Controller Architecture and Performance Optimization for Intensive Deployment Scenarios

Chuanming Zhu, Huiguang Chen, and Jingwen Li(✉)

China Telecom Research Institute, Beijing, China
lijw21@chinatelecom.cn

Abstract. As the scale and complexity of the network increase, SDN controller in the intensive deployment scenario has problems in architecture and performance. Combined with the controller collection and control framework, the acquisition and control separation mode is designed by isolating the underlying protocols, and data collection and configuration delivery operations are performed on NE devices to improve the controller collection and control performance. Ensure that service delivery does not affect operation and maintenance; The controller acquisition and control architecture is optimized to ensure a balanced distribution of tasks within the framework and improve controller performance. Through key capability research and development, framework optimization and performance improvement, SDN controller technology is gradually mature, enabling intelligent operation of cloud network.

Keywords: Intensive deployment · SDN controller · SDN/NFV · Architecture optimization

1 Current Status and Problems of IP SDN Controller's Acquisition and Control Ability

IP SDN controller for IP network, based on the new network technology, through the NETCONF, SNMP, Telemetry, NETFLOW protocol intelligent collection control. By isolating the underlying protocols, the acquisition and control separation mode is designed to perform data collection and configuration delivery operations on NE devices, improving controller collection and control performance and ensuring that service delivery and operation, and maintenance do not affect each other. The controller acquisition and control architecture is optimized to ensure a balanced distribution of tasks within the framework and improve controller performance. Further optimize the acquisition and control capabilities to improve the overall controller performance, reliability, and stability to better cope with future intensive deployment scenarios.

SDN controller is the core capability of the new generation of cloud network operating systems. By optimizing the architecture and performance of the SDN controller and focusing on customers, the value of the controller is fully enhanced, and the operation

Y. Zhang et al. (Eds.): CENet 2023, LNEE 1125, pp. 170–175, 2024.
https://doi.org/10.1007/978-981-99-9239-3_17

management capability for cross-domain, cross-vendor, and cross-professional services and networks is built, which is also the active exploration and practice of operators in the process of cloud network integration.

Although the NETCONF service layer of the IP SDN controller has the global connection pool capability, the underlying real connection does not distinguish between device configuration and NE data collection. In the intensive deployment scenario, the number of network elements is at least one order of magnitude higher than that in the privatized deployment. Frequent NE data collection blocks the delivery of normal service configurations and causes the upstream interconnection system to time out. Normal services are affected.

Currently, the controller collection module mainly includes NETCONF active pull collection, SNMP, Telemetry, and NETFLOW passive push collection. NETCONF collection is coarse and usually collected by NE function module. As a result, the CPU usage of routers in the collection period is too high, affecting the network processing capability of routers. Currently, only TeleDB is supported for collecting data stores. In intensive deployment scenarios, write bottlenecks may occur.

2 IP SDN Controller Key Technologies

2.1 SNMP Protocol

Simple Network Management Protocol (SNMP) is a standard network management protocol widely used on TCP/IP networks. SNMP provides a way to manage network elements (such as routers) from a central computer (i.e., a network management workstation) running network management software.

SNMP has the following operation modes:

(1) The management workstation obtains network resource information through the GET, get-next, and GET-bulk operations.
(2) The management workstation uses SET to set network resources.
(3) The management agent reports traps and informs the management workstation so that the workstation can obtain the network status in a timely manner and the network administrator can take measures in a timely manner.

2.2 NETCONF Protocol

Network Configuration Protocol (NETCONF) is a network configuration and management protocol based on the Extensible Markup Language (XML). Communication between client and server is implemented using a simple RPC-based (Remote Procedure Call) mechanism.

NETCONF provides a way to remotely manage and monitor devices from a central computer (i.e., a network management workstation) running network management software. As the scale and complexity of networks increase, the traditional Simple Network Management Protocol (SNMP) cannot meet the requirements of complex network management, especially configuration management. In order to make up for the defects of SNMP, the NETCONF protocol came into being.

2.3 Telemetry Protocol

Telemetry is a network device monitoring technology that provides the ability to periodically sample statistics and status data within network devices. The traditional acquisition mechanism has some problems, such as poor real-time performance, low performance, no model definition, poor scalability, etc., which cannot meet the requirements of big data. Telemetry has the following advantages over traditional mechanisms:

By using pull mode to obtain device monitoring data, a large number of network nodes cannot be monitored, which limits network growth.

The sampling period accuracy of monitoring data is minute level. You can only increase the query frequency to improve the accuracy of data acquisition. However, this will cause high CPU utilization of network nodes and affect the normal functions of the device.

Because of the existence of network transmission delay, the monitored network node data is not accurate.

Therefore, in the face of large-scale and high-performance network monitoring requirements, users need a new network monitoring method. Telemetry technology can meet user requirements, support intelligent operation and maintenance systems to manage more devices, monitor data with higher accuracy and more real-time, and the monitoring process has less impact on device functions and performance. It provides the most important big data foundation for rapid network problem location and network quality optimization and converts network quality analysis into big data analysis. Strong support for intelligent operation and maintenance needs.

2.4 NETFLOW Protocol

NETFLOW technology is a statistical technology based on network traffic information. It can classify the communication traffic and resource usage in the network, and monitor and manage the network based on various services and resources. Because of the limitations of traditional traffic statistics, new technology is needed to better support the development of network services. NETFLOW technology comes into being. Data output through NETFLOW technology can be used for many purposes, network management and planning, business accounting and sub-department billing, ISP billing, data storage, and commercial data collection.

3 IP SDN Controller Optimization Scheme

It is planned to add a general tagging capability to virtual connections at the NETCONF service layer. Virtual connections and real connections use tag matching to optimize the device collection and device configuration connection allocation algorithms under the constraint of the global device connection number. In this way, live network service configurations are not affected when device collection operations peak. The maximum response time of service configuration can be increased from minutes to seconds when the peak value of the collection is expected (Fig. 1).

It is planned to separate configuration collection from performance status data collection. The former uses NETCONF and the latter uses lightweight Telemetry/NETFLOW to reduce the peak CPU usage from 90 to 70% in the collection period (Fig. 2).

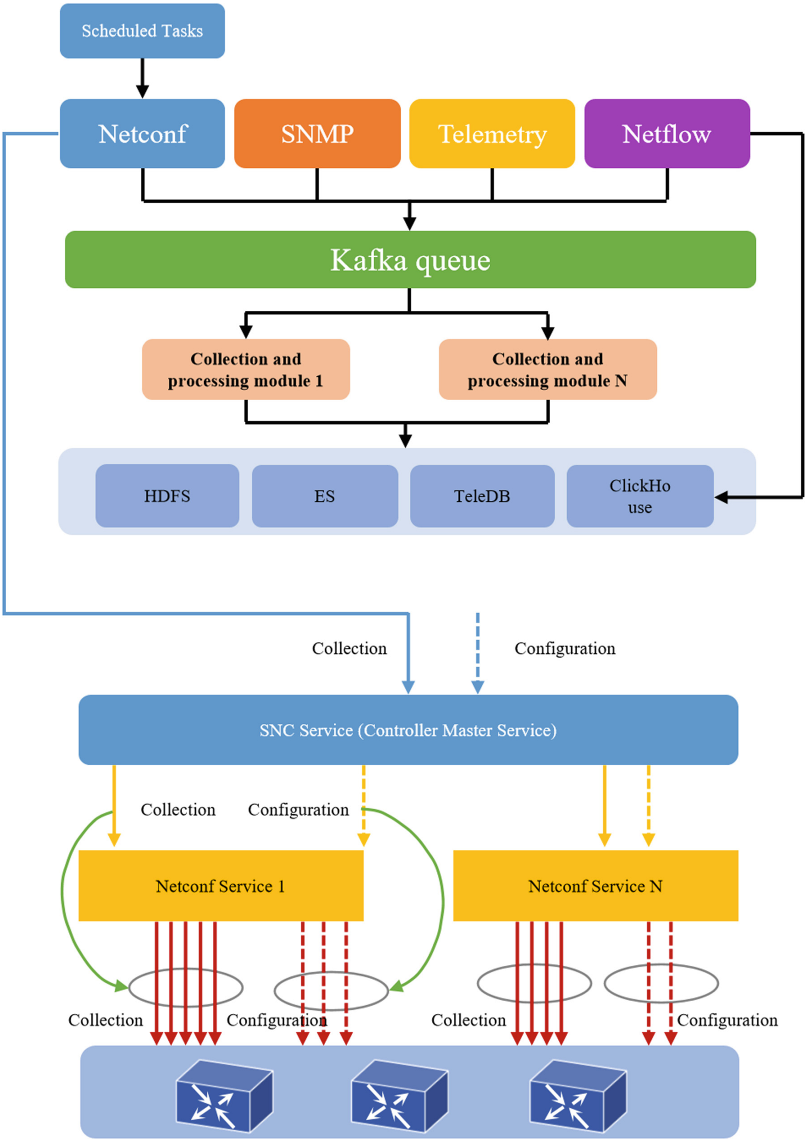

Fig. 1. The separation scheme of configuration collection and performance status data collection is implemented to reduce CPU utilization

4 IP SDN Controller Application

4.1 Configuration Data Delivery

Delivering NETCONF configuration data. NETCONF defines messages in XML format and uses the RPC mechanism to modify configuration information. In this way, the configuration information can be easily managed and interoperability between devices

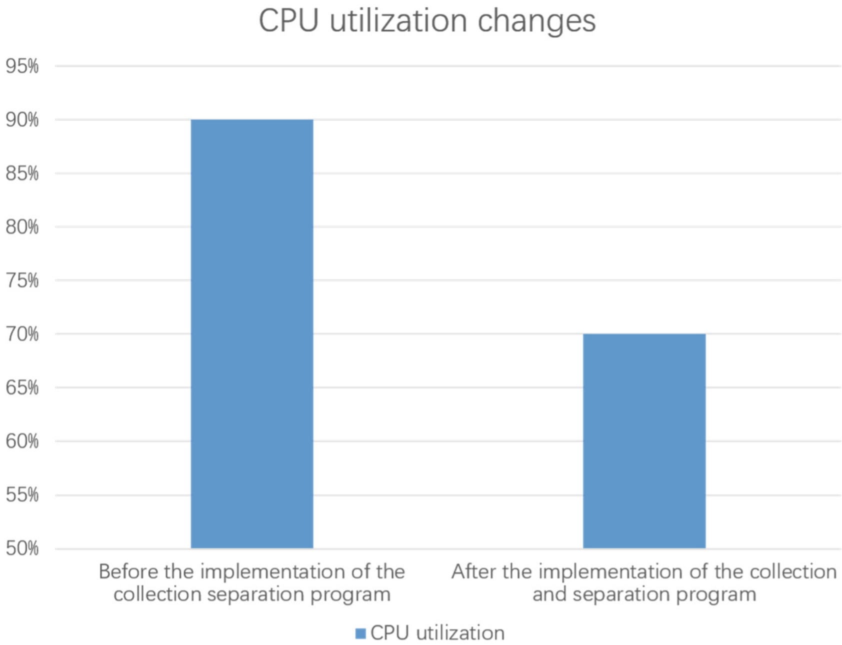

Fig. 2. Changes in CPU utilization before and after the separation of configuration collection and performance status data collection

from different manufacturers can be achieved. SDN control solves problems such as closed standards of heterogeneous vendors, difficult unification, and high operational complexity. NETCONF improves configuration efficiency and reduces network faults caused by manual configuration errors. NETCONF also provides security mechanisms such as authentication and authentication, ensuring the security of message transmission. The controller instantiates the network function model defined by YANG through the NETCONF protocol and obtains the corresponding data from the device or sends the corresponding data to the device for configuration. This module is based on the self-developed FAST YANG tool to complete YANG model compilation/code generation, model instantiation and verification, and interaction with device NETCONF protocol (including model and XML serialization/deserialization).

4.2 Performance Status Data Collection

Telemetry Collects performance data. Telemetry subscription means that the device as the client and the collector as the server connect to the collector for data collection and upload. After you configure the collection requirements, use the NE management micro-service to deliver static configurations of TWAMP and IFIT sampling tasks to devices through NETCONF, for example, to start the sampling tasks. The Telemetry micro-service subscribes to the device and sends the sampled data to the Telemetry micro-service process. The Telemetry micro-service pushes the received data to the corresponding Kafka Topic, enabling the data processing module that subscribes to the Topic to receive Kafka messages. The data processing module calculates the link performance information such as delay, jitter, and packet loss rate based on the logical topology processed by IFIT, TWAMP, and other modules, and pushes messages to Kafka for other modules to use.

Monitoring and managing NETFLOW traffic. NETFLOW monitors and manages networks based on services and resources by collecting statistics on traffic and resource usage. You can configure a specified mode to sample service packets, create a NETFLOW flow based on the quintuple information, age the NETFLOW flow based on the specified mode, and output the NETFLOW flow based on the specified mode and packet version. The NETFLOW micro-service module pushes the received data to the corresponding Kafka topic so that the data processing module subscribed to the Topic receives the Kafka message. The data processing module parses information such as traffic and resource usage based on sampling and pushes messages to Kafka for other modules to use.

5 Conclusion

This paper proposes a framework based on the separation of acquisition and control of SDN controllers. By scheduling the acquisition module and configuration module, the acquisition module and control module schedule different protocols respectively to avoid the interaction between data acquisition and configuration delivery, and adopt multi-instance deployment mode to improve the overall performance of the controller. It provides a new way to improve the performance of SDN controllers for intensive deployment.

In the future, with the intensive deployment and application of SDN controllers, and the gradual optimization and improvement of architecture and performance, SDN controllers will be deployed more quickly and widely to meet complex and diverse service requirements and improve the level of network control.

References

1. Lv, H., Li, Q., Shen, G.: Belt network telemetry method review. J. Software 1–21 (2023)
2. Abdelaziz, A., Fong, A., Gani, A., Garba, U., Khan, S., Akhunzada, A.: Distributed controller clustering in software defined networks. PLoS ONE **12**(4), e0174715 (2017). https://doi.org/10.1371/journal.pone.0174715
3. Li, Z., Hu, H., Hu, H., Huang, B., Ge, J., Chang, V.: Security and energy-aware collaborative task offloading in D2D communication. Future Gen. Comput. Syst. **118**, 358–373 (2021)
4. Cui, Y., Hui, Zhang, H., Xu, H.: Network traffic statistics based on NetFlow technology. Telecommun. Sci. **6**, 62–64 (2003)
5. Xin, Z.: Design of a NetFlow flow analyzer. Mod. Electron. Technol. **21**, 80–83 (2006)
6. L.: Netflow technology principle and application. J. Railway Commun. Sign. **1**, 33–35 (2005)
7. Wang, Y., Ju, W., Cheng, Q.: Optimization of flow classification technology for large-scale high-speed network traffic analysis. Commun. Inf. Technol. **253**(05), 59–62 (2021)
8. Bjorklund, M.: RFC 6060: YANG—A data modeling language for the network configuration prorocol (NETCONF). RFC Editor, USA (2010)
9. Li, Z., Hu, H., Hu, H., Huang, B., Ge, Chang, V.: Security and energy-aware collaborative task offloading in D2D communication. Future Gen. Comput. Syst. **118**, 358–373 (2021)