Distributed Network Traffic Visualization and Analysis for Technical Support at the Beijing Winter Olympics: A Postprint

Authors: Kong Jiaquan

Date: 2023-10-08T00:00:00+00:00

Abstract

At the beginning of 2022, during the difficult moments of global pandemic response, China, in the name of the Winter Olympics, once again provided a Chinese solution for the development of the Olympic movement and contributed Chinese strength to building a community with a shared future for mankind. Xinhua News Agency dispatched a massive reporting team to provide comprehensive coverage of the Beijing Winter Olympics. Throughout the reporting period, various front-line and headquarters technical systems delivered a satisfactory performance with zero errors, among which distributed traffic visualization analysis technology was fully applied for the first time in Xinhua News Agency' s technical support for major reporting events. This paper not only introduces the key technologies and main functions of distributed traffic visualization analysis, but also describes the application of this technology in Xinhua News Agency' s major reporting on the Beijing Winter Olympics.

Full Text

Distributed Traffic Visualization Analysis Technology Supporting Beijing Winter Olympics Technical Operations

Author: Kong Jiaquan
Affiliation: Xinhua News Agency Communication Technology Bureau, Beijing 100803

Abstract: In early 2022, at a challenging moment of global pandemic response, China once again offered a Chinese solution for the development of the Olympic movement and contributed Chinese strength to building a community with a shared future for mankind. Xinhua News Agency dispatched a massive reporting team to provide comprehensive coverage of the Beijing Winter Olympics.

Throughout the reporting period, all frontline and headquarters technical systems delivered a satisfactory performance with zero errors, with distributed traffic visualization analysis technology being fully applied for the first time in Xinhua' s major reporting technical support operations.

This paper not only introduces the key technologies and main functions of distributed traffic visualization analysis but also examines its application in the Beijing Winter Olympics reporting operations.

Keywords: traffic visualization; distributed; edge computing; micro-probe; Beijing Winter Olympics

---

1. Main Challenges in Technical Operations

Today, IT infrastructure development across domestic industries is in a rapid growth phase, with business volumes increasing daily. As data centralization continues and more business systems come online, technical operations departments—serving as the core support for business operations—face enormous challenges and pressures. Effectively monitoring these complex business systems, preventing risks, ensuring high performance and availability of critical services, and optimizing existing operational processes to continuously improve management and operational levels have become urgent issues to explore and resolve. Currently, technical operations departments face several primary challenges.

First, operations management remains reactive, with personnel constantly working in a "firefighting" mode. While the infrastructure layer has achieved certain monitoring capabilities after years of effort—such as hardware status, system resource utilization distribution, and process running states—the existing monitoring system still struggles to detect problems in a timely manner when user access issues occur or are about to occur. Faults are typically discovered first by users or business personnel, with operations staff only becoming aware afterward and rushing to resolve them. The lack of proactive hazard elimination and early warning mechanisms for abnormal events is the main cause of this reactive posture.

Second, rapid technological development has outpaced available human resources, necessitating enhanced automated operations capabilities. As business demands diversify, operations departments face higher requirements for networks and applications. The frequency of new system deployments and network/application changes continues to increase, while the number of devices and applications grows and application architectures become increasingly complex. How to address these changes within the capabilities of existing human resources through automated tools has become a major challenge for many departments.

Third, incident response efficiency for sudden anomalies is insufficient. As information system architectures evolve with business needs, the number of appli-

cation nodes and logical call relationships between systems become increasingly complex, requiring maintenance across numerous links. With monitoring systems operating relatively independently, when problems arise, network, server, middleware, database, and storage personnel investigate causes separately, working in isolation. This leads to difficulties in evidence collection, low efficiency, and even mutual blame. Emergency response lacks clear direction, requiring significant time and communication costs for problem localization, resulting in prolonged incident resolution times that impact business operations.

2. Key Technologies and Main Functions of Distributed Traffic Visualization Analysis

With the rise of cloud computing and edge computing, how to achieve end-to-end network monitoring and full-process performance monitoring from client to server has gradually attracted operations personnel attention. Traffic visualization has been called "the last mile in unlocking big data value." Centered on big data analytics and artificial intelligence technology, it integrates internal information systems by aggregating relevant data from different sources and types for multi-dimensional big data analysis, with personalized configuration based on different positions, users, and business needs and permissions.

In many cases, edge computing and cloud computing have a symbiotic relationship. With the development and application of IoT, virtual reality, and augmented reality technologies, a data explosion will occur in the future. Relying entirely on cloud computing for data transmission and processing would create enormous network latency. Edge computing refers to an open platform that integrates network, computing, storage, and application core capabilities on the side near the source of data or objects, providing the nearest-end services. Its applications initiate at the edge, generating faster network service responses to meet basic industry requirements for real-time business, application intelligence, security, and privacy protection. Edge computing sits between physical entities and industrial connections, or at the top of physical entities. Meanwhile, cloud computing can still access historical data from edge computing.

The distributed architecture of edge computing can reduce latency while improving network resilience, reducing network load, and providing scalability. By processing data near the source, only data requiring further analysis needs to be sent to backend services, reducing networking requirements and centralized service bottlenecks. Caching data at edge locations or devices helps users avoid interruptions and improve system availability. Since less traffic needs processing, the demand for scaling centralized services is reduced, saving costs and lowering device complexity and management expenses.

Traditional traffic visualization analysis platforms, deployed in user data centers as hardware or software, monitor and analyze abnormal events in real time based on traffic and log data collected from the network. However, traditional probes—based on network traffic analysis characteristics—must be deployed close

to the source with low latency, imposing high requirements on the physical environment and necessitating data center deployment. Consequently, traditional network traffic analysis probes are mostly deployed in data centers, with monitoring capabilities extending only to areas with dedicated lines connected to the data center periphery.

The new generation of distributed traffic visualization analysis systems combines edge computing technology by deploying micro-probes on edge computing nodes to collect and analyze edge network traffic information, which is then sent to big data visualization systems deployed in data centers to achieve visual monitoring of edge network operation quality. Micro-probes use a bypass design for non-intrusive network monitoring with "zero" impact on existing networks and systems, enabling comprehensive and refined monitoring of all network traffic and critical services with scalable deployment capabilities. The system achieves both lightweight, portable, and diversified data collection.

Distributed traffic visualization analysis systems not only enable deep network and business performance visualization but also assist network operations departments in daily operational status checks, fault localization, and diagnostic analysis. The main functions include:

Data Unification. The system achieves unified collection, unified dimensions, unified metrics, and unified granularity of multi-source data, eliminating operations "information silos" and providing unified data management and correlation computing capabilities.

Data Visualization. Visualization capability is the core competency of operations, as management requires visibility. Eliminating visualization blind spots is a key user requirement. The system provides comprehensive data visualization capabilities, centrally presenting user experience status for data center access while also customizing end-to-end visualization monitoring based on application mapping results to display real-time operation status of critical application systems, including user experience, business availability, and business load. Data visualization encompasses several key elements: (1) **Unified**: placing traffic, logs, network management, CMDB, APM, NPM, probing, business monitoring, and alarm event data into a single interface; (2) **Practical**: enabling frontline operations personnel to quickly and efficiently identify problems; (3) **Flexible**: accommodating high-frequency interface display changes to meet different personnel, perspectives, and aesthetic needs while rapidly implementing customized views for business systems; and (4) **Aesthetic**: ensuring overall display effectiveness through diversified controls while maintaining practicality.

Data Mapping. When application systems experience anomalies requiring troubleshooting or impact analysis for changes, an accurate and authentic application topology diagram can greatly improve work efficiency. User data centers operate numerous application systems, and manually maintaining topology information would require enormous human resources while likely producing inaccurate information. The system automatically generates authentic, accurate

application topology diagrams based on real business call and access data. When applications change—such as adding new nodes or altering access relationships—the system automatically updates the topology, proactively sensing application changes to provide authentic, accurate data support for end-to-end traceability analysis.

Abnormal Access Identification. Even the most advanced attacks leave traces in the network. The system can obtain full network traffic, including network egress and internal networks. Analysis focuses on access relationships, establishing baselines based on historical behavior to identify newly added abnormal access. Combined with asset information and traffic dimension/metric data, it conducts secondary detection of new access within internal networks to achieve proactive monitoring of abnormal access.

Intelligent Monitoring and Alerting. Currently, most users' monitoring methods remain based on infrastructure-level hardware and resource monitoring, such as real-time operational efficiency of equipment in various machine rooms. While these systems can monitor visible device operation states in fine granularity, they lack monitoring capabilities for service quality and user experience of business systems carried by the equipment. This results in business access anomalies being discovered by business departments rather than monitoring systems. Leveraging the network' s characteristic of carrying applications, business, and user access, the system captures every user access in real time from network traffic, obtains full user experience data through parsing, and monitors the operation status of critical data center application systems through real user access data. When real user access anomalies occur, operations personnel can perceive and handle them promptly, thereby reducing fault impact.

Intelligent Analysis. Fault analysis currently relies heavily on operations personnel capabilities and experience. The system supports AI algorithm libraries and knowledge graphs, with built-in intelligent algorithms for machine learning, anomaly detection, multi-dimensional primary factor analysis, event correlation analysis, and prediction. It also incorporates knowledge graphs covering numerous fault scenarios. When alarm events occur, the system conducts automatic intelligent analysis, provides analysis reports, automatically locates root causes, and improves incident handling efficiency.

Data Inspection. As the carrier of business, network traffic contains extremely rich value. The system provides automated data inspection capabilities, conducting comprehensive data center inspection services based on collected data at regular intervals. It proactively discovers abnormal traffic and potential issues, such as open high-risk ports in internal networks, continuously declining host performance, increasing application service error rates, high-risk domain name access, and sudden abnormal traffic on links. Through scheduled inspections, operations personnel can discover and address hidden dangers in a timely manner, preventing unnecessary faults.

Statistics and Reporting. The system supports customized reporting func-

tions, enabling flexible and diversified reports for different departments, users, and scenarios, such as regularly generating application service quality ranking and optimization monitoring reports. It also supports automatically generating archivable short-term, medium-term, and long-term reports (daily, weekly, monthly) according to schedule, with customizable report types, formats, and content.

3. Application in Beijing Winter Olympics Technical Support

For the 2022 Beijing Winter Olympics coverage, Xinhua News Agency deployed converged applications including text, photos, Xinhua News Agency website, audio-video, voice, and video conferencing across headquarters, the Beijing Main Media Center (MMC), the Zhangjiakou Mountain Media Center (ZPC), and various competition venues. Considering pandemic regulations, a dispatch center was established at headquarters with editorial departments shifting backward, requiring coordinated frontline-headquarters reporting and the establishment of a stable, efficient, secure, and controllable network platform for data transmission among the four reporting planes. Additionally, to facilitate journalists working at MMC and ZPC in querying internet-related information, local dedicated internet lines needed to be accessed with Wi-Fi coverage in Xinhua workspaces to meet mobile terminal access requirements.

The Press Plus service, provided by the Beijing Winter Olympics Organizing Committee for major news agencies, relies on wired and wireless networks in venues to connect all competition venues, opening/closing ceremony venues, and award plazas with offices rented by news agencies at MMC through dedicated high-bandwidth, clearly classified network connections. As a member of the International Olympic Photo Pool (IOPP), all Xinhua photographers relied on the Press Plus network to transmit photos in real time to MMC's image receiving servers.

In previous major coverage events, technical personnel deployed traffic visualization analysis systems at headquarters to monitor and analyze data flows between frontline and headquarters but could not monitor data flows between frontline internet business areas and various frontline zones. For the Beijing Winter Olympics, the first-time deployment of a distributed traffic visualization analysis system enabled comprehensive monitoring of all critical data flows between frontline and headquarters.

At MMC, three micro-probes were deployed: the first on the MMC business aggregation switch to obtain all upstream traffic to headquarters via port mirroring, including intranet, Xinhua News Agency website, and audio-video transmission services; the second on the MMC internet switch to capture MMC internet access traffic via port mirroring, including wired and wireless internet; and the third on the Press Plus access switch to obtain all venue-to-MMC intranet image server transmission traffic via port mirroring, including venue Press Plus instant photo transmission and venue internet photo dispatch ser-

vices. At ZPC, two micro-probes were deployed: the first on the ZPC business aggregation switch to obtain all upstream traffic to headquarters via port mirroring, including intranet services; and the second on the ZPC internet switch to capture ZPC internet access traffic via port mirroring, including wired and wireless internet.

Through customized interfaces, the system can display real-time operational status of monitoring points and related services, including inbound/outbound throughput, packet loss rate, latency, visit volume, TCP establishment time, traffic ranking, and other information [Figure 1: see original paper].

The system can also display data curves for specified venues during designated time periods [Figure 2: see original paper], such as the Bird's Nest data throughput curve on the opening ceremony day, clearly showing large data transmissions around fireworks displays and the main torch ignition, with real-time throughput reaching 800Mbps.

During the Beijing Winter Olympics, frontline technicians used the system' s reporting function to conduct daily statistics on traffic from various business systems and venues. Taking opening day as an example, from 00:00 on February 4 to 00:00 on February 5, 2022: MMC area recorded 38.63 GB of intranet traffic, 8.77 GB of wired internet traffic, 35.26 GB of wireless internet traffic, 4.32 GB of Xinhua News Agency website traffic, and 299.8 GB of audio-video traffic; ZPC area recorded 2.95 GB of intranet traffic, 1.79 GB of wired internet traffic, and 5.76 GB of wireless internet traffic; venue areas recorded 493.65 GB at the Bird' s Nest, 3.09 GB at the National Indoor Stadium, 18.76 GB at the Wukesong Sports Center, 1.89 GB at the Zhangjiakou Biathlon Center, and 16.49 GB of internet photo dispatch traffic.

The distributed traffic visualization analysis system employs edge computing technology and uses micro-probes for traffic data collection and analysis. Meeting Xinhua' s requirements for miniaturized frontline equipment in major coverage events, it enables technical personnel to monitor network quality in frontline and headquarters environments and promptly grasp the operational status and network quality of various business systems and equipment. Additionally, technical personnel can use customized network monitoring views to monitor network performance at MMC, ZPC, the National Stadium, and 14 competition venues and award plazas in real time, providing strong support for Xinhua' s efficient network operations during the Beijing Winter Olympics.

As new technologies continue to develop, distributed traffic visualization analysis technology can help technical management departments evolve operations from tool-based to automated and intelligent approaches. Using data as an entry point for business-oriented data visualization analysis can solve practical problems in current operations management and further enhance operational management levels and technical service capabilities.

References: [1] Shan Desheng, Qian Yekui. Analysis of Main Methods of Network Traffic Monitoring Technology[J]. Electronic Test, 2017(17): 69-70. [2]

Lin Yangguang. Construction and Analysis Methods of Network Traffic Data Visualization[J]. Digital Communication World, 2017(3): 112-115. [3] Xinhua News Agency Beijing Winter Olympics Reporting Team. Panoramic Recording of Extraordinary Ice and Snow Event, Vivid Presentation of Excellent Chinese Answer—Xinhua' s Beijing 2022 Winter Olympics Coverage Successfully Concluded[J]. News Business, 2022(13): 3-5.

Author Biography: Kong Jiaquan (1979-), male, Beijing, senior engineer. Research direction: construction and maintenance of Xinhua News Agency' s basic network platform.

Note: Figure translations are in progress. See original paper for figures.