Design of a Network Topology Using CISCO NSO Orchestrator

Jovanovic, M., Cabarkapa, M. and Budimir, D.

Design of a Network Topology Using CISCO NSO Orchestrator

Mioljub Jovanovic
Wireless Communications Research Group
University of Westminster
London, UK.
Cisco Systems, Diegem, Belgium
m.jovanovic@my.westminster.ac.uk
mjovanov@gmail.com

Milan Cabarkapa
Department of Telecommunications
School of Electrical Engineering
University of Belgrade
Belgrade, Serbia.
cabmilan@etf.rs

Djuradj Budimir
Wireless Communications Research Group
University of Westminster
London, UK.
School of Electrical Engineeing
Univrsity of Belgrade, Serbia.
d.budimir@wmin.ac.uk
d.budimir@etf.rs

***Abstract*— This paper presents the design of a network topology using CISCO NSO orchestrator. The mismatch problem solution between a network service and its monitoring is proposed. Applying the proposed approach, the telemetry efficiency ratio parameter greater than 40 is achieved. All tests are performed in the real experimental conditions using CISCO NSO orchestrator.**

Keywords—intent based network; intent-aware monitoring agent; model-driven telemetry; service assurance

I. INTRODUCTION

NFV orchestrators (e.g., Tacker [1], Cloudify [2], ONAP [3], CISCO NSO [4]) are a crucial part for the dynamic and optimal management and orchestration of various virtualized network resources (e.g., VMs, Virtualized Network Functions). 5G technology, empowered by NFV and SDN, presents a new dimension of complexity that must be addressed by service assurance [5].

Using these orchestration software having higher level of abstraction, the rapid connectivity and provisioning could be achieved at lower prices while letting to operators possibility to build, arrange and preserve network service [6], [7].

Communication Service Provider (CSP) networks – such as Virtual Evolved Packet Core are subject to very dynamic configuration change. Provisioning, modification and termination of packet data services are being done in rapid pace in order to keep up with dynamic environment needs and cater to main business drivers, such as IoT, Video etc. SDN technologies using Network Slicing approach are foundation for such a dynamic environment, allowing automated and programmatic configuration of network services [5].

Traditionally network services are being monitored by deployment of probes which generate traffic and provide feedback on the status of the service. Due to such rapid changes in network service configuration there is open question in regard to monitoring and assuring provisioned services: What is the right approach to take in order to monitor the network which constantly changes? How to ensure network service is operational and carefully selecting probes to monitor network service? [5], [8].

Monitoring using active probes face challenges such as introduction of synthetized traffic within the data flow, end to end monitoring only with no understanding of the data path, lack of comprehension of the configuration intent etc [9]-[11]. Generated traffic using probes should resemble real traffic of the network service, however even with almost perfect synthetized traffic, there is substantial possibility that real network service traffic could be impacted, but probe does not detect such a problem since probe is not part of the actual real data flow [12]. Therefore, there is a gap in regard to monitoring and assurance of the actual network service data flow, with all network elements data traverses on the path between endpoints.

We are proposing solution based on Intent Based Networking (IBN). The proposed approach consists by:

- Extraction of configuration intent by analysing of the network service configuration.
- Discovery of the network elements along the network service data path.
- Leveraging existing network monitoring capabilities of network elements, along with probes and Model Driven Telemetry (MDT) to get more accurate information on the status of desired Network Service.

Research methodology used in understanding benefits of proposed monitoring approach involves qualitative approach, comparative analysis of existing - probe based monitoring and proposed solution based on Intent Based Networking (IBN). By using the proposed approach, we have achieved higher than 40 for the telemetry efficiency ratio parameter.

II. INTENT BASED NETWORK METHODOLOGY

Role of Intent Based Network is transforming Business Intents into configuration changes. As depicted in Fig. 1, Intent at high level represents one or set of different requirements which describe service or network.

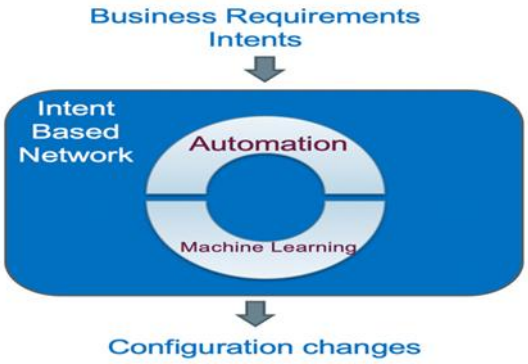

Fig. 1. Intent Based Network – high level description

Those requirements are then being analysed by set of steps, processes or algorithms in order to convert/render high-level requirements into lower form of abstraction, which could then be used to configure computer network elements in order to enable needed service. As business intent is being transformed into configuration on devices it's important to enable monitoring of the network services in order to have understanding whether desired service is operational and functioning in accordance to the business requirements – key performance indicators (KPIs). As graphically demonstrated in Fig. 2, traditionally in legacy network such monitoring would mean enabling monitoring on different data points including but not limited to: SNMP, Netflow/SFlow, telemetry and even Command Line Interface outputs (CLI). Acquiring data from different sources would certainly improve visibility on the state of the network, yet it would greatly impact efficiency and would aplify amount of telemetry data transferred over the network, but without providing clear answer on whether the intent has been fulfilled and whether network service is running and operational as per pre-defined KPIs [13].

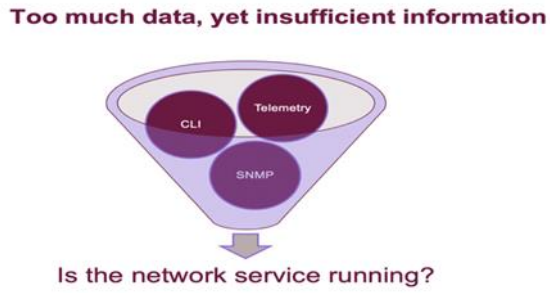

Fig. 2. Main query is - Is the Network Service running according to the pre-defined KPIs?

III. Experimental Setup

Experimental setup consists of the following routers: Simulated customer premises routers (CE), provider core routers (P) and provider edge routers (PE). Fig.3, shows the network with service models which is configured using the orchestration network architecture.

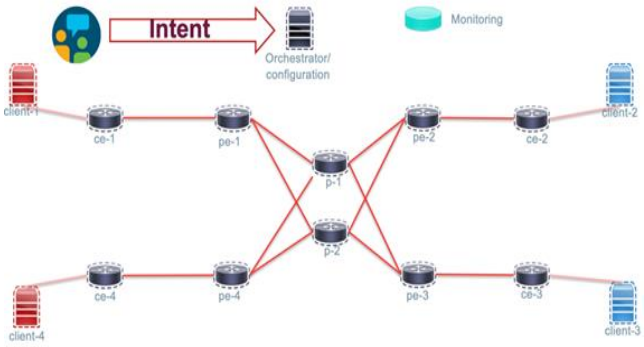

Fig. 3. Business Intent communicated to the orchestrator

In Fig. 4 orchestrator is configuring devices in order to fulfil desired service intent. Orchestrator uses Netconf protocol to access and configure network elements which are taking part in the data path to enable desired service.

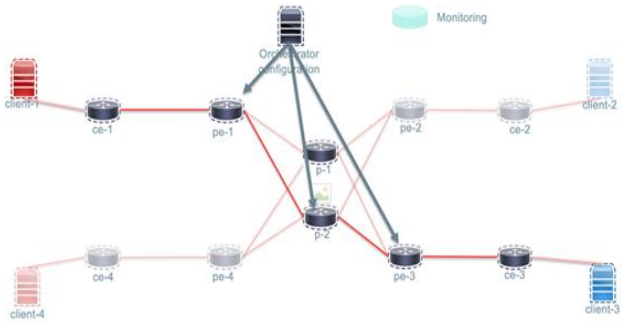

Fig. 4. Orchestrator sends configuration to network devices

In the provided example, actual intent is to establish communication – tunnel service between ce-1 and ce-3 network device in order to enable communication between Client-1 and Client-3. In order to traverse path between Client-1 and Client-3, data packets need to cross pe-1, p-2 and pe-3 as shortest path between the endpoints. Of course, this trajectory may be different in function of routing protocols and connectivity in function of time, but topology discovery and update events will be discussed in future work. At this time, we are focusing on the fixed path through the experimental network and assuming there would not be topology changes throughout the experiment shown in Fig. 5.

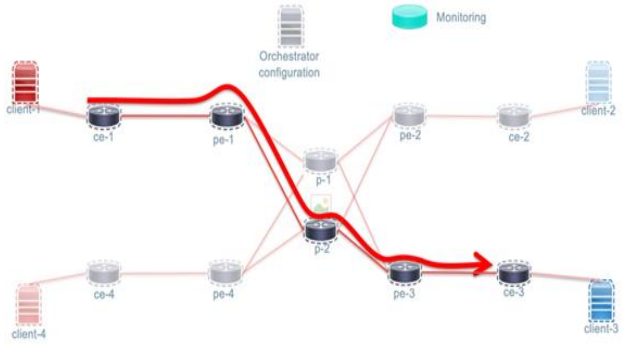

Fig. 5. Service is configured. Question: Service running within acceptable KPIs? Question: Is configuration model mapped to monitoring model?

In Fig. 6 we can observe each of the network devices streaming telemetry data to the collector, monitoring platform which is receiving and processing all telemetry data.

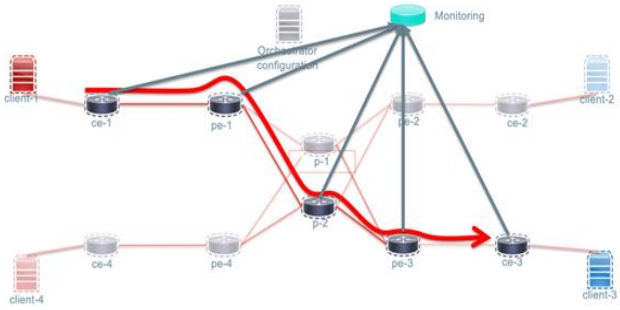

Fig. 6. Telemetry data streamed to Monitoring/Analytics platform. 250000 different stats per router (740 kbps of data)

Thanks to the fact involved network elements are already using Model Driven Telemetry processing data points by collector is simpler. However, as there are so many different data points which are being monitored on devices, there may be information overload since on average router there could easily be 250000 different monitored data points. Such as large number of collected data points could essentially mean that amount of generated telemetry data may be significantly high and could pose challenge for network infrastructure as well as could cause impact to collector processing capacity.

Instead of monitoring all relevant and non-relevant data points, causing unnecessary increase of traffic and compute resources to process large amount of data, we're proposing significant reduction in amount of telemetry data by ensuring that only minimal set of relevant data points is exported from the network devices by means of intent-aware monitoring agent (IAMA). Data reduction task is accomplished by deploying IAMA locally to the network devices, thus leveraging local area network (LAN) links and avoiding use of wide-are links (WAN) for large amount of data points. IAMA is aware of the service details and is also capable of receiving telemetry data. As represented on IAMA architecture in Fig. 7, service intent is received by from the orchestrator while MDT is received from network devices.

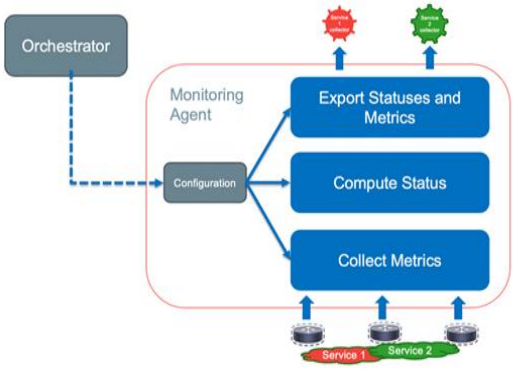

Fig. 7. Intent-aware monitoring agent architecture

IAMA is performing analysis on the received datasets and series of computations in order to determine actual state of the service. Steps performed by IAMA: collecting MDT, processing and exporting reduced – yet more relevant MDT is called IAMA pipeline. Final result of IAMA pipeline is significantly reduced amount of MDT containing only high-level status of the monitored service, as per pre-defined Key-Performance Indicators (KPIs).

IV. Results

Measuring objective was to determine how much data is actually received via MDT under usual telemetry export, with typical data points for router such as environmental, interface stats etc. Result of this work outlines amount of measured data after performing analysis of the incoming telemetry and mapping to service aware MDT. All routers and all incoming data points were taken into account.

TABLE I. Experimental Results

	Intent-Aware Monitoring Efficiency			
	Total MB	**Rate 1 min in kbps**	**Rate 5 min in kbps**	**Rate 15 min in kbps**
Incoming from routers	5200	740.7	700.1	711.7
This work	130.8	17.3	17.2	17.1
Outgoing to Analytics platform	224.9	29.5	29.1	29.3
This work efficiency ratio	40.9	42.8	40.6	41.7

As outlined in Table I, demonstrated experimental results have reduced the amount of incoming MDT from routers from 5.2 GB to 130 MB, while preserving relevant information which is – is service running and operational per pre-defined KPIs.

V. Conclusion

The design of a network topology using CISCO NSO orchestrator has been presented in this paper. The solution about mismatch problem between a network service and its monitoring has been proposed. The telemetry efficiency ratio parameter of more than 40 has been achieved. The amount of telemetry data has been reduced by injecting service aware information in MDT and removing all overhead MDT data points which do not need to be exposed to the network operator who is monitoring the service. Of course, full MDT can also be enabled if desired.

References

[1] https://docs.openstack.org/tacker/latest/

[2] https://cloudify.co/

[3] https://www.onap.org/

[4] https://www.cisco.com/c/en/us/solutions/service-provider/solutions-cloud-providers/network-services-orchestrator-solutions.html

[5] Anil Rao, "Reimagining service assurance for NFV, SDN and 5G", White paper, Analysis Mason, 2018.

[6] R. Mijumbi, J. Serrat, J. l. Gorricho, S. Latre, M. Charalambides, and D. Lopez, "Management and Orchestration Challenges in Network Functions Virtualization," IEEE Communications Magazine,vol. 54, no. 1, pp. 98–105, Jan 2016.

[7] A. J. Gonzalez, G. Nencioni, A. Kamisiski, B. E. Helvik, and P. E. Heegaard, "Dependability of the NFV Orchestrator: State of the Art and Research Challenges," IEEE Communications Surveys Tutorials, pp. 1–23, 2018.

[8] M. Pattaranantakul, R. He, Z. Zhang, A. Meddahi and P. Wang, "Leveraging Network Functions Virtualization Orchestrators to Achieve Software-Defined Access Control in the Clouds," in IEEE

Transactions on Dependable and Secure Computing, pp. 1-14, Nov. 2018.

[9] A. D'Alconzo, I. Drago, A. Morichetta, M. Mellia and P. Casas, "A Survey on Big Data for Network Traffic Monitoring and Analysis," in IEEE Transactions on Network and Service Management, vol. 16, no. 3, pp. 800-813, Sept. 2019.

[10] R. Boutaba, M. A. Salahuddin, N. Limam, S. Ayoubi, N. Shahriar, F. Estrada-Solano, and O. M. Caicedo. A Comprehensive Survey on Machine Learning for Networking: Evolution, Applications and Research Opportunities. J. Internet Serv. Appl., 9(16), 2018.

[11] Cisco Systems, Inc, "GitHub Network Telemetry Pipeline," Cisco Systems, Inc, 2017. [Online]. Available: https://github.com/cisco/bigmuddy-network-telemetry-pipeline

[12] M. Jovanović, M. Čabarkapa, B. Clause, N. Nešković, M. Prokin, B. Đurađ, Model driven telemetry using Yang for next generation network applications, 5th International Conference on Electrical, Electronic and Computing Engineering (IcETRAN) 2018, pp. 1186 - 1189, Palić, Serbia, June, 2018.

[13] B. Claise, J. Clarke, and J. Lindblad "Network Programmability with YANG: The Structure of Network Automation with YANG, NETCONF, RESTCONF, and gNMI", Addison-Wesley Book, 1st edition, 2019.