An Integrated Network Monitoring System for SDN VPN

Yueh-Hsien Lin
Telecommunication Laboratories
Chunghwa Telecom Co., Ltd
Taoyuan, Taiwan, ROC
yhlin@cht.com.tw

Chien-Wen Yang
Telecommunication Laboratories
Chunghwa Telecom Co., Ltd
Taoyuan, Taiwan, ROC
chienwen@cht.com.tw

Ting-Che Chuang
Telecommunication Laboratories
Chunghwa Telecom Co., Ltd
Taoyuan, Taiwan, ROC
chiachun@cht.com.tw

Min Liu
Telecommunication Laboratories
Chunghwa Telecom Co., Ltd
Taoyuan, Taiwan, ROC
sambora@cht.com.tw

Min-Chia Chang
Telecommunication Laboratories
Chunghwa Telecom Co., Ltd
Taoyuan, Taiwan, ROC
ken213@cht.com.tw

***Abstract*—This paper provides an integrated monitoring and analysis method for SDN-VPN. This method establishes a consistent process to monitor the status of SDN-VPN network elements (NE), and integrates the alarm and health information of NE for alarm correlation and service impact analysis. The maintenance personnel can monitor the status of all NEs with a single panel. The proposed consistent process consists of multiple parts, including the mechanism of collecting NE alarms and resource status from Resource Orchestrator (RO), alarm correlation analysis, and service impact analysis. With the process, we can learn the cause of the fault events in SDN-VPN, the nature of the fault, and the scope of service impact, thus accelerating trouble shooting and improving service quality.**

Keywords—Software Defined Network, Virtual Private Network, Network Monitoring, Fault Management.

I. Introduction

Software Defined Networking (SDN) significantly reduces the difficulty of network maintenance and management. Network administrators can replace traditional low-level (hardware) methods to adjust networks with high-level (software) ways [1][2]. SDN has many features, for it is directly programmable, agile, centrally managed, programmatically configured, open standards-based and vendor-neutral [3]. It has become the first choice for enterprises to reduce cost and improve speed of provisioning network and cloud resources. The most important reason why SDN has widespread adoption is that the application needs of emerging technology like Cloud Computing and Big Data have driven the revolution of network[4][5], and the virtualization technology of physical servers triggers explosive growth. These emerging business applications are no longer be limited to be deployed on a single physical server Instead, they can be deployed across multiple servers which can be virtual machines.

Virtual Private Network (VPN) provides a variety of information security services for enterprises by using tunneling and encryption technologies [6]. VPN has the advantages of secure remote data access, quality of service (QoS) guarantee and easy management. The demand for enterprises and telecom operators to VPN has increased, prompting manufacturers to invest related products and service applications [7].

We introduce the SDN architecture on the VPN service to provide a centralized and easily-managed SDN intelligent network to attract customers in need of self-built Private Network. We provide centralized and integrated management of Service Portals for various services, including ordering, startup, setting, and monitoring to achieve rapid service delivery from front-end order receiving to back-end automated provisioning. [8]

II. METHODOLOGY

The following sections describe collecting of NE alarms and resource information through Resource Orchestrator (RO), alarm correlation analysis, service impact analysis, resource information analysis, and a single comprehensive information display panel.

2.1 Collecting network equipment alarm and equipment resource information

An RO is built in this system to monitor the status of SDN equipment, status and traffic of SDN links and virtual links, monitor resource pool and individual virtual network functions (VNF) status, and also provide configuration management (CM) and performance management (PM) functions of SDN, virtual links and VNF.

The RO manages and monitor SDN elements, VNF elements, SDN services and traditional network equipment, and the RO generates Link Down or other events when a SDN link route is changed, a SDN Link is abnormal, a VNF is abnormal or QoS is abnormal. Event information is sent to the integrated monitoring system through the enterprise application integration (EAI) Bus.

This system establishes a Service Orchestrator (SO) to record the configuration information of the physical device and VNF, and generate SDN VPN configuration information regularly.

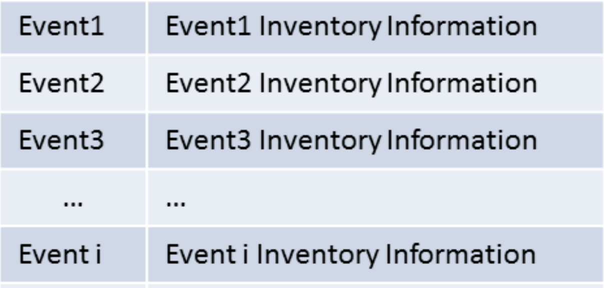
2.2 Alarm correlation analysis

Alarm correlation analysis plays an important role in trouble shooting. The current open events are collected as a set of events through the RO (Fig.1).

Event Sets
{Event1, Event2, Event3,...,Event i}

Fig. 1. Events Sets

This event collection is linked to the device after analysis with inventory information from SO (Fig. 2).



Event1	Event1 Inventory Information
Event2	Event2 Inventory Information
Event3	Event3 Inventory Information
...	...
Event i	Event i Inventory Information

Fig. 2. Event Collection

Based on operational requirements, a number of correlation analysis rules are defined. Each rule has a set of conditions, and each condition is basically defined with the equipment, type, location…, etc. of the alarm origin. Each rule is given an identification code and a readable name (Figure 3).

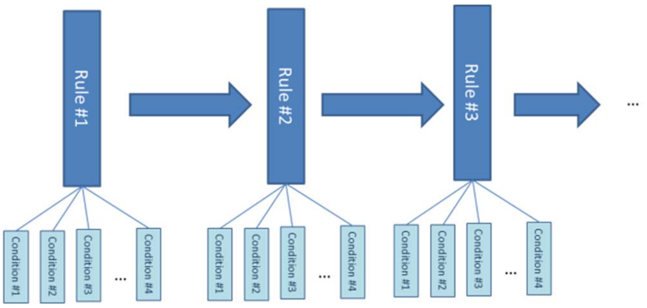


Fig. 3. Correlation Analysis Rules

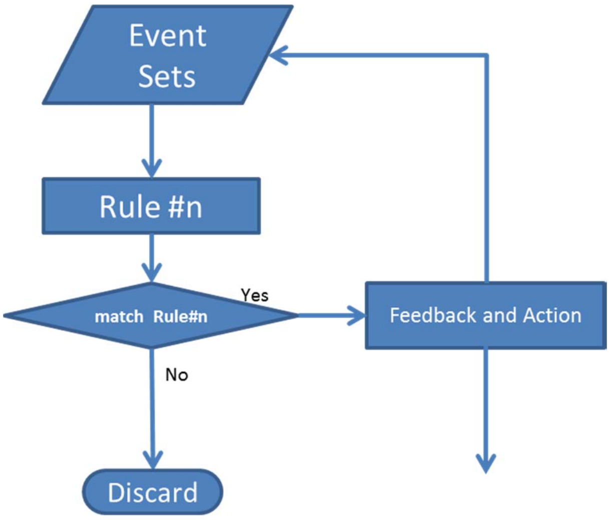


Fig. 4. Alarm correlation analysis Flowchart

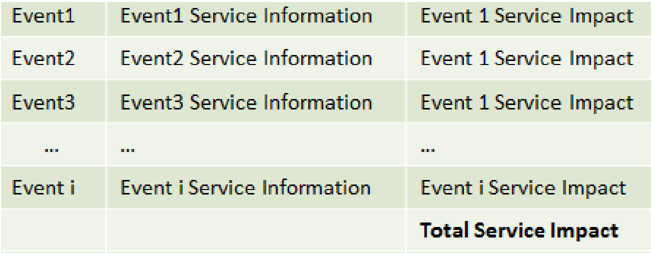
The event sets will be compared with each rule. If all the conditions of a rule are met, the system will generate an event, and the event description field is filled with the rule name. The start time of the event is the time when the event set starts to meet the condition, and the end time is the time when the event set ceases to meet any of the conditions. The events generated here are also appended to the event set (Fig. 4).

2.3 Service Impact Analysis

The service impact analysis allows the maintenance personnel to grasp the scope and status of the current alarms, and assist them in determining the fault handling strategy. The system records the service information in the SO, such as the bandwidth, the number of circuits, the number of serviced users, and the user's service priority according to the Service Level Agreement (SLA). The system uses this information to analyze the current alarms to generate service impact value.

First, the system collects current events from RO and form a set of events. The target of each event in this set is analyzed with the SO information to get the service information and link with the events in the set.

Each event gets one service impact value. The total service impact value of current event set is sum of service impact values of each event removing duplicated calculation (Fig. 5).



Event1	Event1 Service Information	Event 1 Service Impact
Event2	Event2 Service Information	Event 1 Service Impact
Event3	Event3 Service Information	Event 1 Service Impact
...	...	...
Event i	Event i Service Information	Event i Service Impact
		Total Service Impact

Fig. 5. Service Impact Value Calculation

The rules are defined according to maintenance requirements. Each rule has one or more conditions. The condition is composed of threshold value of the bandwidth, the number of users, and the priority of the users. Each rule is given an identification code and a readable name. The service information in the event sets is analyzed with each rule. When all the conditions of a rule are met, an event is generated, the the rule name is used as the description of the event. The start time of the event is the time when the event set starts to meet the condition, and the end time is the time when the event set ceases to meet any of the conditions. The events generated here are appended to the event set.

2.4 Resource Information Analysis

The RO obtains the status and traffic of SDN links, and monitors VNF by connecting to NAPA. RO issues an event when fault occurs. RO also monitors the status of the VPN links and generates an event when the VPN link is down. At the same time, the cloud service network management system also obtains the traffic and status of the virtual links and the resource pool status of Data Centers.

The system collects the above information and combines it with the SO information to become various equipment and service indicators (Fig. 6). These indicators can be directly presented on the monitoring panel. With threshold value setting, an event is generated when the indicator meets the threshold value. The event will be accompanied by a fault impact information feedback to the event set of 2.2, or the service impact information is fed back into the 2.3 event set.

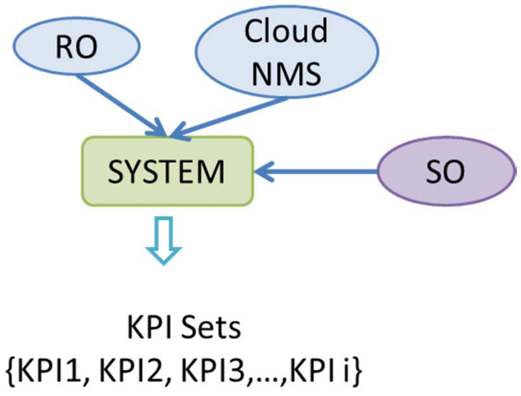


Fig. 6. Resource Information Analysis

2.5 Single panel display

In the aspect of comprehensive monitoring, it is necessary to integrate network obstacles information, resource status, correlation analysis, service impact analysis, and resource information analysis indicators. The integrated results are presented in the form of network topology, graphs or charts.

In addition to the presentation of the results, it is necessary to notify the network management center of the events. The notification can be done manually and automatically. Manual notification means that the on-duty personnel can notify the operator and the supervisor manually of the possible events diagnosed through the panel or an incident that has already occurred. Automatic notification is triggered when the system determines possible events through pre-set rules and the system automatically reports via SMS message or email to personnel of network management center and the system displays them with the warning symbol and alarms on the panel. When the network management center receives the event alarm, the responsible person is immediately assigned to handle the process, and the process needs to be recorded in the system. The responsible supervisor can also learn the current progress from the system.The template is used to format your paper and style the text. All margins, column widths, line spaces, and text fonts are prescribed; please do not alter them. You may note peculiarities. For example, the head margin in this template measures proportionately more than is customary. This measurement and others are deliberate, using specifications that anticipate your paper as one part of the entire proceedings, and not as an independent document. Please do not revise any of the current designations.

III. Implementation

We built a network as shown in Fig. 7. An enterprise has several offices in different locations. Offices and data center are connected by VPN. The network inside each office is a Software Defined Local Area Network (SD-LAN). We create a telecom cloud, which provides SDN VPN services to the enterprise to connect offices and the Data Center.

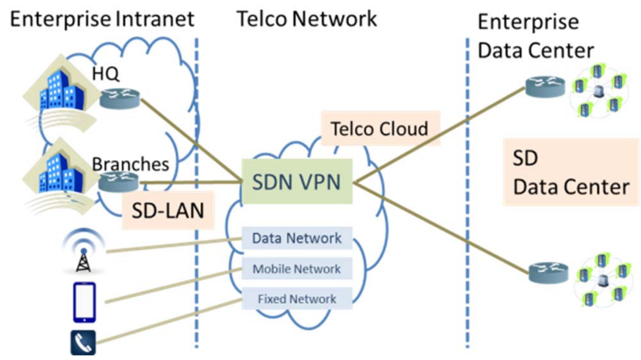


Fig. 7. Network Archetecture

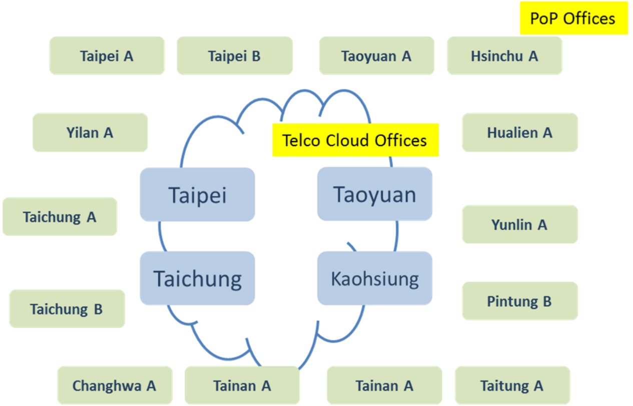


Fig. 8. Network Topology

Fig. 8 shows the current SDN VPN network nodes which are OpenFlow based. The core network is connected by the telecom cloud offices. Each telecom cloud office is connected to a Point-of-Presence (PoP) office as a VPN access point. All telecom cloud office and PoP offices are equipped with both OpenFlow Switchs (OFS) and OpenFlow Firewalls (OFw).

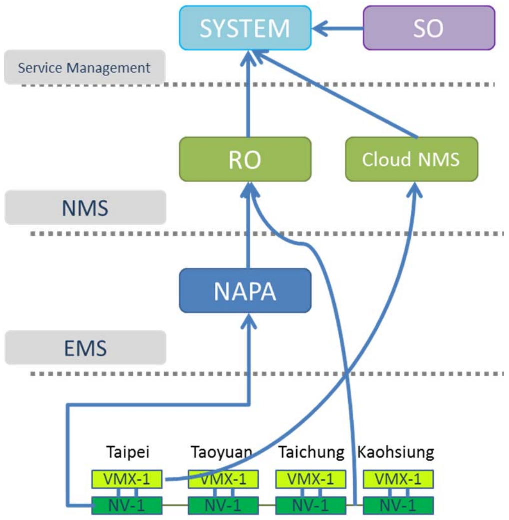


Fig. 9. Information Flow

Fig. 9 shows the information flow. RO receives SDN information through NAPA, and also collects physical NE information. Cloud NMS receives cloud service information. SO collects SDN, physical network elements, cloud services, VPN and other information. The system brings together RO, Cloud NMS, and SO information for analysis and processing.

The system uses EAI Bus to collect data (Fig. 10). The collected data is placed in the Data Pool. The Data Analyzer obtains the data from the Data Pool and performs alarm correlation analysis, service impact analysis and resource information analysis. The analysis results are displayed on the panel, and the results are also fed back to the Data Pool

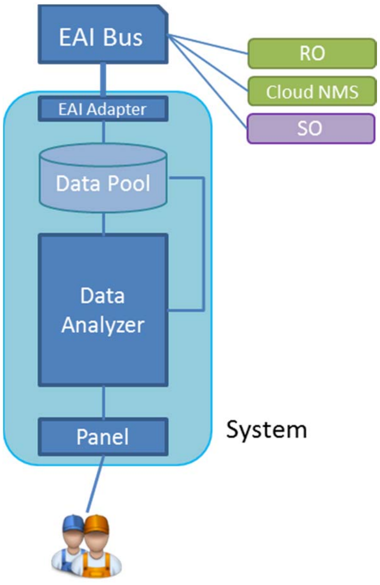


Fig. 10.

The Panel of this system is web-based and has appropriate account/password access control. The Panel is divided into two parts. The first part is the SDN VPN backbone monitoring topology (Fig. 11). This monitor panel displays the status of offices and links in a topology diagram and displays different colors according to the alarm level.

When the maintenance personnel click the office or link with alarms, the panel brings out the list of alarms and their details

The second part is the resource status of the equipment offices. If it is a PoP office, the SDN and actual network resources of the office are displayed. If it is a cloud office, the resource status of this cloud office is displayed.

At the same time, when an alarm meets the conditions, the system actively sends out emails and SMS (short message service) messages to related personne, so that the maintenance personnel can handle the alarm immediately.

IV. CONCLUSION

In this paper, we present a system for the following analysis.

(1) Alarm correlation analysis: Maintenance personnel can speed up the trouble-shooting of alarms.

(2) Service impact analysis: Grasp the situation of affected services and help formulate the strategy to fix the network problems.

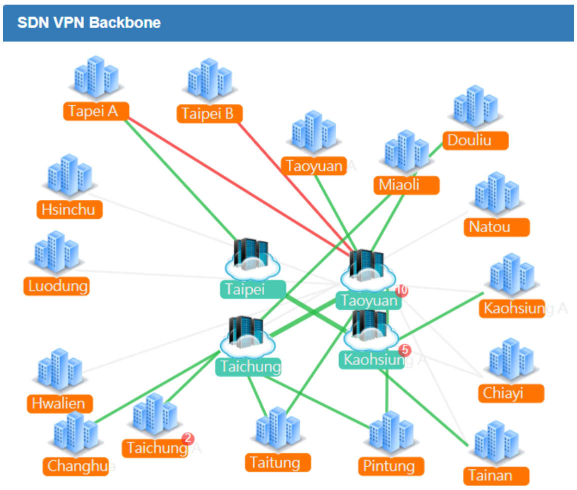


Fig. 11.

(3) Resource information analysis: Looking at the health status of each telecom office and equipment.

This research provides an integrated monitoring and analysis method for SDN VPN networks, a centralized monitoring mechanism for telecom operators to establish new services quickly, grasp the status of the entire network equipment, and centrally manage the SDN VPN network architecture through a consistent process. The SDN flexibility allows this method to be applied to networks composed of heterogeneous digital services, such as IPTV services, Wi-Fi services, NGN services, etc., ensuring that the digital services of various providers can be monitored with the system.

REFERENCES

[1] Marc Mendonca, Bruno Astuto A. Nunes, Xuan-Nam Nguyen, Katia Obraczka, and Thierry Turletti, "A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks," on IEEE Communications Surveys & Tutorials, Volume: 16 , Issue: 3.

[2] Sakir Sezer, Barbara Fraser, David Lake, Jim Finnegan, Niel viljoen, Marc Miller, and Navneet Rao, " Are We Ready for SDN? Implementation Challenges for Software-Defined Networks," on IEEE Communications Magazine, Volume 51, Issue: 7.

[3] “Software-Defined Networking (SDN) Definition”, https://www.opennetworking.org/sdn-definition/ accessed: 20 May 2019.

[4] Rajat Chaudhary, Gagangeet Singh Aujla, Neeraj Kumar, Joel J.P.C. Rodrigues, “Optimized Big Data Management across Multi-Cloud Data Centers: Software-Defined-Network-Based Analysis,” on IEEE Communications Magazine , Volume: 56 Issue: 2.

[5] Diego Kreutz, M. V. Ramos, Paulo Verissimo, Christian Esteve Rothenberg,Siamak Azodolmolky, Steve Uhlig, "Software-Defined Networking: A Comprehensive Survey", Proc. IEEE, vol. 103, no. 1.

[6] R. Venkateswaran, "Virtual private networks," IEEE Potentials Volume: 20 , Issue: 1.

[7] Anjum Zameer Bhat, Dalal Khalfan Al Shuaibi, Ajay Vikram Singh, "Virtual private network as a service — A need for discrete cloud architecture," 2016 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)

[8] Domenico Siracusa, Federico Pederzolli, Matteo Gerola, Andrea Zanardi, Domenico La Fauci, Gabriele M. Galimberti "Demonstration of a Hybrid SDN/GMPLS Control Plane for Optical Virtual Private Networks with Restoration Capabilities," ECOC 2016; 42nd European Conference on Optical Communication