Advances in Computer, Signals and Systems (2024)
Clausius Scientific Press, Canada

DOI: 10.23977/acss.2024.080512
ISSN 2371-8838 Vol. 8 Num. 5

Construction of Traffic Collection Network for Banking Data Centers

Ma Cheng, Lv Jiezhi

Postal Savings Bank of China, Beijing, China

Keywords: Traffic Collection, Traffic Analysis, Intelligent, Corre, Session Tracing

Abstract: In recent years, with the development of banking business and diversification of demands, especially the explosive growth of Internet business, banks have put forward higher requirements for the agile expansion capability of banking information systems. Banks are building a new generation of data centers based on the thinking of cloud architecture. The bank data center is undergoing a transformation from traditional network architecture to a new network architecture that supports multi-business and multi-point active data centers. In this process, network operation and maintenance capabilities are also being built, transformed and upgraded synchronously. Increasing the construction of network traffic collection and visual analysis technology applications to view the network performance, link status and business system operation of various types of devices in the data center in real time has become an important means of network operation and maintenance.

1. Introduction

The rapid development of business and the continuous improvement of operation and maintenance refinement have put forward higher requirements for monitoring indicators. In order to meet the daily operation and maintenance requirements, we use the bypass data packet real-time acquisition method to continuously improve the level of operation and maintenance monitoring. The construction of data packet collection network is an important means for us to solve the problem of insufficient monitoring accuracy and improve the level of operation and maintenance.

2. Industry trends

As network technology continues to evolve, new network architectures and services have placed higher demands on network operations and maintenance. Visualized operations and maintenance have become an inevitable trend for the future. Traditional network management software primarily utilizes the SNMP protocol to monitor the operational status of hosts and network devices in real-time. Users can only view monitoring statistics and are unable to see the content of network traffic or discern whether the transmitted traffic is business-critical that needs to be guaranteed or junk traffic that should be discarded. Traditional network security systems also implement access control or intrusion behavior monitoring at key network points but are incapable of retrospectively analyzing attack behaviors through packet data. Most traditional business analysis software operates by installing client software on business hosts to communicate with business applications at the host level, monitoring the operational status of business application processes. This method can impact the operation of business software. Moreover, as almost all current business operations require data transmission over networks, traditional business analysis software cannot monitor transmissions at the network level. By capturing network traffic via a bypass and sending it to monitoring and analysis equipment for real-time parsing, it is possible to achieve real-time network performance monitoring, security status monitoring, and business performance monitoring. Network traffic bypass capture obtains raw network packet data passively (through splitting or switch mirroring) without needing to install new clients in users' business and network environments, minimally affecting user networks and operations while capturing real-time network traffic. Hence, the method of obtaining packet data through network bypass traffic capture has gained widespread recognition among financial users. Currently, users have extremely high requirements for operational management, and data centers are equipped with a large number of visualization monitoring systems. Initially, these monitoring systems would use probes, collection engines, switch mirroring, etc., to collect traffic from production. As the scale of monitoring systems expands and the number of traffic collection points increases, to meet the needs of multiple systems sharing traffic and different systems classifying and filtering traffic, reducing the complexity at the traffic collection layer, financial institutions have unified their traffic collection layers by constructing a unified traffic collection network. The traffic collection network, serving as the foundation for visualized operations and maintenance, performs uniform collection of raw data and, according to the needs of different tool systems, can deduplicate, slice, add or remove packet header marks, etc., offloading the common packet sorting work of tool systems to the traffic collection network for unified implementation, enhancing the analytical efficiency of tool systems. A unified traffic collection network makes it possible for financial institutions to visualize their entire network, collecting and aggregating the main traffic data from the production network, supporting the deployment and operation of various types of analysis tools. Any tool system can obtain data from the production network through the traffic collection network without needing to modify or configure the production network. Capturing real-time business traffic through the traffic collection network enables non-disruptive real-time monitoring of operations and allows for the addition of new tools for network analysis and monitoring as needed. The construction of a traffic collection network enables various types of analysis tools to share data at the traffic collection layer and optimizes the deployment and use of tools, saving overall investment for users.

3. Requirement analysis

As banking services continue to expand, the construction of branch networks and data center networks is also constantly expanding and improving, carrying an increasingly rich array of services. One of the challenges currently faced by network, security, and business operations teams is how to effectively monitor the operational status of the network, its security condition, and the operational status of the services it carries in a timely and effective manner. Currently, there are numerous tool software and systems available in the industry that can analyze raw network packets, parse various common and business protocols, analyze packet content, thereby achieving monitoring of network status, application status, and business status. "By deeply parsing the content of network traffic, real-time monitoring of user network behavior is possible, allowing for the immediate interruption of illegal operations. Additionally, past operation records can be stored for subsequent investigation and evidence collection."[1] This enables users to timely understand the characteristics of business traffic carried in data center networks, optimize network configuration adjustments to ensure the stable operation of core business applications in data centers, and promptly identify and resolve network fault risks and hidden dangers. For the banking industry, selecting tool-based software for gradual deployment to achieve visualized operations and maintenance is one of the inevitable steps to enhance operational strength. Various tool systems require collecting traffic from the network during deployment, and key nodes in the production network are locations of interest for each tool. If each tool system were to use its own method for traffic collection, it would result in redundant construction at the data collection layer, wasting investment. To better provide underlying traffic support for various tool systems, constructing an independent traffic collection network offers strong support for tasks such as network planning, network optimization, network monitoring, security surveillance, business traffic trend analysis, and fault localization.

4. Development journey

The traditional data collection network uses a simple networking approach, constructing the traffic collection network with an access and aggregation layer structure. Production traffic enters the traffic collection network through the access layer, where VLANs are added on the access layer devices before being sent to aggregation devices. From there, the aggregation devices forward the traffic to network, security, and application monitoring and analysis equipment, meeting their traffic collection needs. However, with the demand for traffic collection continues to increase, some problems will be resulted as shown in Fig.1:

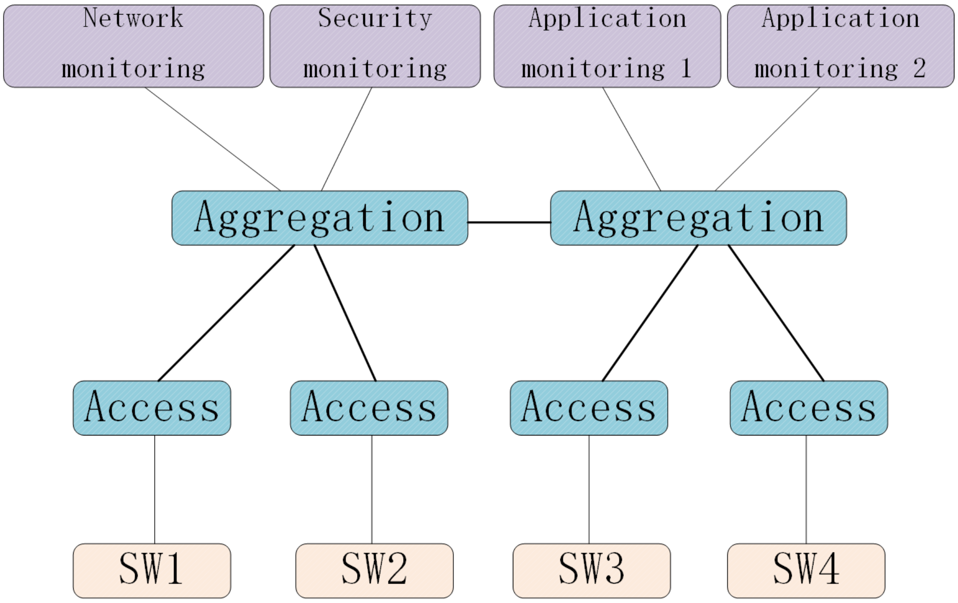

Figure 1: Figure Traditional data collection network

Low convenience in configuration

The configuration is complex, and adding new services requires changes to all devices along the path.

Difficulty in troubleshooting

As more services are continuously added, the configuration becomes increasingly complex and its readability is compromised, posing significant challenges for management and making problem diagnosis difficult.

Lack of redundancy

The traffic collection network devices are interconnected using a single line, and any interruption in these lines can affect normal traffic collection and forwarding. All traffic monitoring and analysis equipment are connected to the aggregation devices, and if the aggregation device fails, all the above traffic monitoring and analysis equipment will be unable to receive traffic.

Difficulty in expansion

With the increase in the number of devices, the amount of configuration increases geometrically, leading to unclear and chaotic traffic flows, making maintenance and expansion difficult.

5. Next-generation traffic collection network construction

To meet the continuously increasing operational and maintenance requirements, the banking industry has adopted the advanced SPINE-LEAF architecture to construct a next-generation traffic collection network. The next-generation traffic collection network has the following characteristics as shown in Fig 2:

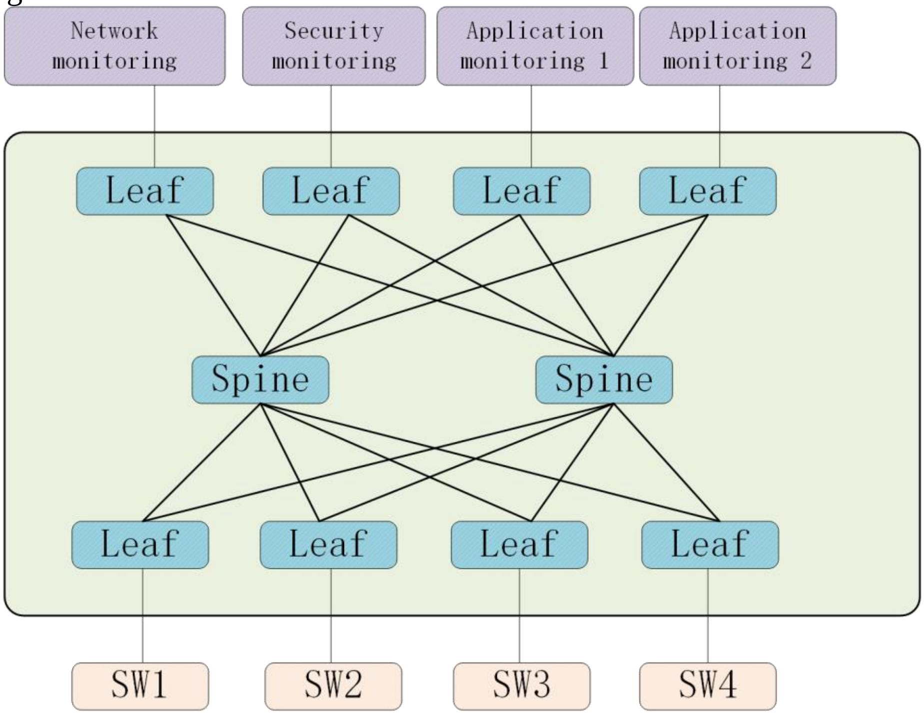

Figure 2: Figure Deployment architecture of traffic collection network

Unified configuration and management

The next-generation traffic collection network employs cluster technology to logically transform the entire traffic collection network into a single device. There is no need to log in to each device for configuration individually. Instead, one only needs to identify the corresponding interfaces of the traffic collection and monitoring analysis equipment, apply filters as needed, and traffic forwarding configuration can be completed. This achieves port-to-port traffic forwarding, simplifying both configuration and troubleshooting. The unified management platform provides comprehensive reporting functions, offering detailed insights into various aspects of traffic collection and transmission. This facilitates routine operational maintenance changes, data path organization, and troubleshooting efforts.

Easy to scale

Lateral expansion of devices is relatively easy, with leaf devices directly connecting to spine devices to join the cluster.

High link redundancy and availability

The traffic collection network is designed using a "Spine-Leaf" architecture, deployed in a three-tier structure consisting of access layer, aggregation layer, and monitoring output layer. "An irrational scheduling scheme can lead to overloading of certain processing cores while leaving others idle, resulting in packet loss and affecting the system's throughput performance."[2] To avoid packet loss, the technical implementation adopts a cluster deployment approach to achieve intelligent stacking or virtualization deployment of Network TAPs, forming a fully connected, intelligent load-sharing redundant cluster architecture with Network TAPs at the access layer, aggregation layer, and monitoring layer. The traffic from the traffic collection layer to the output layer is forwarded through the Spine for load distribution. The failure of a single interconnection link or a Spine device does not affect the entire traffic collection network's forwarding, achieving high availability of the architecture (Fig.3).

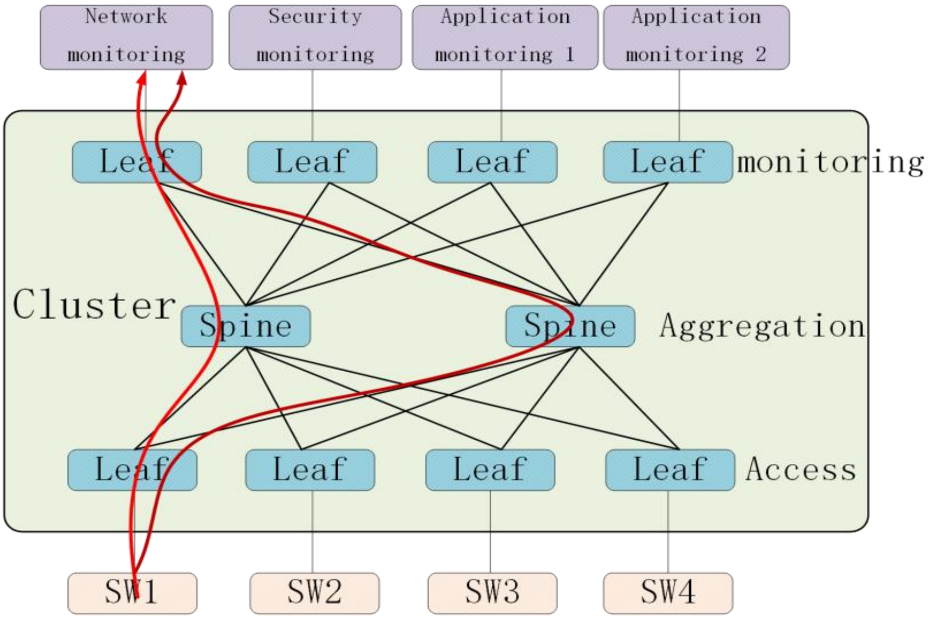

Figure 3: Figure Fault Traffic Forwarding Diagram

Metro cross-data center cluster formation

Using wavelength division multiplexing equipment to interconnect the Spine devices of the traffic collection networks in metro data centers, a cluster is formed across data centers, achieving sharing of the traffic collection layer and output layer. The same type of monitoring and analysis equipment only needs to be deployed in one data center, saving on equipment investment, as shown in Fig.4.

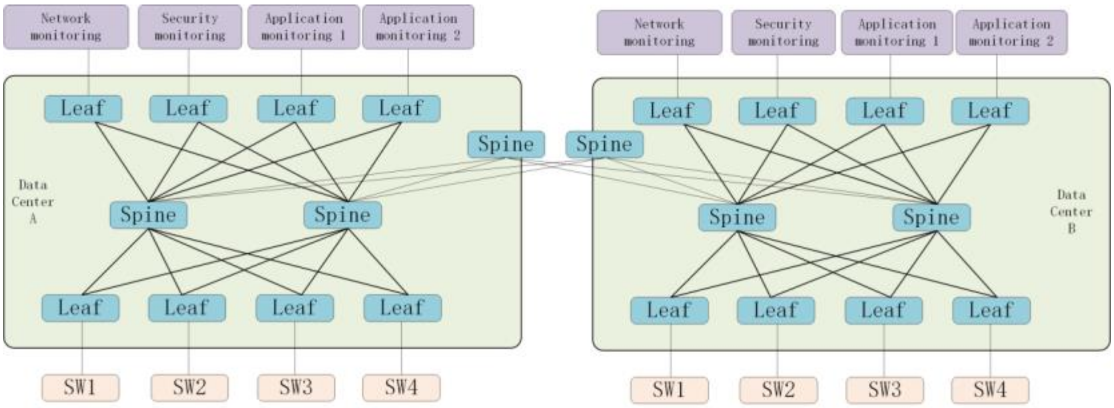

Figure 4: Figure Metro Data Center Architecture

Deployment of collection nodes within the cloud

As cloud services increasingly dominate the financial industry, there is a growing need for intra-cloud traffic collection. To meet this demand, traffic collection nodes are deployed within the cloud, achieving both internal and external cloud traffic collection through a combination of software and hardware approaches.

Support for advanced features

Advanced engines support data masking, deduplication, label stripping, packet slicing, IP tunnel termination, and other advanced features.

6. Conclusion and outlook

The initial deployment of the next-generation traffic collection network has been completed, providing strong support for network, security, and application traffic monitoring and analysis. As data center scales continue to expand, accommodating an increasingly diverse range of applications and traffic, we face more challenges. We believe that with the efforts of operations and maintenance personnel, our traffic collection network will be further refined to provide robust support for operational visibility, enhancing the business experience for our customers.

References

[1] Tang Zhibin. Survey of network data collection and security audit technology. Network New Media Technology, 2020, 9 (1): 11-20.

[2] Li Chuanhong, Zeng Xuewen. Survey of Network Full Traffic Collection and Analysis Technology [J]. Journal of Computer Science and Technology. 2022, 11 (02): 1-9.