|  |  |  |  |
| --- | --- | --- | --- |
| SDN Functional Decomposition | | | |
| Date: 2015-01-13 | | | |
| **Authors:** | | | |
| Name | Affiliation | Phone | Email |
| Antonio de la Oliva | UC3M | +34657079687 | [aoliva@it.uc3m.es](mailto:aoliva@it.uc3m.es) |
| Juan Carlos Zuniga | InterDigital |  |  |
| Luis Miguel Contreras | Telefonica |  |  |
| **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

Software Defined Networks (SDN) is a new paradigm based on the splitting of control and data plane of networking elements. Basically it works by pushing the intelligence related to the operation of a certain service to a central controller, while the data path (user data packets) is handled based on the orders of the central controller in separate and specialized elements. 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

## 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.

## 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.

### 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.

### 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.

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
* 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..

### 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.

### 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 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 relay 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

TBD

### Event Handling

TBD

### Statistic gathering

TBD

## 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 of security associations between the controller and the data path elements (including terminal)

TBD

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

TBD

### Support of security associations between AN controllers and CIS servers

TBD

## 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