TELECOM INFRA PROJECT

Disaggregated Cell Site Gateway
Technical Specification

Authors:

- **José Antonio Gómez Atrio**
  - Optical Transport & SDN Architect, Vodafone.
  - jose-a.gomez@vodafone.com
- **Manuel Julián López Morillo**
  - IP&SDN Distinguished Engineer, Vodafone.
  - manuel-julian.lopez@vodafone.com
- **Paolo Agabio**
  - Transport System Engineer, Vodafone.
  - paolo.agabio@vodafone.com
- **Luis Martin Garcia**
  - Network Technologies Manager, Facebook.
  - luismg@fb.com
- **Diego Marí Moretón**
  - Network Engineer, Facebook.
  - dmmorten@fb.com
- **Andy Sutton**
  - Principal Network Architect, BT
  - andy.sutton@bt.com
- **Victor López, PhD.**
  - Systems and Network Global Direction (gCTIO), Telefónica
  - victor.lopezalvarez@telefonica.com
- **Mamadou Birrou Diallo**
  - Network Architect, Orange.
  - mamadoubirrou.diallo@orange.com
- **Silmar Freire Palmeira**
  - Technology Executive, Innovation & Technology, TIM Brazil
  - spalmeira@timbrasil.com.br

Contributors:

- **Luis Angel Muñoz Marin**
  - IP Transport, Sync & SDN Architect, Vodafone.
  - luis-angel.munoz@vodafone.com
- **Stefano Fogli**
  - Head of NGA Network Architecture, BT
  - stefano.fogli@bt.com
- **João Gabriel Aleixo**
  - Technology Specialist - Innovation & Technology, TIM Brazil
  - jaleixo@timbrasil.com.br
- **Washington Correia**
  - Senior Specialist - Innovation & Technology, TIM Brazil
  - wcorreia@timbrasil.com.br
- **Glaucio Peragene**
  - Telecom Specialist - Transport Network Engineering, TIM Brazil
  - gperagene@timbrasil.com.br
- **Michel Ouellette**
  - Network Engineer, Wireless Connectivity Deployment, Facebook
  - michelouellette@fb.com

- **Ivan de Francesca**
    - Transport Expert
    - ivan.defrancesca@telefonica.com
- **Juan Rodriguez**
    - Technological Expert, gCTIO, Telefonica
    - juan.rodriguezmartinez@telefonica.com
- **Luis Miguel Contreras**
    - Technological Expert, gCTIO, Telefonica
    - luismiguel.contrerasmurillo@telefonica.com

Change Tracking

Date	Revision	Author(s)	Comment
23/02/2018	v0.1	Manuel, José Antonio, Paolo, Luis	Draft version
07/05/2018	v0.2	Manuel, José Antonio, Paolo, Luis	Initial version
07/05/2018	v0.3	Andy	Contributions from BT
29/05/2018	v0.4	Mamadou Birrou	Contributions from Orange
31/05/2018	v0.5	Victor	Contributions from Telefónica
27/06/2018	v0.6	Joao	Contributions from TIM Brazil
03/07/2018	v1.0	José Antonio, Luis	Stable version
12/09/2018	v1.0.1	Young Bae	Minor clean up based on comments/corrections from Michel Ouellette (FB)
25/09/2018	V1.1	José Antonio, Manuel	Stable version with additional feedbacks & modifications.
23/10/2018	v.1.1	Victor, Ivan, Juan, Luis	Contributions from Telefónica
26/10/2018	v.1.1	DCSG Sub-group	Final version – 1.1

Table of Contents

Table of Figures

1. Introduction

This document describes the technical specification for a Disaggregated Cell Site Gateway (DCSG) device that operators can deploy in current and future generations of mobile transport networks. The document describes the necessary hardware, software and regulatory requirements that the device needs to meet in order to be deployed in the networks of the specific operators participating in this specification.

1.1. Why DCSG?

The goal of this project is to develop a solution that overcomes the most relevant issues operators are facing nowadays when deploying mobile transport networks, specifically cell site gateways. The issues are very relevant in 2G/3G/4G deployments today and will become even more critical for the upcoming 5G deployments. Some of those issues are:

- Vendors providing monolithic platforms that make it impossible to introduce innovation from other vendors in different parts of the device stack
    - Lack of open HW that can run different software flavours
    - Lack of open SW that allows extensibility or the execution of arbitrary agents
    - Lack of fully open APIs that allow external software to interact with the device
- Limited interoperability across vendors that brings significant operational challenges to enable multi-vendor environments
- Lack of features and tooling for zero touch provisioning and initial auto-configuration
- Lock-in to same-vendor pluggable modules
- Unreasonable licensing practices to enable third-party components or to leverage all the hardware resources available

The Disaggregated Cell Site Gateways group in TIP, and this technical specification aims to define an open and disaggregated platform based on commercial off-the-shelf components and open software that can replace traditional cell site solutions – such as proprietary routing appliance and Microwave IDU – reducing deployment and operational costs while providing the scalability required for last mile evolution.

1.2. Scope of the document

The aim of this document is:

- To describe the DCSG platform architecture and requirements that will need to be met by the system in terms of HW and SW features.
- To describe the end-to-end network architecture covering interconnecting aspects between the DCSG and the rest of the network.
- To describe the management of DCSG combined with SDN controllers.

The definition of a detailed low level TRS (Technical Requirement Specification) will be done immediately after the publishing of this document, as a basis for the technical discussion with candidate platform HW & SW manufacturers

1.3. Document Structure

This document is structured as follows:

- Chapter 1: Introduction
- Chapter 2: Platform Architecture & HW/SW specifications
- Chapter 3: Network Architecture
- Chapter 4: DCSG and SDN
- Chapter 5: Glossary

2. Platform Architecture & Hardware/Software Specifications

The DCSG consist of commercial off-the-self HW and open software and interfaces. The main modules/components of the platform are described in the picture below:

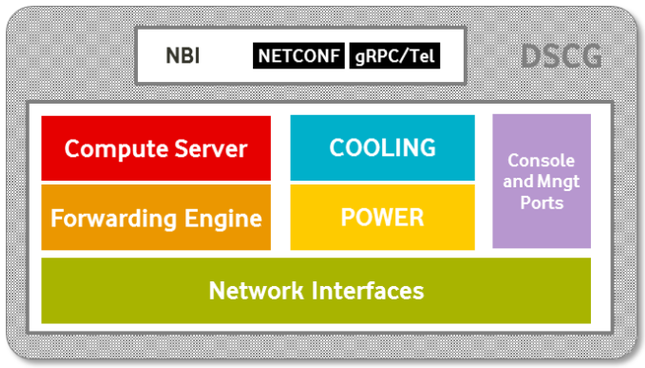

Figure 1. DCSG platform high level architecture components

The system must not impose explicit restrictions that limit the software that can run on it. In other words, the system must allow users to install arbitrary operating systems on it, even if those are implementations from a third-party. If the platform provides the capability to verify that the software has been signed with a particular certificate or cryptographic key, it must be possible to disable such verification at any time, through software/firmware configuration, without the need for any specific or additional license.

When possible, network operating systems for this platform should be provided in the form of binary installers compatible with the Open Network Install Environment (ONIE) specification, as defined by the Open Compute Project (OCP).

2.1. Form Factor, Environmental and Power Supply Requirements

The DCSG will be used in standard cell site locations with DC/AC power supplies, 1U form factor with a maximum depth of 300mm – ideally no more than 250mm to ensure optimal airflow and cabling – for installation in a standard 19” rack (300mm/450mm/600mm ETSI standard rack).

The DCSG airflow shall be Front to back in order to simplify the deployment.

The equipment shall conform to or exceed ETSI standard ETS 300 019-1-3 Class 3.4 (-40ºC to +70ºC):

- -40 to 70ºC, up to 1,000 feet (300m)
- -40 to 65ºC, up to 6,000 feet (1800m)
- -40 to 55ºC, up to 13,000 feet (4000m)

Additional environmental specifications are included in the document below:

Mechanical Characteristics.xlsx

2.2. Network Interfaces and Forwarding Capacity

In terms of forwarding capacity, the DCSG shall be able to cope with current demands (for 3G/4G networks) and also with future and higher capacity demands for 5G deployments. The interfaces shall be Ethernet based and the platform shall support between 8 and 12 of them, working at different speeds from FE to 10GE with two of them to be used for network-facing IEEE 802.by-compliant 25GE connectivity. All the interfaces shall be configurable to work either as UNI or NNI.

For 25G interfaces, support of eCPRI and /or other 3GPP standards will be examined.

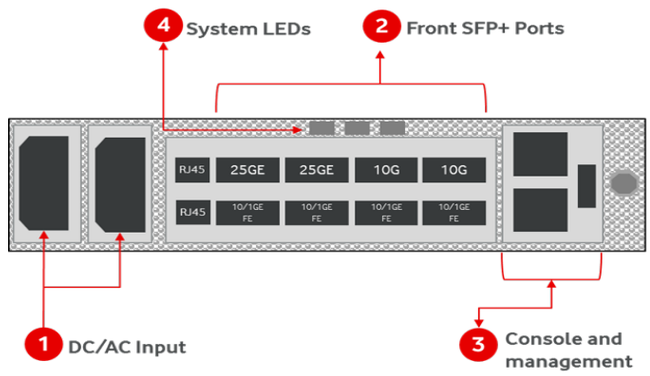

Figure 2. Example of DCSG target front view

The ports shall be able to support SFP/SFP+ pluggable modules that can operate at the temperature range of -40C to +70C range and configurable by software. The platform shall be compatible with a pay as you grow model defined by software licences.

The platform shall be fully interoperable with any 3rd-party pluggable optics (SFP/SFP+), including SR/LR and SX/LX types.

Starting from the same single SKU/chassis, given the available SFP slots, and by using different combinations of pluggable modules, the following standard configurations (SC) are envisioned:

- SC1: 4xGE+1x10G client, 1x10GE line
- SC2: 4xGE+2x10G client, 2x10GE line
- SC3: 4xGE+2x10G client, 2x25GE line

Additionally, the DCSG must provide at least 2 x RJ45 traffic ports (100/1000BaseT), 4 desirably.

One of the SFP ports shall be capable of supporting a pluggable SFP module that can support various time synchronization methods.

The system shall be compatible with fiber optic/electrical transceivers and System-on-an-SFP miniature converters, to transport TDM over packet switched networks (SFP with TDM emulation over packet).

The system shall be compatible with third-party coloured WDM pluggable optics (tuneable & fixed).

Current definition of the DCSG device form factor & capacity does not prevent the definition of additional HW variants with higher number of ports and higher capacity/scalability in the future. In particular, the option of platform stacking for higher scalability could be considered.

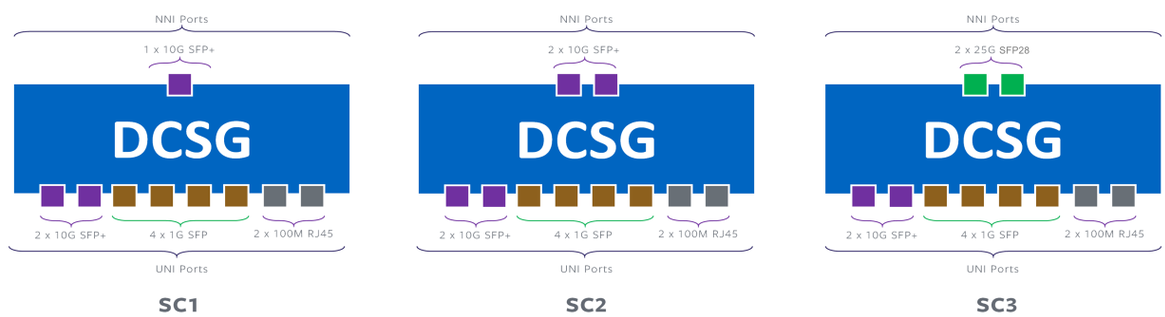

Figure 3. Examples of standard configurations showing SFP+ combinations

In addition to the basic DCSG configuration mentioned above, the operators are open to consider platforms with higher density (higher port count, higher interface speeds, switching capacity, etc.). For example, the following configuration could be a possible reference:

- SC4: 25xGE+16x10GE+8x25GE client, 2x100GE line QSFP28 / CFP4 DCO (in this case for WDM implementation)

With regards SW packages, it should be possible to differentiate between a basic SW license (for a Customer Edge –CE- application), a MW SW license (the equipment works as a MW IDU) and an upgrade license with extra SW capability (to be able to work as a Provider Edge -PE). We could call these packages as Basic SW package (BSW), MW SW package (MWSW) & Provide Edge SW package (PESW).

In the following sections we describe the HW & SW capabilities for the basic DCSG application (working as a CE) and in section **Error! Reference source not found.** we describe the additional capability set for a provider edge (PE) use case. These, jointly with the MW software package, describe 3 levels of SW functionality that can be implemented over the same HW – there shall be no limitations in the HW to support any of these SW packages.

2.3. Management Interfaces and Miscellaneous

The platform shall include a console and a management ports (RJ45) and a USB port as described in the Figure 2, for local configuration & debugging.

The platform shall include status indicators including per port LED and housekeeping interfaces (see excel attached in section 2.1).

2.4. CPU and ASIC

The DCSG CPU shall be based on a x86 architecture, 64bits.

The ASIC shall support line-rate forwarding across all ports without any limitations. The forwarding capacity of the platform shall be able to support all interfaces at full rate with no limitations. ASIC shall support all features and packet types defined in software section.

2.5. Frequency & Time Sync Distribution

The DCSG shall be able to provide frequency and time synchronization to 2G/3G/4G/5G base stations which are connected to it. Additionally, as it will be explained in section 3, the DCSG will be potentially deployed in many different scenarios so it shall also be able receive the time sync signal (e.g. from another DCSG on a ring) and propagate it to other network elements close to it in the network (e.g. to other DCSGs on a ring).

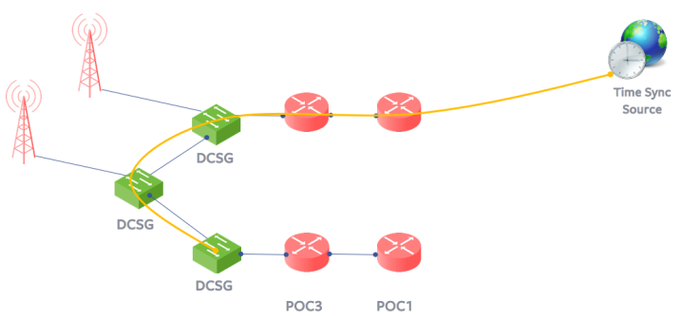

Figure 4. Time Sync distribution example with DCSG

The platform shall support the following time sync requirements:

- Network quality model (microsecond precision) according to ITU-T G.8271.1 Network conditions and reference model where the Boundary Clock is requested to work.
- Node performance (noise generation, tolerance, transfer and holdover) according to ITU-T G.8273.2 Section 7.1/7.2/7.3/7.4.
- Node performance (upon wander, failure, holdover) according to ITU-T G.8273.2 (7.2/7.3/annex) Boundary clock quality objectives in holdover mode
- Interoperability based on IEEE1588 profile defined in ITU-T G.8275.1 with Boundary Clock and SyncE support for holdover purposes and Grandmaster redundant sources support. This requirement corresponds to the support of IEEE1588v2 profile for telecoms – Precision Time Protocol and includes SyncE support in Ethernet interfaces as mandatory as per ITU-T G.8262 and G.8264.

It will be also interesting to receive a detailed information on the electronics used to build up the phase sync regeneration capability (type of oscillator, type of Best Master Clock Algorithm, whether its implemented via SW or HW, etc).

The DCSG shall also support a SFP input for GPS. The platform shall be interoperable with most of the SFP providers' solutions in the market in order to avoid interoperability issues. This GPS input shall be used only in scenarios where the time sync signal cannot be received from the backhaul network through a standard Ethernet traffic port in case time sync distribution mechanisms are used.

The DCSG shall provide a 1PPS in/out external sync interface.

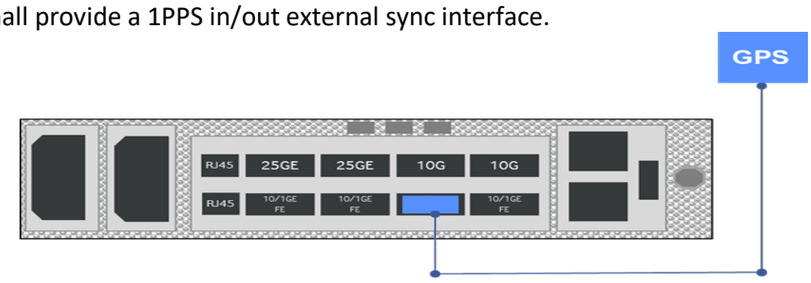

Figure 5. GPS SFP for Time Sync equipped in a traffic port

2.6. MACSec

Current security/encryption architectures for transport networks are evolving and the DCSG shall support the most advanced security/encryption capabilities like MACSec.

The platform shall support the following MACSec requirements:

- MACSec Support
- MACSec Security Mode: Static Connectivity Association Key Security Mode
- MACSec Security Mode: Dynamic Secure Association Key Security Mode
- MACSec hop by hop mode
- MACSec Multi-hop in tunnel mode

The Platform shall be at least HW ready in order to implement the abovementioned capabilities. The activation/support of MACSec shall be available only with a SW upgrade/license activation (w/o HW changes).

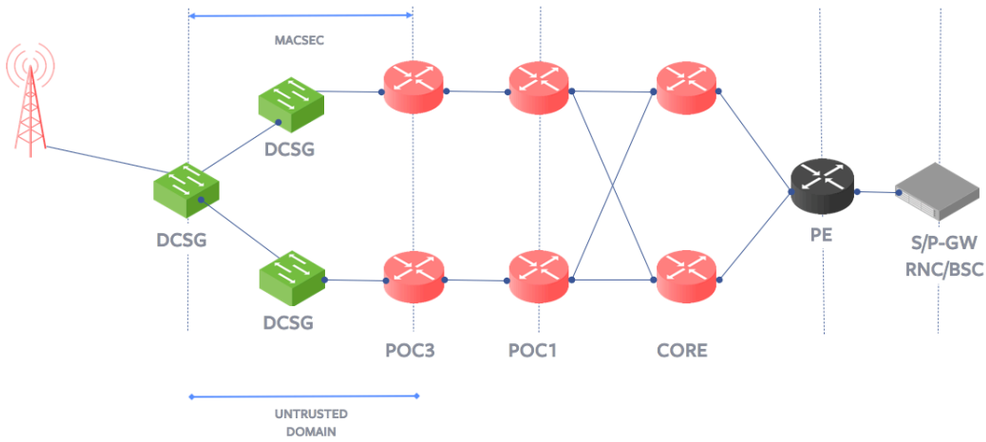

Figure 6. MACSEC application scenario

Additionally, the DCSG shall support EAP – TLS IEEE 802.1x. EAP-TLS will be used in scenarios where MACsec is not implemented.

Finally, the DCSG shall support MD5 for authentication with other NEs/DCSGs.

2.7. Software Architecture

The DCSG is being thought as a modular box, that can run any SW on top of the selected HW versions. In order to ensure the maximum flexibility in terms of the SW that can be loaded in the DSCG, it will be equipped with ONIE. ONIE will enable any operating system to run on top of the DCSG.

ONIE defines an open source “install environment” that runs on routers and switches subsystem. This environment allows end SW suppliers to install the target NOS as part of the initial system setup.

3. Basic SW package (BSW): Customer Edge application

The platform shall support as part of the Basic SW package (as it will be explained in sections 3) features in order to be able to work at layer 3. In order to simplify the architecture and the feature set that the DCSG will use, the L3 capabilities (e.g. OSPF and ISIS) will be used only in the required scenarios.

In terms of L3 features support, the DCSG shall support at least, the following:

- OSPFv2 (RFC 2328)
- OSPFv3 for scenarios where IPv6 is used (RFC 5340)
- eBGP for CE to PE communication
- OSPFv2/v3 for CE to PE communication
- IS-IS for IPv4 supporting Level 1, Level 2 and Level 1 and 2 in any interface of this device.
- IS-IS implementation shall support all standard network-addressing models and in particular for IPv4 and IPv6 compatible mapping.
- IS-IS ready for supporting IPv6 and IPv4/IPv6 dual stack.
- MACSec support (according to Section **Error! Reference source not found.**).
- Support off EAP – TLS IEEE 802.1x. EAP-TLS will be used in scenarios where MACsec is not implemented.
- MD5 support for mutual authentication with other NEs/DCSGs.

The DCSG shall also support dual Stack IPv6/IPv4 (in case the NodeBs are using IPv6 addressing but the backhaul network is not).

3.1. Quality of Service

The DCSG shall be able to perform the following QoS actions for the IP traffic delivered by the 2G/3G/4G/5G base stations marked with the DiffServ Code point (DSCP) value as defined by the GSMA and based on some other parameters as VLAN Identifier and MAC addresses.

Next picture describes the main building blocks to implement IP QoS. A more detailed definition below.

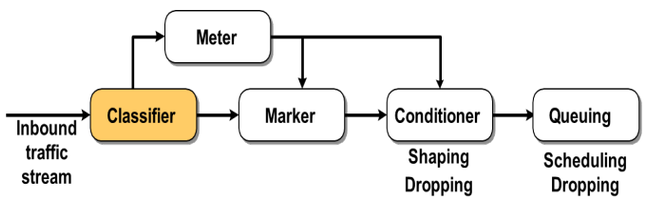

Figure 7. IP QoS implementation

- Traffic classification: The DCSG shall be able to classify traffic in the ingress port based on at least, but not limited to, the following parameters: source MAC address, destination MAC address, source IPv4/IPv6 address, destination IPv4/IPv6 address, VLAN ID (including VLAN stacking), IP DSCP value, physical port, Ethernet CoS field.
- Once the inbound traffic is classified, the DCSG shall be able to apply a policing function to that stream to take a decision to do. The actions shall include, but not limited to:
    - Forward the traffic to the outbound interface without applying any other action (no metering, marking or conditioning).
    - Apply policing (metering) and decide to a) Drop the exceeding traffic over the SLA in the conditioner block, b) Remark the exceeding traffic with a lower IP priority to differentiate between in-profile traffic and out-profile traffic and c) shape the traffic flow to be adapted to the destination user device in order not to be overloaded with burst traffic.

- Once the traffic was classified, metered and eventually taking the action “only forwarded. remarked, or shaped”, the traffic shall be delivered to the outbound interface and store in the output queue system to manage traffic class differentiation before delivering to outbound interface.

Note that not all the functions defined in the blocks diagram are required for all type of traffics but the DCSG shall support all of them to permit to apply the required functions per type of traffic.

- The DCSG shall permit to define policing for any inbound traffic rate defined by the operator and will permit to forward, drop or remark the exceeding traffic.
- The DCSG shall permit to perform traffic shaping to adapt the traffic flow to the destination device; this shall be done in the outbound interface and shall be supported for any rate defined by the operator. The DCSG shall support per physical port, per virtual port (VLAN id) and per group of VLAN shaping. These shaping mechanisms shall work simultaneously.
- Once the traffic goes from the inbound to the outbound interface, it has to be store in the output queue system to treat traffic according to its type and priority. The output queue system shall support at least:
    - Two priority queues for low latency, real time and synchronization traffic.
    - Four weighted fair queues to permit the mapping of the four traffic classes defined in Assured Forwarding (AF) standard. The weigh and the queue depth shall be configured in a flexible way for each of the four queues.
    - For each of the previous WRR queues, three different drop precedence shall be configured to fully implement the Assured Forwarding standard Random Early Discard (RED). The configuration of the RED threshold shall be configured with full flexibility.
    - An additional Best Effort queue with some guarantees shall be also supported for BE traffic.

H-QoS shall be supported by the DCSG due to this functionality will be required in the scenario where two mobile operators implement RAN sharing. The DCSG shall implement H-QoS with at least three levels.

The DCSG shall also be able to map the client traffic classes into the VLAN (IEEE802.1q) tagging values for the scenarios where DCSG is acting at layer 2 (Enterprise scenario). An example (for enterprise traffic) is shown in the picture below:

Class Name	802.p
Premium	5
Enhanced	3
Standard	1
Default	0

Figure 8. Traffic classes

3.2. Performance monitoring and telemetry

The Platform shall support the following performance monitoring requirements:

- ITU-T Y.1564 support:
    - Y.1564 Tech Specifications
    - Y.1564 IOT with Third Party
    - Y.1564 IOT with JDSU
    - Y.1564 Layer 2

  - Y.1564 Layer 3
  - Y.1564 CoS Tests
  - Y.1564 Time Stamping
  - Y.1564 Loopback tests
  - Y.1564 Full line rate
- RFC 5357 TWAMP support:
  - TWAMP Active Performance Monitoring
  - TWAMP Active Performance Monitoring IOT with Third Party Controller
  - TWAMP Sessions & CoS
  - TWAMP Time Stamping Accuracy
  - TWAMP HW Time Stamping
  - TWAMP No Traffic Impacts
  - TWAMP-light support

3.3. Additional Features

The DSCG shall support:

- BFD support including HW based implementation.
- LAG support between UNI interfaces or between NNI interfaces, with Bidirectional Forwarding Detection (BFD) on Link Aggregation Group (LAG) Interfaces according to RFC7130 for faster detection. Ideally, BFD per each individual link in the LAG group.
- Different ports (e.g. 1GE and 10GE) in the same LAG.
- L2 Multicast support capability with IGMP proxy & relay to be evaluated – As an opportunity to extend the applicability of the DCSG to fixed access aggregation.

3.4. Software Scalability figures

As a reference, the following scalability figures shall be supported by the platform SW:

IPv4 prefixes	80K
IPv6 prefixes	40K
MAC table size	80K
Maximum number of IS-IS adjacencies	TBD
Maximum number IS-IS concurrent instances (simultaneous IGP areas the router can belong to)	TBD
Maximum number of NEs per IS-IS area	TBD
Maximum number of prefixes per Global Routing Table	TBD
Support of Jumbo frame (The vendor shall specify the max value in bytes) - min 9k	TBD
Maximum Number of QoS queues	TBD
Queue depth range	TBD
Maximum number of Simultaneously active QoS policies (ACLs)	TBD
Maximum Number of schedulers	TBD
Number of Internet (IPv6/IPv4) routes	TBD

Figure 9. SW platform scalability figures (BSW)

This is just a preliminary scalability table; The final values will take into account the HW cost. And in all cases, these scalability figures need to be encompassed by the platform HW.

3.5. Local Regulation Compliancy

The solution shall be compliant with EU GDPR regulation: REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

For the Brazilian market, the solution must have a Certificate of Conformity issued by a Designated Certification Body and approved/homologated by ANATEL.

3.6. Network Architecture

We introduce here the DCSG deployment models and network architectures where it will be used. These include IP/MPLS, Microwave and Optical network scenarios.

3.6.1. DCSG in IP/MPLS networks

During the last 10 years, network operators have been using different technologies to aggregate mobile traffic, one of the most implemented (probably the most common one) is IP/MPLS.

Implementing full IP/MPLS architectures including the cell sites has been a complex task for network operators, mainly because of the lack of support of some specific features in the smaller IP/MPLS boxes. The objective in this project is to keep the architecture as simple as possible, reducing the complexity of the DCSG and the aggregation network while leveraging on advanced control capabilities provided by SDN.

In this case the DCSG shall work as a simple CE router, running an OSPF instance together with the other DCSGs that might be part of the same ring and the POC3s (the interfaces that belong to the ring will be included in L3VPN) where this ring is closed. The DCSG will be treated in this case as a customer edge connected to the PE routers in the IP/MPLS network. The traffic received from the DCSG will be transported by the IP/MPLS network (as an example) in a dedicated L3VPN till the Core network, as described in the picture below.

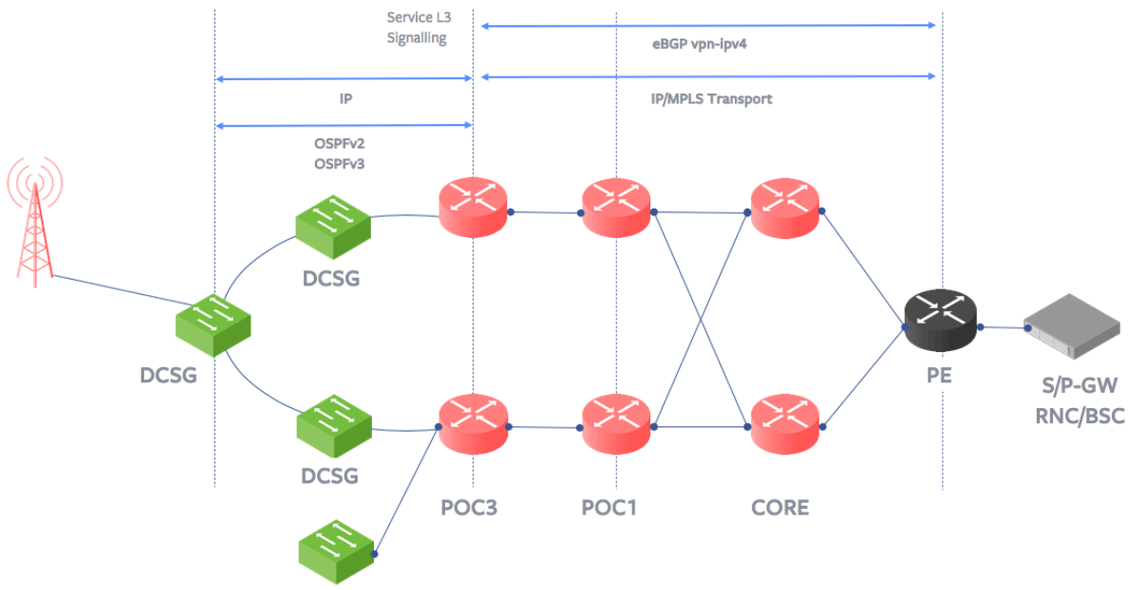

Figure 10. Scenario 1: Dual-home IP/MPLS Ring

The picture describes a network where IP/MPLS is used for performing the E2E transport of mobile traffic (including 2G, 3G, 4G and 5G) from the Backhaul to the Core network.

The IGP protocol will also be used as a protection mechanism combined with Bidirectional Forwarding Detection (BFD) for faster detection in order to achieve better protection times. BFD intervals shall be

adjusted to reduce as much as possible the detection time but also keeping in mind that BFD is quite intensive and will consume a lot of resources of the system. The BFD interval shall be adjusted based on the network scale/size.

The DCSG shall support also OSPFv3 (RFC 5340) to be IPv6 capable. The use of OSPFv3 shall be decided based on the operator network addressing strategy. In case of using ISIS as IGP, it shall be IPv6 ready.

Given the fact that the solution shall be IPv6 capable and the required scalability with regards memory addressing (to allow RAM addressing higher than 4Gb) the best option for HW architecture is to be 64bits based.

3.7. Auto Configuration

The DCSG shall be designed to support auto-configuration mechanisms. The intention is to simplify and automate as much as possible the deployment process. Any additional configuration will be performed by the SDN controller.

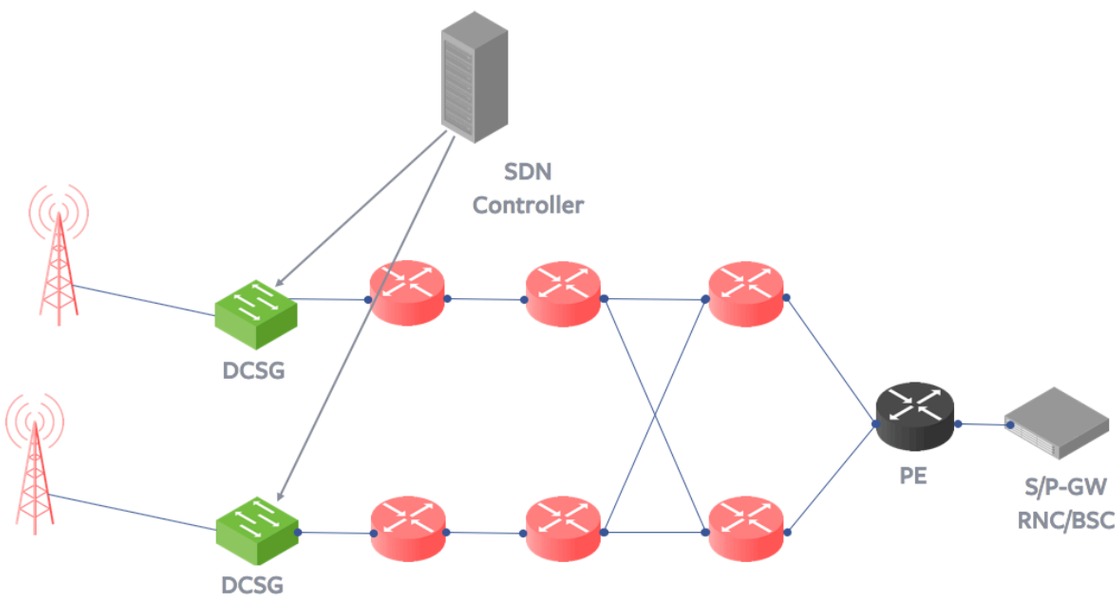

Figure 11. Auto Configuration

The different in-band management models/architectures, depending on the network architecture/scenario, including auto-configuration support, will be described in the following sub-sections.

3.7.1. DCSG Auto Configuration in IP/MPLS Networks

In case DCSG is deployed in an IP/MPLS network (see section 3.1), the SDN controller needs to have connectivity to those DCSGs so it can push the target configuration as soon as the DSCG has connectivity.

In order to automatize as much as possible, the configuration process ZTP (Zero Touch Provisioning) will be used. The DSCG will used DHCP (Dynamic Host Configuration Protocol) to get the location of its configuration file (IP address and path of the file of the HTTP/FTP server). The DSCG will use then HTTP or FTP to download then configuration file located on the server with the most detailed onfiguration.

The DSCG will need to have just access to the DHCP server through a DHCP relay agent in the operator network (e.g. POC3).

In some cases, DHCP could not be a viable solution for executing the IP configuration of the DSCG. In order to cover as many scenarios as possible, the DSCG should have the option to enable by default all the mechanisms that could be implemented in order to grant the connectivity towards the SDN controller that will execute all the start-up configuration.

IPv4 Scenarios without DHCP

In this scenario, the IANA allocated IP prefix 169.254/16 will be used for initial link local communication towards the aggregation device (e.g. POC3). Dynamic Configuration of IPv4 Link-Local Addresses will be used in order to automate the IP configuration based on RFC3927. The DCSG shall use the interface MAC address in order to generate a unique IP address in the above-mentioned prefix. The DCSG shall run also an IGP instance (e.g. OSPFv2 or ISIS). The aggregation device will then have a management L3 VPN where the OSPF/ISIS information is imported and propagated. The SDN controller will be part of that L3VPN as well so it gets E2E connectivity with the DCSG (The DCSG will behave in this case as a CE).

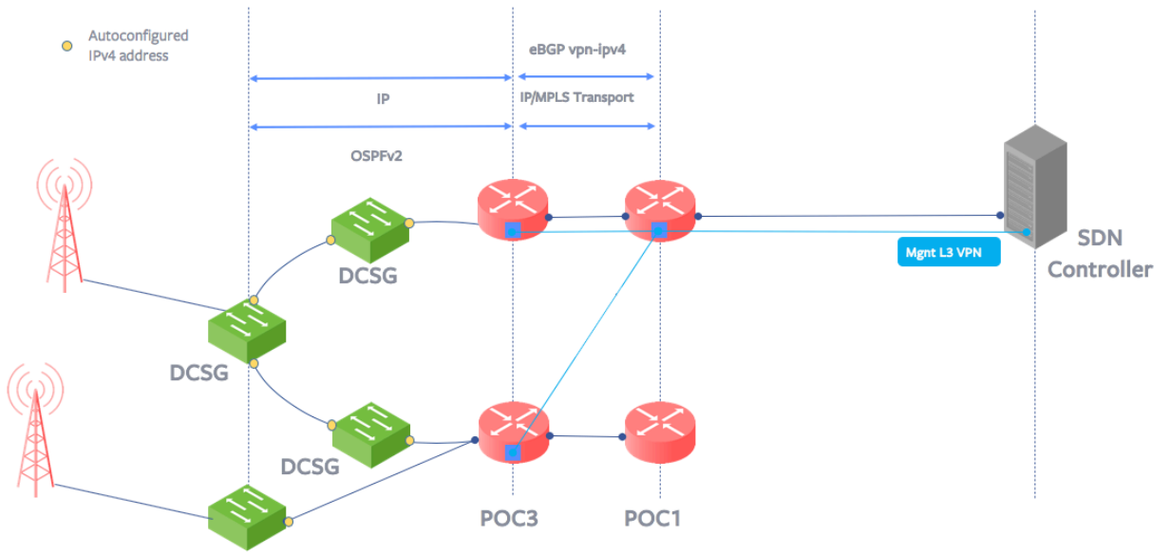

Figure 12. Auto Configuration without DHCP

IPv6 Scenarios without DHCP

The DSCG, as explained before, shall be IPv6 capable. In scenarios, where IPv6 is being used a mechanism is needed that allows a host to obtain or create unique addresses for each of its interfaces (IPv6 EUI-64 addressing mode). Nodes (DCSG) begin the auto configuration process by generating a link-local address for the interface based on the MAC address of this interface. A link-local address is formed by appending the interface's identifier to the well-known link-local prefix. Before executing the autoconfiguration process the DCSG will verify that the address is not already in use. As soon as the process is completed, the DCSG will have IP connectivity with the rest of the Nodes in that network including (other DCSGs or an aggregation box). As explained previously, and OSPF instance (in this case OSPFv3) shall be running by default in the DCSG so all them in the same area able to discover each other and the aggregation boxes that will provide the connectivity towards the SDN controller or management system. The OSPFv3 information will then be exported by the aggregation device into a MPLS L3VPN used only for providing in band management connectivity. The PE then, redistributes the IPv6 routes received via OSPFv3 for that VRF into Multiprotocol-Border. Gateway Protocol (MP-BGP) and advertises VPNv6 routes to the other PE routers. In order to ensure that the addresses are unique in that network, the MAC address shall be used to generate it (EUI-64 standard) together with the well-known prefix fe80::/64.

The intention is to evaluate the feasibility of performing this auto configuration process through the DCSG RFI process

Last but not least, other methods for executing the automatic configuration of the DCSG will be valid, like USB sticks containing the target and previously designed configuration.

4. Microwave SW package (MWSW): DCSG as Microwave IDU

There are some scenarios in which the DCSG could be considered to be used in microwave networks acting as IDU (Indoor Unit). Those cases are limited to the ones where the microwave modem is implemented as part of the ODU (Outdoor Unit)[1] so the IDU needs to implement only basic networking functions (those described in section 3) and support optimal inter-operability with microwave equipment and link peculiarities.

DCSG is connected to the ODU using standard GE and 10GE Ethernet interface. In this case the DCSG receives different service VLANs from the ODU and maps services on L3 network towards the POC3 all the way to the Core.

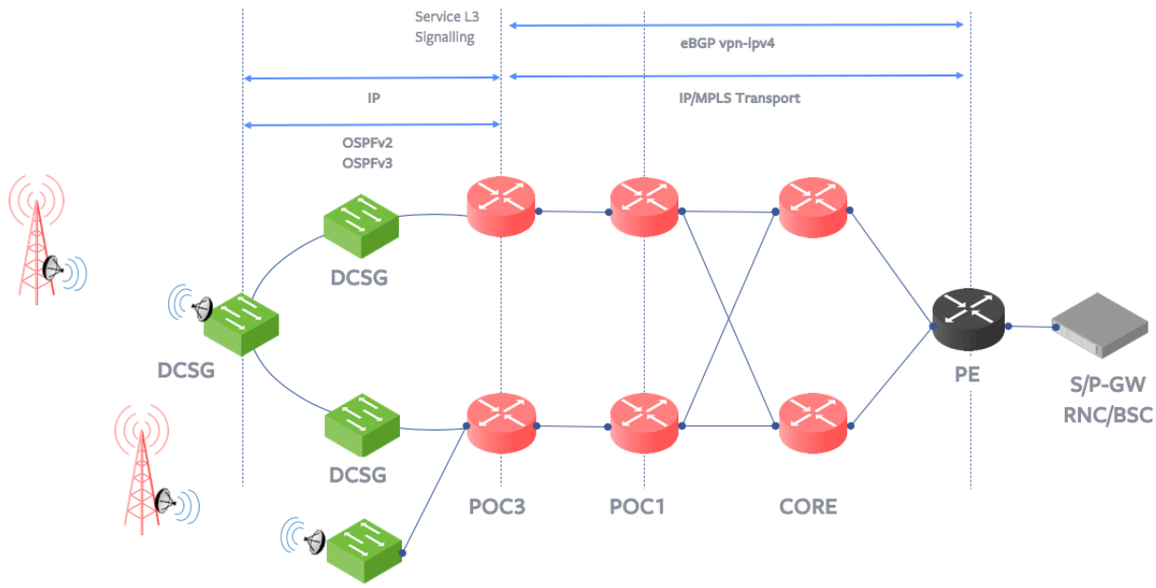

Figure 13. DCSG working as MW IDU

DCSG shall support ITU-T Y.1731 Bandwidth Notification (ETH-BN) in order to be informed in real time on the actual microwave link capacity and to take appropriate actions (e.g. real time traffic shaping); this will ensure DCSG is fully aware of microwave link peculiarity (variable capacity due to Adaptive Code & Modulation, ACM).

DCSG will also provide management connectivity for microwave ODU:

- Towards management platforms (EMS/NMS/SDN controller)
- For local management on Console & Management port of DCSG

4.1. DCSG Auto Configuration in Microwave Networks

In case DCSG is deployed as Microwave IDU the management VLAN used across the Microwave link will be transported by relevant L3 (IP) service on the DSCG towards POC3. Microwave management service

[1] The case of Split Mount microwave (where modem is split from the ODU radio) is not considered for integration in the DCSG. This is because modem is proprietary technology (different across manufacturer and across products of same manufacturer) with proprietary interface towards the ODU.

will be carried by IP/MPLS transport from POC3 allowing communication between the SDN controller and the DCSG as well as the Microwave link

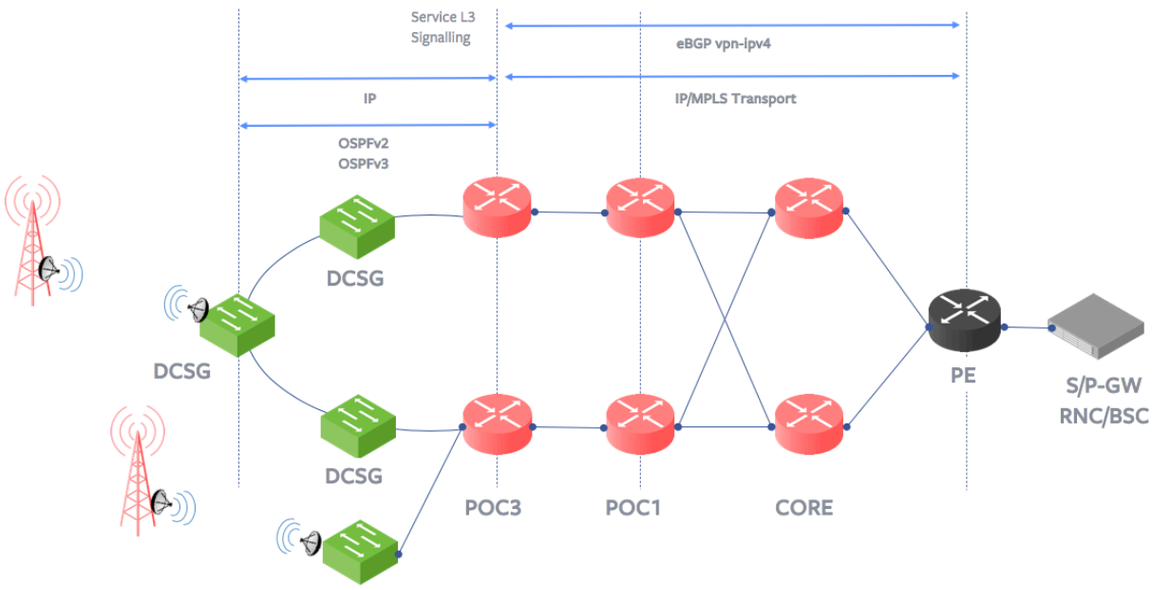

Figure 14. Auto Configuration in MW networks

5. Provider Edge SW package (PESW): DCSG working as PE

The following main capabilities are required to be included as part of an additional SW package to be installed in the platform together with the basic one, for the application of a cell site gateway solution used as a router in backhaul (shown in Figure 15 working as a POC3): This is what we call a Provider Edge application.

In order to enable different software packages, the DCSG solution shall rely on “trusted based” systems so there is no need to have a licensing server or internet connectivity. In most of the cases it’s expected that the SDN controller or the management systems will be able to activate the different software packages based on the operator request.

The main IP & service additional requirements are the following

- Transport requirements
    - Segment Routing (SR) and traffic engineering (TE) extensions. Using as IGP either OSPF or ISIS (both are required in the basic SW package) with one or the other implemented depending on the operator.
    - Segment Routing TE for traffic engineering
    - Segment Routing TI-LFA (Topology independent loop free adjacency) For fast restoration.
    - Segment Routing with MPLS data plane.
    - Additional Segment Routing advanced features (micro loop avoidance, etc)
    - Optional LDP for MPLS LSP transport, for the case that SR is not supported in the rest of the backhaul network
- Service requirements
    - T-LDP (target label distribution protocol) for PW E-line services.
    - MP-BGP (multi-protocol BGP) for standard L3VPN over MPLS and EVPN
    - EVPN (Ethernet VPN) and L3VPN support (VRF, EVI, etc)
    - Routing protocol to the CE (customer Edge) in case of L3VPN (VRF): minimum required static routes, OSPFv2/v3 and external BGP. Optional ISIS
    - EVPN supporting E-LINE, E-TREE & E-LAN (port based and VLAN based)
    - EVPN support with single homing and dual homing (with Hot-Standby and Load Balance in this case)
    - PWE termination into EVPN for L2 services.
    - VxLAN termination into EVPN for L2 services (optional)
- SDN NBI in the DCSG
    - PCEP support for both NE and SDN controller PCE initiated LSP’s (see section **Error! Reference source not found.**)

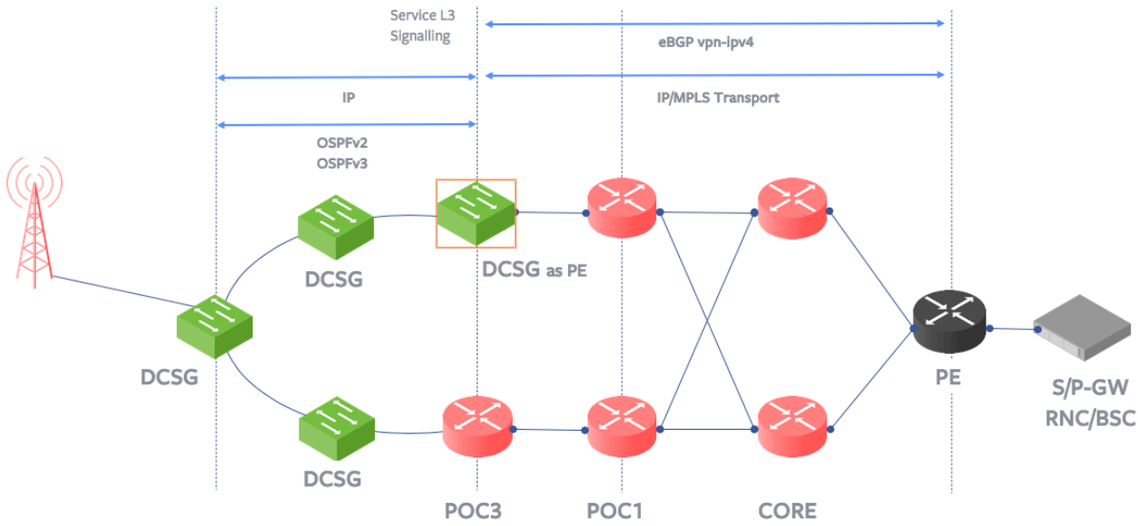

Figure 15. DCSG working as a Provider Edge router (PE) in a backhaul network (orange box)

5.1. L2 service requirements (MEF)

In case the DCSG is used for providing L2 services to enterprise customers (out of mobile access/backhauling context) the DCSG shall be MEF 2.0/3.0 Compliant (E-LAN, E-LINE, E-TREE and E-ACCESS) and will have to be certified accordingly.

The L2 services will be provided by using PWE and/or EVPN over IP/MPLS network

The DCSG shall support:

- Ethernet services must allow customers to use full range for CE-VLANs (4095)
- Y.1731 (OAM functions and mechanisms for Ethernet-based networks) and Y.1564 (Ethernet service activation test methodology) ITU-UT standard compliancy.
- H-QoS shaping
- Quality of service mapping; To set the P-bits on the network port depending on the Color of the service
- ETH CFM according to Y.1731/G.8013. Ethernet OAM IEE 802.1ag. MEF SOAM.
- ETH OAM MEG LEVEL 3 and Level 4

The DCSG shall allow (acting as a NID for L2 services) to do reporting of: Latency, Frame Loss Ratio, Frame Delay variation/Jitter, Availability.

There is also an ask on the DCSG (NID) to be able to perform bearer and service testing RFC2544 & Y.1564 respectively in order to provide real service certification results for the customer, but this will be further detailed in the NID section.

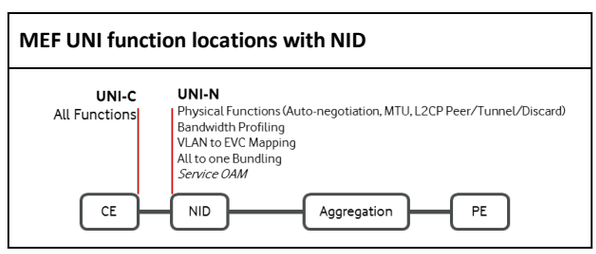

Figure 16. MEF UNI functional delivery model with DCSG working as Enterprise NID

The Metro Ethernet forum specifies multiple different types of UNI described in MEF13 and MEF20. Support of UNI2.1 including the 1522 byte MTU without any further optional attributes is required. This capability will be backward compatible with UNI type 1.0 and 1.1.

5.2. Scalability figures

As a reference, the following additional scalability figures shall be supported by the platform SW together with the PE Software package:

Y.1731 S-OAM flows	4096
Maximum number of VRF per system	TBD
Maximum number of IPv4 prefixes per VRF	TBD
Maximum number of EVI (EVPN instance) per system	TBD
Maximum number of MACs per EVI (EVPN instance)	TBD
Maximum number of customers BGP peers	TBD
Maximum number of networks BGP peers	TBD
Maximum number of BGP prefixes	TBD
Maximum number of T-LDP Sessions	TBD
Maximum number of PW	TBD
Maximum number of labels for SR label stacking	TBD
Maximum number of EVCs	1000
Maximum Number of E-LAN hub	1000
Maximum Number of E-LINE EVPL hub	1000
Maximum Number of logical interfaces for VRF	TBD
Maximum Number of logical interfaces for E-LINE	TBD
Maximum Number of logical interfaces for E-LAN	TBD
Number of VPN (IPv6) routes	TBD
Maximum Number of PE-CE BGP sessions	TBD
SW scalability IPV4/IPv6 simultaneous	TBD

Figure 17. SW platform scalability figures (PESW)

This is just a preliminary scalability table; The final values will take into account the HW cost. And in all cases, these scalability figures need to be encompassed by the platform HW.

6. DCSG and Software Defined Networks

As explained in previous sections, additionally to the CLI support for local & SSH based configuration, the intention is to have a centralised control entity (an SDN Controller) managing the DCSG in a smart and automatic way.

The SDN controller shall manage and optimize the DCSG domains in order to perform SLA fulfilment and service provisioning.

All the configuration and management of the DCSG shall be done using Netconf (RFC 7803). Additionally, the controller will also use BGP-LS to collect all the OSPF-TE/L2 topology information in the DCSG domains.

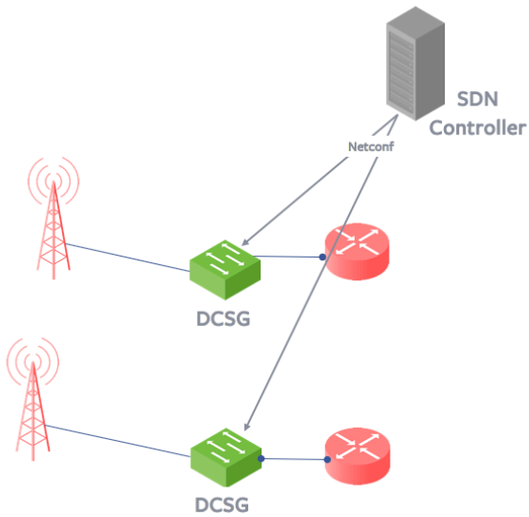

Figure 18. SDN controller and Management

Therefore, the interfaces needed at both the DCSG and the SDN controller are:

- Netconf (RFC 7803); connections could be encrypted using Transport Layer Security (TLS) [RFC5246] or Secure Shell (SSH) [RFC4251], being TLS the preferred option.
- PCEP (Included as part of PESW package in the equipment): DCSG NE shall support PCEP protocol to support PCC (Path Computation Client) function, reporting LSP status in order to use PCEP protocol in NBI interface both to instantiate PCE initiated paths, and modify PCE delegated LSP involving the NE from the stateful PCE placed at the CO. Additionally, it shall support SDN controller PCE initiated PCEP.

Standard data models shall be used as much as possible. The definition/selection of the target/needed models will be done in future releases of this specification. As an example we could highlight OpenConfig YANG models (refer to OpenConfig Data models & APIs web page) which is one of the options under consideration at the moment (pending to analyse full support of DCSG features & capabilities). Current level of standardisation can be seen in the figure below:

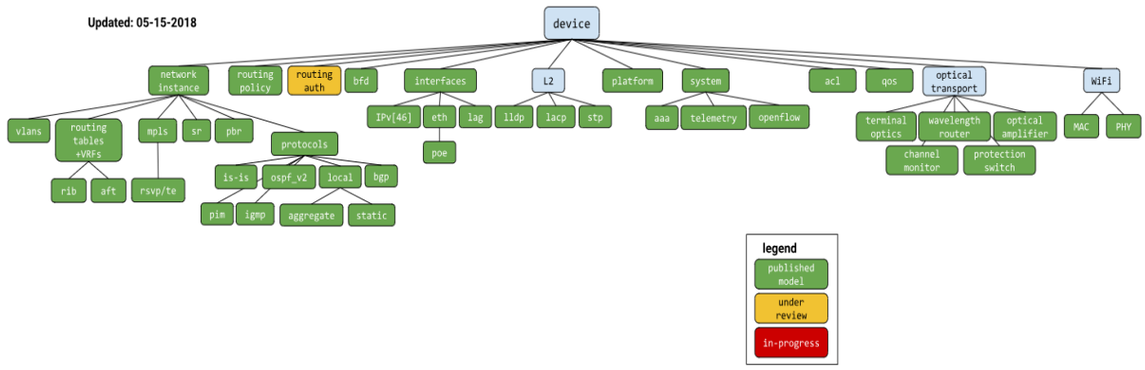

Figure 19. OpenConfig YANG models available (May '18)

In the case of the YANG models not covered by OpenConfig today we can augment with the standard IETF YANG models (for instance OSPFv3 not available at the moment in OpenConfig – see figure) until they are available in OpenConfig

The controller shall support also BGP-LS in order to collect the topology information from the DCSG domains, but the POC3 will act as a gateway for BGP-LS.

Regarding SDN features related to microwave applications, DCSG shall support ONF TR-532 data model.

Additionally, in order to ensure that the DCSG is capable to be integrated with legacy back-end system, SNMPv3 (RFC 3411 / RFC 3418) and SYSLOG (RFC 5424) shall be supported.

6.1. DCSG Telemetry and SDN

As explained in previous sections, the DCSG shall support advanced monitoring and telemetry features. Those features will be used by the SDN controller in order to monitor the status of the platform and the different services instantiated in the DCSG.

Therefore, the features needed at both the DCSG and the SDN controller is:

- gRPC Network Management Interface (gNMI), gPB (Google Protocol Buffers) proto3 for encoding, and data exported (modelling) based on YANG models.

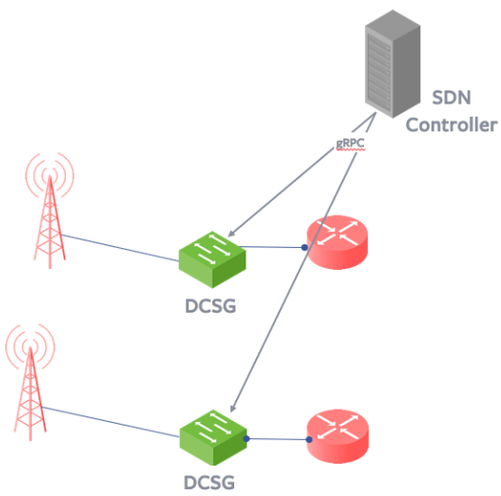

Figure 20. SDN controller and Management

6.2. Access Security and Anti-Theft

In general, the solution must support the necessary security mechanisms to authenticate and encrypt communications between the network element and its management system or controller.

The network element should offer the possibility of only enabling local traffic after the device has been authenticated by the management platform/controller.

The system should also offer the possibility to enable anti-theft mechanisms that prevent the use of the equipment in any other environment than the one it was conceived in.

7. GLOSSARY

BFD Bidirectional Forwarding Detection

CE Customer Edge

IDU Indoor Unit

MNGT Management

ODU Outdoor Unit

PE Provider Edge

PoC1 Point of Concentration 1st level. Highest level on aggregation network hierarchy, connects to the core network.

PoC2 Point of Concentration 2nd level: intermediate aggregation level between POC1 and POC3, sometimes it also aggregates Cell Sites directly. Normally connected to POC1 in ring architectures or slightly meshed, always with optical fibre.

PoC3 Point of Concentration 3rd level. First aggregation point in the hierarchy after last mile/access)

SDN Software Defined Networks

DCSG Disaggregated Cell Site Gateways

BGP Border Gateway Protocol

OSPF Open Shortest Path First

UNI User Network Interface

NNI Network Node Interface

OAM Operations, Administrations, Management

EVC Ethernet Virtual Circuit