC2579](https://tools.ietf.org/html/rfc2579)]). SMIv2-based MIB modules can be automatically translated into YANG modules for read-only access. However, YANG is not concerned with reverse translation from YANG to SMIv2.

To finalize this clause, it is worth noting that some Task Groups in the IEEE 802 are already working towards the definition of YANG models for the management of the configuration of some technologies. One example of this is the IEEE 802.1Qcp, defining the YANG model for bridges and bridged networks.

## Use Cases

### Setup of interfaces and nodes

Through SDN a central controller can implement a control logic enabling it to configure several parameters in the nodes and interfaces of the data path. Within the possible set of configuration parameters there are three main families:

* SDN control configuration
* Short time scale configuration
* Long time scale configuration

SDN control configuration refers to the required setup of the parameters ruling the communication between the data path element and the controller. These parameters may include IP address of the controller, kind of protocol, VLAN or interface used for the communication and certain timers governing the transmission of keep alive messages or the tear down of it in case of failure. These configuration parameters must also include the different timers, ports and protocols used for the communication between the controller and the data path element.

Short time scale configurations are related with the configuration of parameters, which may change in very short time scales. For example transmission power, MAC QoS parameters, antenna selection, etc..

Long time scale configuration refers to the long-term configuration of the node or interface; the parameters used by the controller are the typical ones an OAM system may use. Examples of these parameters include the operational frequency, configuration regarding credentials or authentication servers to use, supported authentication modes, VLAN configuration, etc.

While considering what parameters can be configured by a central controller, one may think of all the current parameters defined in MIBs for IEEE 802 technologies.

### Detection of terminal attachment

A very important operation required to use SDN control in the access network is the possibility of detecting the attachment of new terminals. The user’s terminal, typically will not include any kind of SDN software nor they are aware of connecting to a network using an SDN controller. In this way, it is needed some mechanism to handle the detection of the terminals while attaching to the network PoAs. In a PoA where the wireless interface (IEEE 802.11) is bridged to a switch, this detection of terminal attachment can be done thanks to the switch sending a LLC SNAP message upon attachment of a new terminal. In other technologies some other mechanisms should be analysed.

For the IEEE 802 technologies is quite important to define mechanisms able to provide a central controller with information on the user attachment. Simple mechanisms as the one presented for IEEE 802.11 (bridged to a switch) are not compatible with more complex technologies involving exchanges with the AAA service of the network. In addition, technologies such as IEEE 802.16 rely on complex protocols and interactions with the core to manage the user association. A clear view on how to detect user attachments per technology should be consider in order to apply the SDN concept to a complete network.

### Data Path Establishment

An IEEE 802.1cf network does not include IP layer, hence path establishment mechanisms using above layer-2 information are out of the scope of this document. In order to establish a path, a controller requires to be informed of the new flow, including its requirements in terms of capacity, delay and jitter. After receiving this information the controller can compute the best possible path and communicate this decision to the data path elements. After this, the data path elements will enforce the controller decision on the different packets traversing the data path.

For this specific clause, it is important to distinguish between the concept of SDN and the actual implementation of this concept, such as OpenFlow. While SDN is basically the concept of control/data plane split and centralized control applied to a network, OpenFlow realizes these ideas on IEEE 802.1 compliant switches. It is very important for IEEE 802 readers, to understand the differences between the technologies and how the SDN idea can be implemented on them. As an example: while a network composed completely out of switches can be discoverable by an OpenFlow controller, a network in which these switches are connected also to a wireless network composed of several nodes, cannot. This is due to the differences between the IEEE 802.1 switch and an IEEE 802.11 portal. In this case anything below the portal will be invisible to the OpenFlow controller (although IEEE 802.11ak work will solve some of these issues).

For the general case, in order to perform the data path establishment, the following information/functionality is required:

* Topology information
* Mechanisms to compute best path based on some criteria
* A mechanism in the IEEE 802 device able to apply a per-flow/per-packet policy. This policy will be named rule in the following.
* Communication mechanisms to set specific rules in the data path to decide output port/modifications to frame
* The data path must support some mechanism for packet matching. This mechanism can be arbitrarily complex. It can include simple mechanisms as input port matching, VLAN tag matching or complex rules indicating logical combination of parameters, including internal state of the data path element.
* The data path must support the application of forwarding rules to the input traffic. In this way the decisions taken by the controller will be applied and the packet will be sent through the appropriate output port.
* The data path element may support actions over the packets and internal state. The data path element may be able to modify certain parts of the packet and modify internal state variables, such as counters, monitoring variables, etc..

Also consider that in some of the technologies considered, a packet may not be accessible. For example, an optical link performing optical passthrough. In this cases, the data path setup will consist on the configuration of the parameters defining how the flow is managed, not in an specific packet per packet based.

### Data Path Teardown

A certain path can be created for a specific flow. Once the flow finishes, there is no need to have the path established any longer, freeing resources allocated to the path. In order the controller to tear down a path, it needs to discover that the path can be deactivated. This can be done through monitoring metrics or flow information coming from the flow originator. Once the controller knows that the path can be removed, it can communicate the data path elements its decision. At this moment all data path elements will remove the stored state corresponding to this path. This implies the IEEE 802 device must be able to obtain performance statistics and reporting them to the central controller.

### Data Path Maintenance

Typically a data path element will configure forwarding rules with a certain lifetime. The rules must be updated within their lifetime, or the data path element will remove them. Upon expiration of the rule, the data path element should inform the controller about the removal of the rule. In this way, the controller can keep record of the current status of the paths in the network.

### Control Path Maintenance

In the same way as with data paths, the communication between the controller and the different data path elements must be kept alive through the exchange of some control packets. The actual configuration of the timers to use should be one of the parameters considered in 1.4.1.

### Path relocation

Due to several reasons such as traffic engineering, movement of the terminal or QoS degradation, it may be necessary to relocate a data path. With relocation we meant to change the data path elements the data path goes through, while keeping the most similar allocation of resources. This functionality can be divided in a sequence of Data Path establishment and Data Path Tear Down.

### Affecting the behavior of Coordination and Information System

Terminals and network nodes can rely on Coordination and Information Services (CIS) to gather information helping them to take some decision, such as candidate network selection, channel to use, etc. A controller may interact with the CIS in a standalone way o it may mediate in the communication between the terminal and the CIS. This later approach allows the controller to modify, apply policies, add more information or simply query different servers based on terminal information such as its user profile.

### Configuration of connection between the Core Network and the Access Network

An IEEE 802 access network is connected to a Core Network through a network known as backhaul. Typically the backhaul network is composed of IEEE 802 switches or MPLS/IP routers. For the scope of this specification we will focus on the former. In addition, there is a currently a trend pushing for a separation between the radio part of the access network (implementing only some parts of the physical/MAC layers) and the processing of the signal or remaining stacks of the protocol layer in a separated way. The network connecting both elements is known as the fronthaul and has some specific and highly constrained requirements, such as high bandwidth and extremely low latency. Examples of this network in the IEEE ecosystem is the work performed in IEEE 1904.3 and IEEE 1914. Both approaches rely on IEEE 802.3 switches to perform the actual forwarding of the data.

Considering both transport networks (the backhaul and fronthaul), these networks must carry the user packets to the point of connection to the Core Network. The Core Network may connect to the Access Network in several points, and the Access Network (or even the transport) can be shared among multiple tenants. For this specific case, the traffic must consider to build the paths towards the destination, not only what is the most appropriate point of connection to the Core, but also what isolation mechanism to be used to transfer each tenant traffic. Hence mechanisms for establishing VLAN, Q-in-Q or MAC-in-MAC paths through the network and automatic configuration of the end points is needed.

### Event Handling

Current SDN southbound protocols provide mechanisms for Event Handling. As an example, OpenFlow is working on the definition of Alarms and it already includes mechanisms to notify of the change in the status of ports, among other things. The current problem of these approaches is their limitations, since they do not consider the multiple and different characteristics of the IEEE 802 technologies. In this way, for example, there is no concept of wireless port, hence none of the wireless specific characteristics, such as e.g., number of retransmissions crossing a certain level, can be rolled back to the controller. Mechanisms such as the Event Service of IEEE 802.21 may be used to solve this problem, although a common way to report this events and the definition of the data models related should be considered by the IEEE 802.

### Statistic gathering

In the same way as with the Event Handling in clause 1.5.10, SDN southbound protocols implement mechanisms for Statistics gathering, which can be used to alter the way flows are treated within the network. Regarding IEEE 802 technologies, this faces the same problem as Event Handling, since the statistics defined are mostly based on packet counting and do not consider the specific characteristics of IEEE 802 technologies.

## Functional requirements

The following requirements apply to the SDN procedures.

### Support of a control connection between the different data path elements and the controller

Elements in the network subject to be controlled or communicate with a controller SHOULD use a secure control connection for the communication. This includes the terminal in case it communicates with the controller.

### Support for data path elements with heterogeneous technology interfaces

Controllers SHOULD support the configuration of parameters for multiple technologies. Abstract parameters, common for multiple technologies SHOULD be used when possible. The data path element SHOULD provide common controlled behaviors to all the interfaces attached to it, regardless of their technology.

### Support of communication mechanisms between the terminal and the controller

The terminal SHOULD use a secure communication channel to communicate with the controller.

### Support of per packet matching, forwarding rules and actions in the data path element

Data path elements SHOULD include mechanisms for packet matching, forwarding rules and actions (packet modifications).

### Support of state recording in the data path elements

Data path elements SHOULD be able to store operational parameters so they can be retrieved for monitoring.

### Support for data models specifying the characteristics of IEEE 802 technologies, including configuration parameters, events and statistics

IEEE 802 SHOULD work towards the definition of data models which can be used by Southbound protocols implementers to enable protocols to interact with IEEE 802 technologies

### Support for interfaces enabling the configuration of VLAN, Q-in-Q and MAC-in-MAC tags

Data path elements SHOULD support interfaces enabling the configuration of VLAN, Q-in-Q and MAC-in-MAC tags for different flows.

## SDN specific attributes

This section lists possible parameters for the different functions involved in the SDN operation.

### Abstract parameters

* Supported Rates
* TxPower, TxPower levels supported
* Operational Frequency
* Statistics: Tx error, Rx error, Number of stations

### Terminal Configuration

* Terminal Controller:
	+ LIST of control capabilities
	+ LIST of interfaces and their capabilities
	+ LIST of protocols to manage interfaces
		- E.g., interface X supports CAPWAP+OF
* Interface
	+ Abstract parameters
	+ LIST of parameters to be configured
		- Technology specific: e.g., BSSID to connect to, RTS Threshold, Short retry, long retry, fragmentation threshold, Tx/Rx MSDU lifetime, enable Block Ack, etc.
		- Security parameters (technology dependent)

### Access Network Configuration

* Configuration of interfaces
	+ Abstract parameters
	+ LIST of parameters to be configured
		- Technology specific: e.g., BSSID, RTS Threshold, Short retry, long retry, fragmentation threshold, Tx/Rx MSDU lifetime, enable Block Ack, etc.
		- Technology specific security parameters: WPA/WPA2/WEP, parameters for key management, etc.
	+ Queue configuration: Capacity, max number packets, rate limitation
* Configuration of nodes
	+ Parameters to configure the connection to controller:
		- Protocol+port
		- Credentials
		- Output physical port to use to connect to controller
		- ID
* Configuration of data path ports
	+ VLAN configuration
	+ Number of tables

### Data path Establishment

* Matching rule and actions
	+ Matching rule definition and associated actions

### Triggering technology specific features

* Type for feature
	+ E.g., send 802.11v frame, configure 802.11aa groupcast mode
* Content of feature
	+ E.g., BSS to attach to, groupcast mode, concealment address, stations to be added

### Interacting with CIS

* Parameters to enable the communication
	+ Protocol to be used, credentials
* Adding/removing/modifying information at the CIS
	+ CIS specific
		- E.g., IE elements to add to ANQP

### Communication between CN and AN

TBD

### Event handling

TBD

### Statistic gathering

TBD

## SDN basic functions

Controller discovery and configuration is out of the scope of Omniran

### Configuration of interfaces

Once a data path element or a terminal is attached to a controller, it can configure the different characteristics of the interface. Typical example of this can be taken from the world of IEEE 802.11 where WLAN controllers configure the different parameters of the technology. The typical parameters that the controller will setup are operational frequency and transmission power. Depending on the technology the controller will also be able to configure additional parameters such as RTS threshold or ESSID/BSSIDs of the different APs. The actual configuration to be installed may come from different sources ranging from fully automatic algorithms computing the best allocation of e.g., frequency/transmission power to static allocations.

### Data path establishment/modification

Once the controller is connected to the data path elements it must decide the path data flows will follow. Depending on the technology of choice (e.g., OpenFlow, MVRP, SNMP, etc.) the data path will be installed based on static rules such as port allocated VLANs or it will be installed based on intelligent packet matching rules. As result of this operation each data path element should have a rule stating the forwarding behavior for packets belonging to a certain flow. The computation of the path to be installed depends on the technology of choice for the controller, since there are technologies computing a path in a distributed way and technologies that can run traffic engineering+policying algorithms.

In addition to the pro-active instantiation of a path described in the above text, a data path element may reactively interact with the controller due to some event, new packet arrival or pre-installed rule among others. Following this, the data path element may interact with the controller in order to build a path for a specific new flow that has just appeared and for any reason should not be forwarded through the pre-configured paths.

### Data path teardown

Once a data path is no longer in use, the rules indicating the forwarding behavior for each data path element may be removed. Generally this is done through lifetime timer expiration but the controller can choose to remove the rules actively. Note that rules installed in a data path can also be permanent or semi-permanent, not requiring the refreshing of the controller.

### CIS communication and controller as proxy for CIS

Nowadays CIS databases are filled with information provided by multiple sources but controlled by the operator. It would be desirable for the AN controller to be able to communicate with the CIS system in order to add/remove/modify its information based on its knowledge about the network. One example would be to update the list of services being advertised in 802.11aq based on information obtained from the network.

In addition to this, a controlled network can be configured in such a way that the controller is used as proxy for the CIS communication. In this way the controller will get the answer from the CIS and can modify it accordingly to get some expected behavior in the network. For example, a controller may be used as proxy to access a MIIS and after receiving the response filter it in order to remove the surrounding networks that do not belong to a specific operator, in this way enforcing some policy in the terminal.

### Triggering technology specific functionality from the controller

Although SDN controllers have been used typically to just setup data paths in the network and configure characteristics of the interface, the complete possibilities of controlling the specific features of the technologies have not been yet analyzed. The use of technology specific features by a controller can yield to further advantages for the network. For example, a controller may configure the QoS across a mix of wireless and wired domains, by triggering the QoS configuration mechanisms of each technology. Another example may use management frames of IEEE 802.11v to control the point of attachment of the user terminal. To open all this functionality the controller needs of a clear view of the capabilities of the interface and new APIs to trigger it in a remote way.

### Event Handling

TBD

### Statistics Gathering

TBD

## Detailed procedures

TBD