

Field trial of programmable L3 VPN service deployment using SDN-Based Multi-domain Service Provisioning over IP/Optical networks

Samier Barguil^{*}, Victor Lopez[†], Cristyan Manta-Caro[§], Arturo Mayoral Lopez De Lerma[†], Oscar Gonzalez De Dios[†], Edward Echeverry[‡], Juan Pedro Fernandez-Palacios[†], Janne Karvonen[¶], Jutta Kempainen[¶], Natalia Maya[¶], and Ricard Vilalta^{||}

^{*}Universidad Autonoma de Madrid, Madrid, Spain

[†]Telefonica I+D, Ronda de la Comunicacion, Madrid, Spain

[‡]Telefonica Movistar, Transversal 60 No 114^a -55. Bogotá, Colombia

[§]Wipro Technologies Ltd., Doddakannelli, Sarjapur Road Bengaluru - 560 035, India

[¶]Infinera Corporation, 140 Caspian Court, Sunnyvale, CA 94089, USA

^{||}Centre Tecnològic de Telecomunicacions de Catalunya (CTTC/CERCA), Castelldefels, Spain

Abstract—Network operators can not change their footprint to upgrade the entire network to support SDN from scratch. This why network operators adapt the original SDN concept into a hybrid SDN approach to have a pragmatic, evolutionary, and economically viable solution. This paper tests an SDN architecture based on a hierarchical structure of a Software-Defined Transport Networking (SDTN) controller, which deals with the end-to-end service provision and topology collection on top of a set of SDN controllers for each technological domain. The authors demonstrate L3/L2 VPN service deployment using an underlay multi-domain IP/Optical networks in a field trial. The approach allows a service provider to migrate brownfield scenarios into SDN domains using programmatic interfaces.

I. INTRODUCTION

Software-Defined Networking (SDN) has emerged as the new reference paradigm to promote network automation and programmability. It has promoted the idea of a radical transformation in all aspects of the: service delivery, network, and traffic management; because end-to-end automatic service provision, automated monitoring, fast issue detection, and event-based decision taking are mandatory functionalities to offer a high-quality customer experience [1].

Conceptually, SDN allows a full decoupling between control and forwarding plane on Physical Network Functions (PNFs). This concept allows the centralization of complex processing tasks and enables integrating white boxes (i.e., smaller equipment, high port density, low processing capacity, facts with generic hardware, and lower production cost) in the network access layers. However, this promise is still not a reality on the service provider networks. Although the term SDN seems new, it has already been more than twelve (12) years since a Stanford team defined OpenFlow and founded NICIRA (NICIRA was the first company to develop a commercial SDN controller (NOX)). Nowadays, despite millionaire investments and several SDN controller solutions available [2], [3] on the market, almost no service provider has a full operative SDN

network controller deployed. Some of the main barriers found by service providers until now are:

- There are still many dependencies on manually executing tasks.
- Network control tasks can not be fully centralized.
- The stack of protocols deployed in the network is very complicated. The knowledge that network operators require to solve problems continues to be very specific.
- Confidence in automation solutions is not very high.
- Many networks have grown via company acquisitions. In many cases internally they operate as independent carriers.
- Standardization is not complete, generating a lack of full interoperability between vendors.

Several new approaches have been gradually released in recent years to adopt SDN as a hybrid solution in brownfield scenarios. Some of the most promising methods were defined using agile methodologies, as software development and IT operations (DevOps) solutions [4]. These agile methodologies usually take a small network task and solve it using a programmatic approach. It allows the simple and more frequent integration of new functionalities. Network provisioning is one of the recurrent tasks selected for agile automation; because it is a diary job that includes the usage of well-defined templates to deploy MPLS-based services on the network.

The Layer 3 Virtual Private Network (VPN) service defined in RFC 4364 [5] provides a multi-point, routed service to a customer over an IP/MPLS core. L3VPNs are widely used in carrier-grade networks to deploy 3G/4G, fixed, and enterprise services. Traffic policies can be applied in these services to reuse the same transport network, and it also makes it feasible to combine access technologies over an MPLS core. On the other hand, L2 services belong to the class of IP virtual leased line (VLL) services or virtual private LAN (VPLS) services

[6], which are a fundamental part of the service portfolio offered by service providers.

This work proves the viability of the implementations of programmable network interfaces for the deployment of L2/L3 services in IP over optical networks using common standard models and protocols. A field trial including multiple network controllers (two for IP/MPLS and two for DWDM) and a real-commercial-multivendor-operative network was installed by Telefonica in their premises in Colombia to validate the concept.

The paper is structured as follows: Section II provides a review of the State of the Art both on the provisioning of automated L2/L3 VPN services. Section III describes the SDN reference architecture and details the principles of the network programmability, including concepts of YANG and used protocols. Then, Section IV details the test architecture, including commercial network controllers and the results obtained in this implementation. Finally, conclusions and perspectives are drawn in Section V.

II. STATE OF THE ART

The IP service models are YANG modules defined to support the creation, deletion, and retrieval of L3/L2VPN services and the IP/MPLS network topology collection. The models used in this work are abstract models that technologically describe the network requirements and are RFCs or working-group-drafts inside the IETF.

1) *L3VPN Service Model (L3SM)*: Multi-Protocol Label Switching (MPLS) Virtual Private Networks (VPNs) have seen an unparalleled increasing adoption during the last years. Although their flexibility as transport technology and their effectiveness for traffic engineering are well recognized, VPNs are hard to set up, operate, and manage, due to the complexity of the network, the protocols involved, and possible multi-vendor parameter discrepancies.

Some service models have been defined and standardized until now to support the L3VPN creation. L3SM [7] is a Customer Service Model that describes an L3VPN service's configuration parameters based on customer requirements. The L3SM model keeps some commercial customer information as the "customer-site-location". This model provides an abstracted view of the Layer 3 IP VPN service configuration components. However, it is mainly focused on BGP PE-based VPNs and doesn't have specific parameters to configure the different network elements in multi-vendor scenarios nor has the possibility to bind the services with specific transport options inside the MPLS network.

L3NM [8] is a complementary Network Model of the L3SM. It differs from the L3SM because it is entirely network-centric and groups all the provider edge routers (PE) configurable parameters. Network controllers can expose the L3NM to manage and control the VPN Service configuration in multi-domain scenarios. It contains valuable information to operate the service, such as each network element's identifier in the IP/MPLS domain (NE-ID) and the interface identifier of each

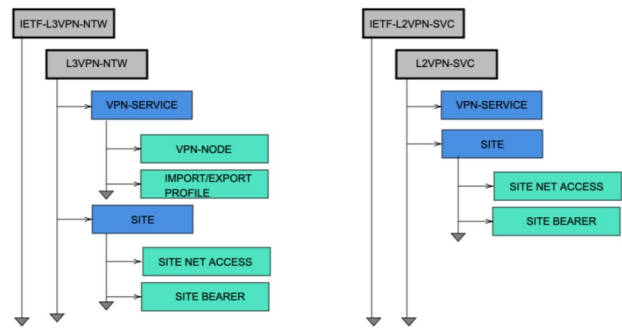


Figure 1: L2NM and L3 Data models structures. The hierarchy represents a container in the YANG model. The lines represent cross references between the containers.

customer access. It includes resources such as Route Targets (RTs) and Route Distinguishers (RDs).

L3NM is populated based on the services request (f.i. L3SM query) and an SDN controller includes network-specific information in the message sent to the domain controllers like transport LSP binding, routing profiles, or encryption profile. It assigns logical resources such as route targets or route distinguishers to keep the data synchronized between domains. Figure 1 shows the structure of the L3NM YANG data model, where the main container (VPN Service) is used to group the information of the VPN-Node (VRFs) and the VPN-Network Accesses (Interfaces).

2) *L2VPN Service Model (L2SM)*: Similarly, the IETF has standardized YANG models for the L3VPNs; there is already a standard for the L2 services. The model is named L2SM [9].

The L2SM is a customer-centric model; It has two main sets of parameters, the VPN Service and the site information. The fig. 1 depicts the main components of the L3NM and the L2SM as a tree structure. The VPN service contains all the technological parameters of the services that are going to be deployed, for example, service type or service topology. The "site" includes all the customer information, like the "customer-location" and the access parameters between the Customer-Edge (CE) and the Provider-Edge (PE).

This model lacks some specific network parameters; those need to be stored or derived by the network controller to deploy the network device's configuration. For futures implementations, additional work to complement the current standard can be proposed.

III. SDN ARCHITECTURE

iFUSION is a reference model architecture defined by Telefonica to reinforce the network automation and programmability in a service provider environment. iFUSION is hierarchical, with specific domain controllers per technological domain (IP/MPLS, microwave, optical) and a hierarchical controller to provide real-time control of multi-layer and multi-domain transport network resources. The iFUSION main principles

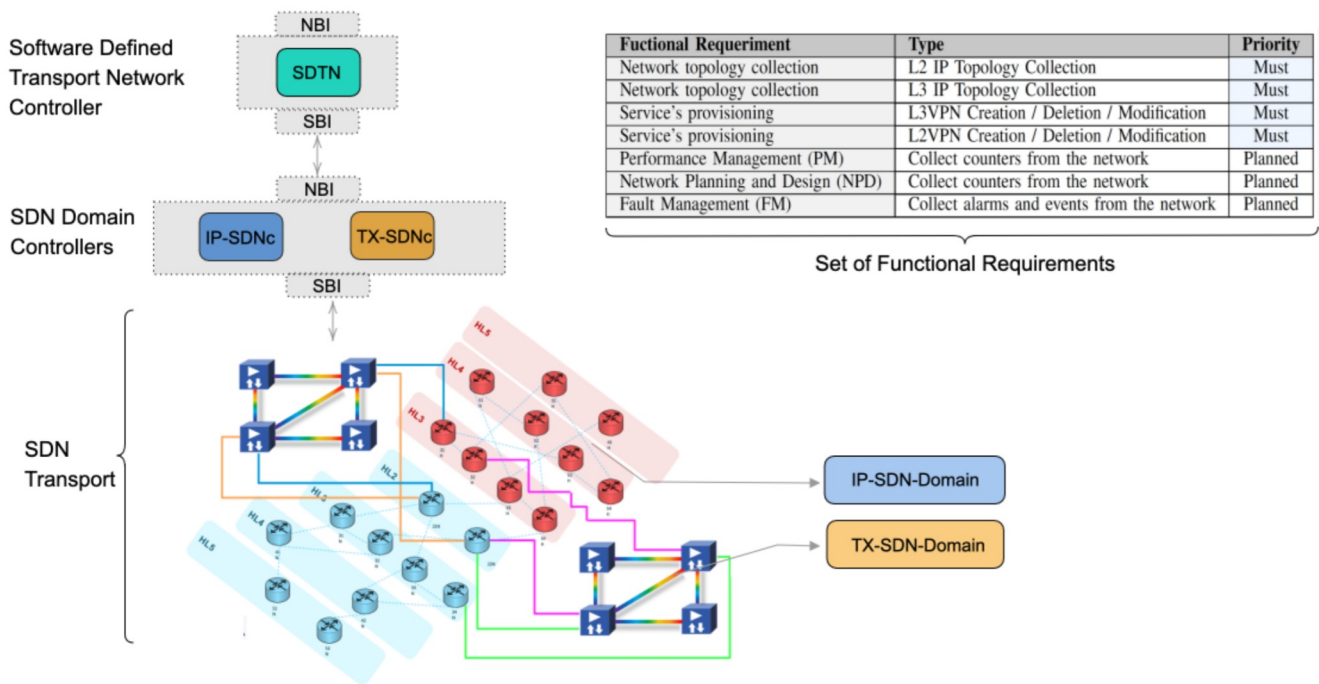


Figure 2: iFUSION [10] architecture has two control layers. The first one having the SDTN controller with the end-to-end view of the network. Second control layer includes the SDN Domain controllers. Those controllers interact with the network devices (Fusion Network). The set of use cases Tested in the POC are listed.

include the use of: (1) Standard interfaces based on RESTCONF/YANG [11] for the communication between controllers and NETCONF/YANG [12] to configure the network elements; (2) YANG data models based on latest developments in the standards-development organizations (SDOs): IETF, ONF and OpenConfig.

The main elements of the SDN iFUSION architecture are the following:

- **SDN Domain:** It is a set of network elements under the supervision of the same SDN Controller. There are several possible levels in the decoupling of control and data planes. The preferred level of decoupling depends on the network technology. For example, network element runs the distributed protocols (e.g. IS-IS TE, RSVP-TE) in MPLS, and the controller only needs to configure it.
- **SDN Domain Controller (SDNc):** This element is in charge of a set of network elements. It has standard southbound interfaces that depend on the technology, but not in the equipment vendor, to communicate with the network elements. It also has a northbound interface to communicate with the SDN Orchestrator and the OSS.
- **Software Defined Transport Network (SDTN) Controller:** In case several SDN Domains are needed, the SDN Transport Controller is in charge of providing services through several domains.

The iFUSION architecture was designed as a hierarchical model where a dedicated SDN Domain controller controls

each network segment. Due to its complexity, the transport network is divided into three main technology domains: IP, Optical for transmission, and Microwave. The proposed architecture can be shown in terms of components and relationships among them, as depicted in fig. 2.

The SDTN Controller is responsible to orchestrate the respective SDNcs within the transport segment (IP, Optical and MW) through the Domain Controllers' NBI, providing an end-to-end transport network vision. The SDTN Controller aggregates demands from the management and services layer exposing a unified NBI which should provide resource configuration abstraction and technology agnostic service definition.

A. IP Domain

Traditionally IP networks are deployed following a regional model mixing equipment from different vendors. The IP boxes are interoperable at both data and control plane levels (e.g., routing protocols such as IS-IS, OSPF, or BGP). Due to scalability and resiliency reasons, the IP administrators divide the whole network into IP domains, so the routing and control protocols are the same in an administrative area.

The goal SDN solution for the IP segment is composed of a single IP SDN controller, whose goal is to configure all the IP network elements. The target SBI for vendor-agnostic device configuration shall be compliant with NETCONF standard protocol. Due to the maturity level, the set of device configuration data models are the ones defined used in iFUSION

are OpenConfig. It is expected that the IP SDN controller will assume the control/management of:

- Device configuration of interfaces (VLANs) and routing protocols (BGP, ISIS, ...)
- Traffic Engineering of MPLS tunnels (LSPs).
- Overlay networks services (L2/L3 VPNs) device configuration (VRFs, ...)

The IP SDNc will be the main entry point to the network elements, to avoid overloading the elements with external requests and providing a full and coherent network view. The NBI of the controller in iFUSION follows IETF YANG models and they are implemented on RESTCONF with JSON encoding.

B. Optical domain

Optical transport networks from different system vendors are deployed on a regional basis, either for technology redundancy, due to different optical performance requirements (metro vs. long-haul), or simply for commercial reasons.

Without line-side interoperability of the different optical transceivers and Reconfigurable Optical Add-Drop Multiplexers (ROADMs), there is not a competitive advantage on a uniform configuration interface of the optical devices, since they cannot neither be mixed in a multi-vendor scenario, due to the fact that both line systems and transceivers must be from the same vendor.

With this in mind, in the short term, Optical SDNc are expected to provide network programmability and interoperability towards upper layers (multi-layer) and between vendors (multi-domain, multi-vendor) through the support of standard NBIs (i.e. coordination will be provided by upper layer hierarchical SDTN). This short term approach will enable the setup and tear down of connections in optical channels (OCh and ODU layers), the discovery of the network resources to compose a layered uniform view based on the OTN hierarchy, and the monitoring of the optical network in a vendor agnostic fashion thanks to the utilization of ONF Transport API (T-API) 2.1 [13], having been experimented in several proof of concepts [14]. Please note, that in this transport domain, T-API + RESTCONF is also proposed to be the NBI of the hierarchical SDTN Controller towards Service B/OSS layers.

In the medium and long term, the direct programmability of the components can have interest in Point-To-Point, Metro and Regional scenarios, where disaggregation of optical transceivers and line side components can play an important role. In this line, OpenROADM [15] and OpenConfig projects have already defined device configuration models for transponders and open line systems.

C. Integration of SDTN in the overall operator's systems architecture

One of the main reasons for deploying an SDTN controller is service automation. It facilitates that manual services and network configurations become automated and available through its NBIs, enabling the network automation progressively. As the main design principle, the abstraction level

provided by the SDTN can be different based on the needs of consumers. Thus, the information exported through the NBI towards OSS and other platforms will cover several functional areas with several levels of abstraction: (1) network topology, (2) service provisioning, (3) performance management, (4) network planning and design, and (5) fault management.

Network topology and service provisioning are tested in this paper, the full set of use cases tested as described in the fig. 2. Progressively, the SDTN will include the rest of the functionalities (marked as planned). On its SBI, the SDTN will integrate with the domain controllers. Each SDNc shall expose vendor-agnostic network-level programmability and resource discovery functionalities. So the SDTN will be able to perform the correct data integration and functionalities exposure.

D. Multi-domain IP L3VPN provisioning

The L3VPNs services are not exclusive of single domain implementations; multi-domain IP L3VPN is a common requirement in the service providers. Multi-domain services include: multiple-AS, multiple-IGPs, or multiple-vendor segmentations. Based on this, a set of interactions with more than one IP SDNc may be required to accomplish the service provision process.

The scope of this work includes two IP domains connected by a common core; The IP domains were part of a different IGP process, so each network has its own IP SDNc. Each of the controllers has implemented the IETF L3NM model described in subsection II-1 to support the service creation requirements. We have proved the SDTN as a network orchestrator to create a multi-domain L3VPN, delegating the required provision parameters to each domain controller and after exposing a unified view of it.

The parameters delegation done by the SDTN had the following four steps per domain.

- 1) Create Site: Indicates the place where the services endpoints are located. It include magement information and service descriptions.
- 2) Create Bearer: Indicates the NE and the Port assigned to the service.
- 3) Create VPN-Node: Indicates the VRF deployment and all its attributes on the PE. It includes the import/export policies.
- 4) Create Site Network Access: Refers to the CE-PE connectivity attributes. Such as routing protocol exchanged, IP addressing or ethernet encapsulation.

Figure 3 depicts the corresponding workflow to create the L3VPN. Each step in the figure matches the sequence previously described. A similar workflow was used for all the RESTCONF operations like Create, Read, Update and Delete.

IV. FIELD TRIAL ENVIRONMENT FOR iFUSION SDTN DEMONSTRATION

In this work, we have deployed the iFUSION architecture in a Telefonica Colombia field trial environment. The field trial includes not just the iFUSION SDN control layer

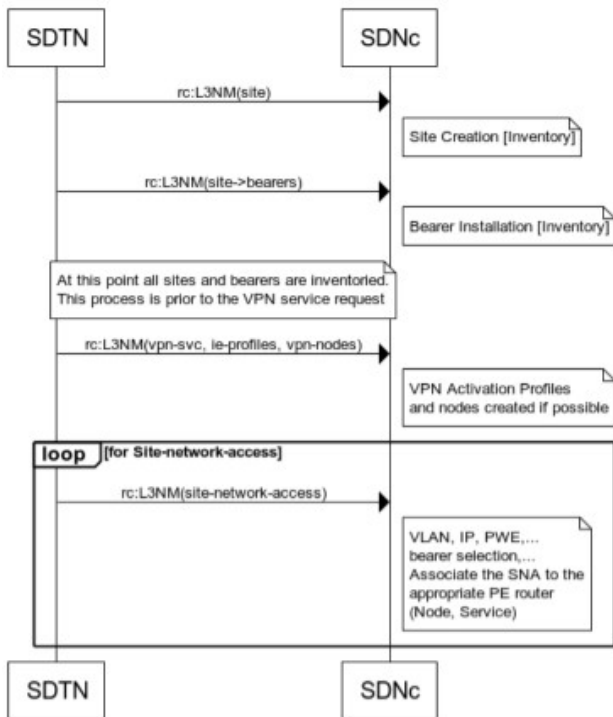


Figure 3: Messages Interchange for IP multi-domain L3VPN service creation.

(Section IV-A), but also the network elements described in Section IV-B.

A. SDN Control Layer

The SDN control layer architecture was built upon the reference design guidelines described in Section III. The key elements of the control layer was:

- Infinera Trascend Maestro, acting as SDTN controller.
- 2 x IP SDNcs one for each IP domain.
- 2 x Optical SDNcs one for each optical domain.

SDNcs communicate with NEs via NETCONF/YANG and RESTCONF/YANG with SDTN using the Data Communication Network (DCN). The optical and IP SDNcs are commercial products from the network element vendors.

B. Network Elements

The set-up for this field trial uses a full network with all the Hierarchical Levels (HL) that compose a Service Provider real environment. In our notation and architecture the IP/MPLS-based network is comprised of five (5) HLs with the following responsibilities:

- HL1: Core PE-Routers acts as Toll Gates for the Service Provider's interconnection with other carriers and using eBGP logical structure for publishing public IPv4/IPv6 prefixes.
- HL2: Core P-Router is responsible for the transportation of traffic between main cities and metropolitan areas sending/receiving traffic to HL1 interconnections from/to

the International Internet. Two (2) vendor B routers were used as HL2. The core routers run in an isolated IGP domain.

- HL3: PE-Routers are responsible for the aggregation of traffic from metropolitan and regional areas for both fixed and mobile services. Moreover, some HL3s provide connectivity to 4G/5G platforms (EPC, packet core, etc.). Four (4) routers were used as HL3s, distributed in two IGP domains (two for each vendor).
- HL4s collect traffic from fixed access networks (DSLAM/CMTS/OLT) in metropolitan areas and high capacity corporate services. Five (5) routers were used HL4 devices: three (3) for vendor A and (2) for vendor B. Each PE has connectivity to the both HL3 routers of its island.
- HL5: Cell Site Routers connects corporations, enterprises, small businesses and mobile terminal nodes (BTS, NodeB, eNodeB) in remote areas. Formerly known as cell site routers in Mobile Service Providers, but they evolved and converged to serve multiple fixed plus mobile segments. One HL5 was used in these tests from vendor A.

The IP/MPLS network was build using seamless MPLS option-C. Clusters and rings organized the network—IP clusters groups devices of a specific vendor. As a seamless MPLS, the underlay signaling requires that every origin PE-Routers (HL4) from a cluster can establish an end-to-end path to the destination PE-Router (HL4) even if the destination belongs to a different cluster.

Thus, the HL3 routers from each region establish an eBGP session against the Core-Routers (HL2). This session exports the Router-ID plus Label information of all the routers in the region using BGP label unicast (LU). Additionally, another eBGP session between the HL3 of the region and the core Router-Reflectors to export the VPNv4 routes from each VPN service. This eBGP session requires a mandatory Next-Hop-Unchanged configuration to avoid network loops or misconfigured paths.

Two-vendor WDM infrastructures transported the IP/MPLS links of vendor B HL2s and vendor A HL3s. The optical transport infrastructure was built as two independent metropolitan optical networks. We used (4) four nodes in each optical network with 100Gb and 10Gb lambdas for these experiments.

C. Multi-domain IP L3VPN provisioning

This section presents the test results for the Hierarchical SDTN Controller integration with the controllers in the IP/Optical domains. Two types of tests have been done to demonstrate orchestration functionalities in the multi-layer/multi-domain/multi-vendor network environment, as depicted in Figure 4. In a first stage, each SDN controller was validated individually. RESTCONF-based queries were sent towards each of the SDNcs to change and retrieve the network information and validate each implementation's compliance. This initial certification aimed to make functional tests over each solution and speed-up the entire solution's

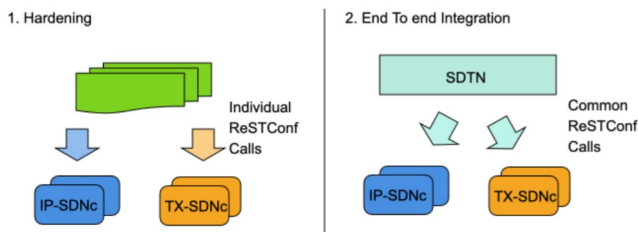


Figure 4: The two types of tests have been done in order to demonstrate orchestration functionalities in the multi-layer/multi-domain/multi-vendor network environment . (1) Hardening process includes single domain tests. (2) End to end integration includes the SDTN delegation of resources to the domain controllers.

final integration. The scalability and efficiency of the SDTN solution is limited to the SDNc performance.

Once each domain controller was independently certified during the individual validation process, the end-to-end integration was done using multi-domain functional tests. In that case, the Transcend Maestro GUI was used to orchestrate the entire service lifecycle. For example, to create a service between two domains, the SDTN provided a Graphical template to fill the service creation parameters. The parameters depicted in Figure 5 includes the user-defined configuration requirements and the auto-assigned parameters by the SDTN. In both cases, the SDTN stored the whole service resources, and It continuously monitors the network state to keep the set of values synchronized. The workflow used is by the SDTN is depicted in Figure 3. Each time a user created a service, a set of request calls was instantiated between the SDTN and the corresponding SDNc. Finally, once the SDNc confirms the service creation to the SDTN, the Transcend Maestro provided three visualization options: (1) Service details, (2) Geographical view, and (3) Layered view, as depicted in Figure 5.

- 1) The VPN service details including the service name, the topology and end-points.
- 2) The service route in the topology view, this view includes the full path including the IP and Optical devices compromised in the service.
- 3) Layered view of the service. This view splits the service connections between layers, so the IP Links connection is in the top. The Ethernet connections between routers are in the second layer and physical plus optical layers are decoupled in this hierarchical structure.

The configuration of the IP L3VPN service in the network elements was verified by using their command line interface as well as the IP-SDN controllers GUI. To validate the data plane, a traffic generator was used in site to introduce traffic on both ends of the network and tested the multi-domain L3VPN service. Figure 6 shows the traffic statistics as seen on the command-line interface of the PE routers. In this figure, the two interfaces connected to the VPN services are selected, and

their traffic counters are showed. The occupancy of the 10G ports is close to the 95% during the test.

V. CONCLUSIONS AND FUTURE WORK

A key angular stone for the SDN adoption in service provider networks is the definition of the data models and protocols to be used by the architecture components for the integration between them. Historically, integration using proprietary interfaces delay the introduction of programmability and automation and have a high economic cost. In this work, RESTCONF with IETF YANG models was tested for the integration between the SDTN and the IP SDNcs. The main focus was the validate a standardized API to provision and retrieve services to a multi-vendor underlay network.

The tests included the provision of L3VPN using IETF YANG data models and the topology collection. The SDTN orchestrated the service creation assigning the resources to each domain controller. During the service retrieval, the SDTN composed the services based on the information exposed by the domain controllers.

For additional tasks, there are still gaps to cover all the IP/MPLS network operation requirements. A brief summary of the issues faced during the integration, as reference point to future work are:

- Connectivity, latency and internal processing times between the HCO and some of the SDNcs can impact the integration and result in miscommunications creaking the timeout of SDN transport protocols, ie. RESTCONF and NETCONF.
- *Ghost* objects which would not be completely deleted in the controllers can lead to misunderstand in the topology construction.
- The unsolicited data retrieved by a lack of standardization or a bias in the implementation of the standards can lead to uncompleted transactions or loops in execution tasks.
- Absence of data in the SDN domain controllers for an automatic inter-domain link discovery.
- Differences in the RESTCONF/YANG implementations on the SDN Controllers. Even if the YANG models were the same, the parameters translation between NBI and SBI can restrict some configurable parameters (i.e max length size of a description field) and may generate implementation differences. This would derive in possible errors during the execution of the creation process.
- Differences in the RESTCONF/YANG error handling. A set of well defined error codes is mandatory in the hierarchical architecture.

The APIs designed in this work demonstrates the viability of the iFUSION architecture with an SDTN orchestrating an underlay multi-vendor, multi-layer, and multi-domain network environment. The iFUSION APIs allow any service provider to migrate brownfield scenarios into SDN-ready domains using programmatic interfaces.

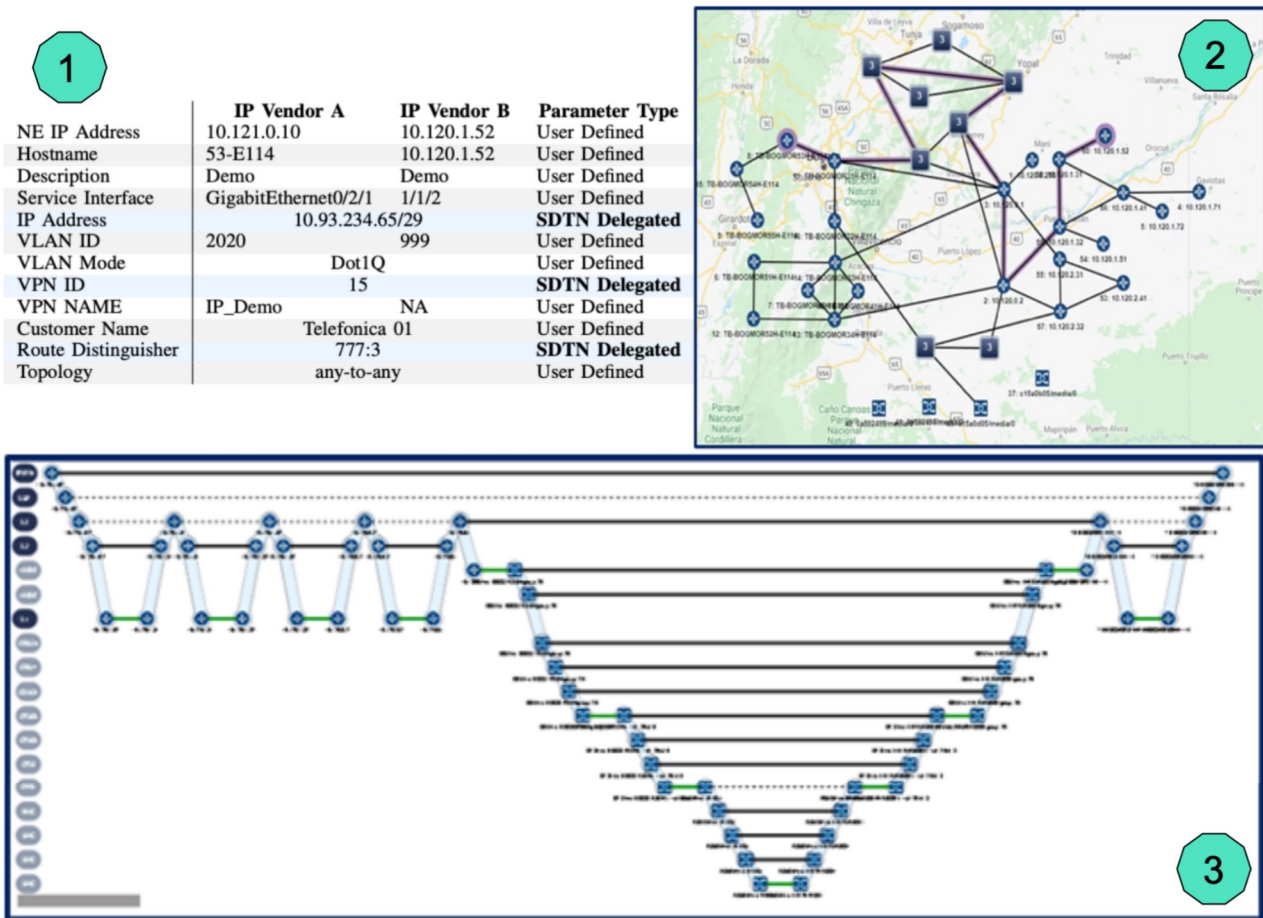


Figure 5: L3VPN service creation results retrieved from the SDTN GUI. Included three visualization panes: The service details (Name, Topology, RD and Endpoints), the geographical view and the hop-by-hop connection view.

A. Future Work

As future work, the hybrid SDN deployment done until now must be complemented with an integration between the NBI exposed by the SDTN and the OSS applications ecosystem. The OSS ecosystem can include for example strategic and tactical planning applications, able to support the year by year demand management and planning tasks done within the organization. A common interface defined and available for these tasks would allow the OSS systems providers to focus on the quality of the applications developed, forgetting the complexity of the network management. Economically it will generate direct reductions in the applications integration time.

ACKNOWLEDGEMENTS

This work has been supported by Telefonica I+D as part of the Fusion, iFUSION, OpenFusion projects and partially funded by the EC 5GPPP TeraFlow (101015857) and MINECO AURORAS (RTI2018-099178-B-I00). Authors would like to thank to all the SDN technical teams and leaders that participate in the development, deployment, and testing of this SDTN architecture. Many thanks for their contributions to

Manuel Santiago, Gloria Gomez, Julia Rodriguez and Zdravko Stevkovski from Infinera, Randy Quimbay, David Rocha from Telefonica Colombia, and Andrea Valencia, Juan Suarez, Juan Agredo and Daniel Hernandez from Wipro.

REFERENCES

- [1] J. Ordonez-Lucena, P. Ameigeiras, D. Lopez, J. J. Ramos-Munoz, J. Lorca, and J. Folgueira, "Network slicing for 5g with sdn/nfv: Concepts, architectures, and challenges," *IEEE Communications Magazine*, vol. 55, no. 5, pp. 80–87, 2017.
- [2] J. Medved, R. Varga, A. Tkacik, and K. Gray, "OpenDaylight: Towards a model-driven sdn controller architecture," in *Proceeding of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks 2014*. IEEE, 2014, pp. 1–6.
- [3] P. Berde, M. Gerola, J. Hart, Y. Higuchi, M. Kobayashi, T. Koide, B. Lantz, B. O'Connor, P. Radoslavov, W. Snow *et al.*, "Onos: towards an open, distributed sdn os," in *Proceedings of the third workshop on Hot topics in software defined networking*, 2014, pp. 1–6.
- [4] T. Choi, T. Kim, W. Tavernier, A. Korvala, and J. Pajunpää, "Agile management and interoperability testing of sdn/nfv-enriched 5g core networks," *ETRI Journal*, vol. 40, no. 1, pp. 72–88, 2018.
- [5] E. Rosen and Y. Rekhter, "Rfc 4364-bgp/mpls ip virtual private networks (vpns)," *Internet Engineering Task Force (IETF)*, 2006.
- [6] L. Andersson and E. Rosen, "Framework for layer 2 virtual private networks (l2vpns)," RFC 4664, September, Tech. Rep., 2006.

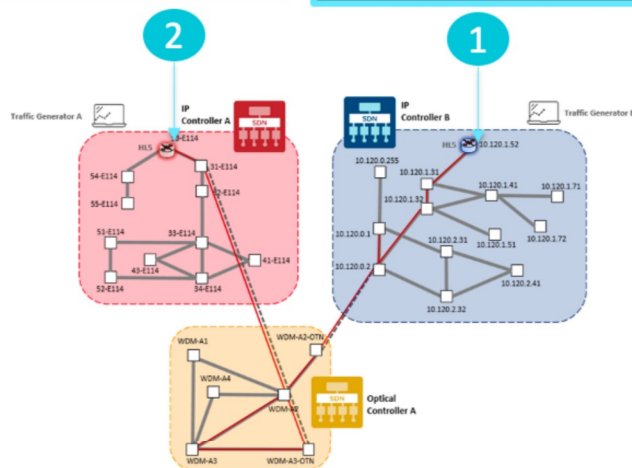
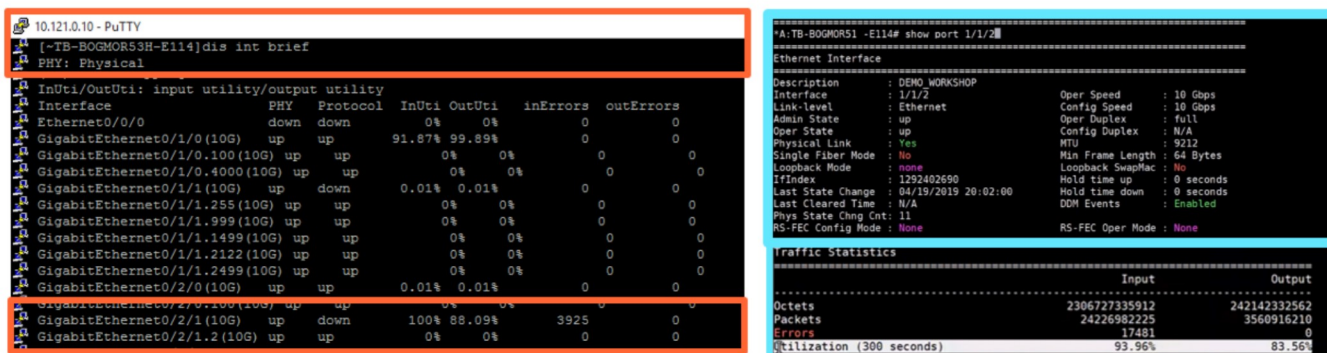


Figure 6: Traffic counters measured on the end-points of the service. The utilization in both ends is close to 95% due to the traffic injected by the generator.

- [7] Q. Wu, S. Litkowski, L. Tomotaki, and K. Ogaki, "YANG Data Model for L3VPN Service Delivery," RFC 8299, Jan. 2018. [Online]. Available: <https://rfc-editor.org/rfc/rfc8299.txt>
- [8] D. Voyer and L. Munoz, "Internet engineering task force a. aguado internet-draft nokia intended status: Standards track o. gonzalez de dios, ed. expires: March 27, 2020 v. lopez telefonica," 2019.
- [9] B. Wen, G. Fioccola, C. Xie, and L. Jalil, "A yang data model for layer 2 virtual private network (l2vpn) service delivery," *Internet Eng. Task Force, Fremont, CA, USA, Rep. RFC*, vol. 8466, 2018.
- [10] L. Contreras, Ó. González, V. López, J. Fernández-Palacios, and J. Folgueira, "ifusion: Standards-based sdn architecture for carrier transport network," in *2019 IEEE Conference on Standards for Communications and Networking (CSCN)*. IEEE, 2019, pp. 1–7.
- [11] A. Bierman, M. Bjorklund, K. Watsen, and R. Fernando, "Restconf protocol," *IETF RFC 8040*, 2017.
- [12] R. Enns, M. Bjorklund, J. Schoenwaelder, and A. Bierman, "Network configuration protocol (netconf)," 2011.
- [13] V. Lopez, R. Vilalta, V. Uceda, A. Mayoral, R. Casellas, R. Martinez, R. Munoz, and J. P. F. Palacios, "Transport api: A solution for sdn in carriers networks," in *ECOC 2016; 42nd European Conference on Optical Communication*. VDE, 2016, pp. 1–3.
- [14] A. Mayoral, R. Vilalta, R. Muñoz, R. Casellas, R. Martínez, M. S. Moreolo, J. Fàbrega, S. Yan, A. Aguado, E. Hugues-Salas *et al.*, "First experimental demonstration of a distributed cloud and heterogeneous network orchestration with a common transport api for e2e services with qos," in *Optical Fiber Communication Conference*. Optical Society of America, 2016, pp. Th1A–2.
- [15] S. Oda, M. Miyabe, S. Yoshida, T. Katagiri, Y. Aoki, J. C. Rasmussen, M. Birk, and K. Tse, "A learning living network for open roadm networks," in *ECOC 2016; 42nd European Conference on Optical Communication*. VDE, 2016, pp. 1–3.