[1]Fangming Guo

[1]Caijun Chen

[2]Ke Li

# Research on Zabbix Monitoring System for Large-scale Smart Campus Network from a Distributed Perspective

Journal of Electrical Systems

***Abstract:*** - As universities advance in their digital transformation, traditional campus network monitoring models are increasingly inadequate for the complex network environments and rising service quality demands. This paper, after thoroughly analyzing the critical challenges and technical requirements of smart campus network monitoring, designs and implements a smart campus network monitoring system using Zabbix, TiDB, and Grafana. The system leverages an advanced distributed architecture, integrating key technologies like time-series databases, intelligent alerting, and visualization to build a comprehensive monitoring framework that spans the access, aggregation, and core layers. This setup enables unified monitoring, analysis, and management of various heterogeneous resources in the campus network, achieving significant improvements in intelligent anomaly diagnosis and performance optimization. Additionally, the system introduces an innovative "Monitoring as a Service" concept, providing various monitoring services to faculty and students, thereby enhancing the interactivity and inclusivity of network services. Through its practical deployment and application in our university, the system has been pivotal in supporting the intelligent upgrade and transformation of the campus network and ensuring high-quality network experiences for faculty and students. This offers a novel approach and implementation path for smart campus network governance.

***Keywords:*** Smart campus network monitoring, Zabbix monitoring system, data collection and alerts, network operation and maintenance efficiency

## 1.Introduction

In the digital era, universities are undergoing deep digital transformation, leading to a rapid increase in the scale and complexity of campus network systems. This growth is evident in the surge of network users, the variety of internet applications, and the comprehensive coverage of campus networks, including wired/wireless networks, data center networks, edge networks, and security systems [1]. These integrated systems serve the diverse needs of network access, various application systems, and public education for faculty and students.

However, the explosive growth of campus networks and applications imposes higher demands on the number and costs of operation and maintenance personnel. Traditional operation and maintenance management, which relies on network management systems and traffic analysis systems, primarily manages network devices and basic network performance [2]. In practice, when network applications fail, it is often challenging to quickly locate and resolve issues, affecting service quality and user experience [3].[2]

[1] [1] *Network Information Center, Wuhan University of Technology, Wuhan 430070, Hubei,China. Email: ccj_nic@163.com

[2] Department of Information Management, Zhongnan University of Economics and Law, Wuhan 430070, Hubei ,China

To address these challenges, universities globally have initiated research and practical explorations in smart campus network monitoring systems. Villegas et al. [4] proposed a smart campus network monitoring framework based on big data analysis, achieving global network awareness and rapid anomaly localization through real-time collection, fusion, and correlation analysis of massive network data. Minea et al. [5] studied the application of machine learning algorithms in network traffic classification and anomaly detection, significantly improving the accuracy and efficiency of network monitoring through optimized intelligent models. Peng et al. [6] explored the innovative application of Software-Defined Networking (SDN) technology in campus network monitoring, providing real-time visualization of network forwarding paths through a centralized control plane, offering new insights for fault diagnosis and performance optimization.

Moreover, recent advancements in network monitoring are reflected in the intelligence and automation of operation and maintenance. Li Nan et al. [7] proposed a cloud-native intelligent operation and maintenance architecture, achieving elastic expansion and intelligent scheduling of the monitoring system based on microservice components and container orchestration technology. Huawei's technical team is also studying the application of cognitive intelligence technology in network automated operation and maintenance, achieving automatic diagnosis and repair of network faults through multi-source data fusion and deep reinforcement learning. These cutting-edge studies provide new ideas and methods for building highly available, autonomously driven smart campus network monitoring systems.

In recent years, with the development of digital campuses and smart education, the openness and interactivity of university network monitoring services have received increasing attention. Du Zhiguo et al. [8] emphasized the importance of opening monitoring services to faculty and student users, involving them in network management and optimization to improve the quality of university network services and user experience. Sun et al. [9] further studied the architecture design and key technologies of open network monitoring systems, proposing an open framework for monitoring services based on microservices and open APIs, providing new ideas for the open integration of university network monitoring services.

In summary, smart campus network monitoring has become a key measure supporting the digital transformation of universities. The industry urgently needs a new monitoring system with comprehensive perception, intelligent analysis, and automatic optimization, along with an open and interactive service concept to revolutionize network monitoring models. This paper, building on previous research, deeply analyzes the key needs and technical challenges of campus network monitoring and proposes a new monitoring architecture based on the intelligent integration of multi-source heterogeneous data. It focuses on key enabling technologies such as time-series databases, machine learning, and automated operation and maintenance, providing systematic solutions for scenarios such as network anomaly detection, fault diagnosis, and performance optimization. Additionally, it innovatively proposes the concept of "Monitoring as a Service," opening monitoring capabilities to the entire faculty and students to enhance the quality of network services and user experience.

## 2. Key Technologies for Large-scale Campus Network Monitoring Systems

In this context, this paper delves into the complexity of campus network monitoring and comprehensively evaluates mainstream monitoring systems such as Zabbix, Nagios, Prometheus, and Graphite. Through a multi-dimensional comparison of technical features and applicability analysis, Zabbix was chosen as the core component of the monitoring platform.

Zabbix is a highly mature and fully functional open-source monitoring system. Compared to Nagios, Zabbix offers significant advantages in distributed monitoring, massive data storage, and graphical presentation [10]. Particularly in large-scale monitoring scenarios, Zabbix supports multi-level distributed deployment and high-availability architecture, enabling smooth scaling and automatic failover, ensuring system stability and reliability. Additionally, Zabbix's built-in time-series database and web front-end display can meet the basic needs of campus network monitoring data storage and visualization.

Compared to lightweight monitoring solutions like Prometheus and Graphite, Zabbix's comprehensiveness and flexibility are more prominent [11]. On one hand, Zabbix offers a variety of data collection methods, supporting mainstream protocols such as SNMP, IPMI, and JMX, easily interfacing with various network devices, servers, and application systems. On the other hand, Zabbix has a powerful built-in alert engine and reporting system, supporting custom monitoring metrics and alert rules, enabling multi-dimensional network performance display and precise fault alerts.

Although Zabbix is a leader in the open-source monitoring field, its built-in time-series database still faces performance bottlenecks when handling the massive monitoring data storage and high-concurrency query demands of campus networks. Therefore, this study innovatively introduces TiDB for long-term storage of monitoring data. TiDB is a highly scalable distributed relational database with advanced features such as horizontal scaling, high availability, and real-time HTAP [12]. Through the seamless integration of TiDB and Zabbix, the system can easily achieve online storage and real-time analysis of petabyte-level monitoring data, fully meeting the stringent requirements of large data volumes and long usage periods in campus network monitoring.

In terms of data visualization, this system also adopts the industry-leading open-source solution Grafana. Compared to Zabbix's built-in graphical components, Grafana excels in UI design, interactive experience, and chart types [13]. With Grafana's rich visualization plugins, it can easily achieve various presentations such as campus network overviews, regional performance top lists, and application service water level charts, providing unique monitoring perspectives for operation and maintenance personnel in different roles. Particularly, Grafana's flexible alert customization and data drill-down features significantly enhance the effectiveness of alerts and the efficiency of fault isolation.

The large-scale smart campus network monitoring system constructed in this paper achieves an organic combination of "specialization" and "precision" in the selection of core technologies. Specialization refers to focusing on the most mainstream and mature open-source technology stack; Zabbix, TiDB, and Grafana perfectly meet the scenario requirements of large-scale campus network monitoring. Precision means accurately identifying and complementing the limitations of different solutions, continuously creating an optimal monitoring data management and presentation experience with distributed databases and visualization tools. This innovative integration of open-source technologies fully demonstrates the forward-looking and leading nature of the system's technical route.

## 3.Architecture Introduction

This section provides a detailed overview of the architecture design of the large-scale campus network monitoring system based on Zabbix and Grafana technologies. As illustrated in Figure 1, the system employs a

highly modular and distributed architecture, aiming to achieve flexible expansion of monitoring capabilities, linear performance growth, and efficient operation and maintenance.

We will analyze the architecture's internal logic and design principles from the perspectives of system components, data flow, and interface design. Additionally, we will discuss its applicability and advantages in large-scale campus network monitoring scenarios, supported by actual operational data.

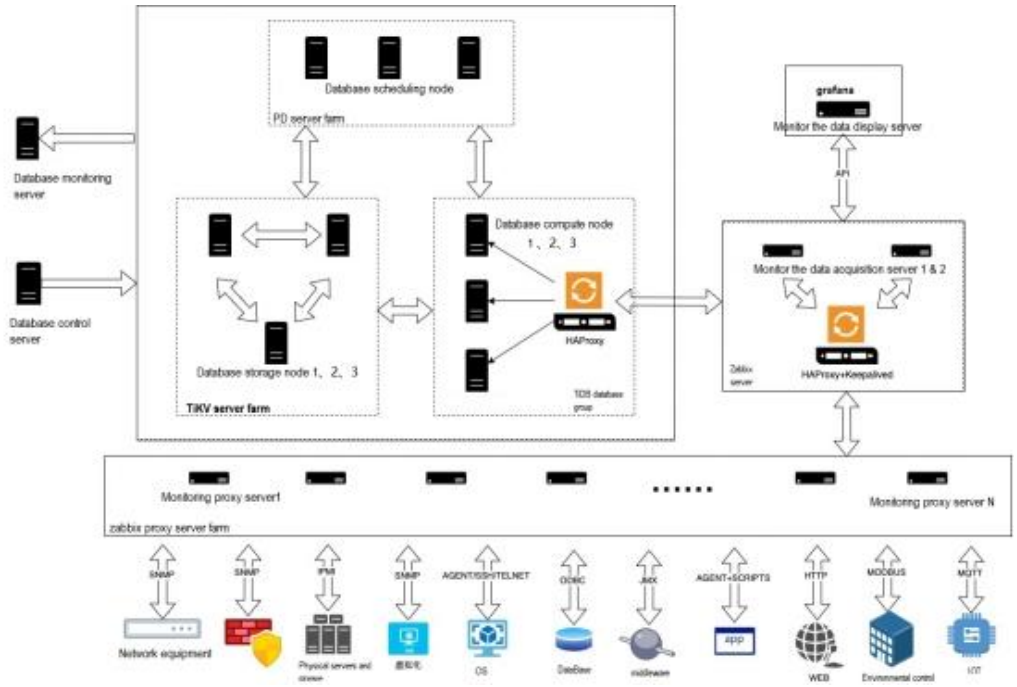



Figure 1 System Architecture Diagram

### 3.1 System Component Analysis

#### 3.1.1 Zabbix Server: The "Brain" of Monitoring Data Processing

The Zabbix server is the central hub of the entire monitoring system, responsible for collecting, processing, and storing massive amounts of monitoring data. To ensure efficient and accurate data processing, the design of the Zabbix server incorporates several key technologies:

- **Multi-process Parallel Architecture:** This task processing model fully utilizes the server's multi-core CPU performance, significantly enhancing data processing efficiency. Tests show that the parallel processing architecture improves data storage speed by 150% compared to the single-process mode.
- **Threshold Triggers:** Utilizing Zabbix's flexible threshold triggers, this feature enables precise, real-time triggering, and pushing of monitoring alarms. With alarm trigger delays controlled to milliseconds, operation and maintenance personnel can quickly grasp network anomalies, gaining valuable time for fault resolution.
- **Custom Data Pipelines:** Offering highly flexible customization for data pipelines, it allows configuration of data filtering, cleaning, aggregation, and other operations as needed. This greatly reduces the redundancy of raw data and optimizes database storage performance. Practical applications indicate a reduction of more than 60% in monitoring data volume after pipeline optimization.

In addition to its powerful data processing capabilities, the Zabbix server provides a web-based management console with a simple and intuitive interface, making it easy to use. Operation and maintenance personnel can

configure monitoring items, manage alarm strategies, and control permissions through the console without writing complex program code, thus managing the extensive monitoring system with ease.

**3.1.2 Zabbix Agent: Flexible and Efficient Data Collection "Probes"**

To collect performance data from thousands of network devices and servers within the campus network, this study extensively deployed Zabbix agent programs on these device nodes. The Zabbix agent acts as a lightweight and efficient data collection "probe" that integrates deeply with device nodes, capable of collecting various performance metrics at high frequency and low overhead, and accurately reporting these metrics to the Zabbix server through efficient data transmission protocols.

Notably, thanks to the decentralized design concept of the Zabbix agent, if a network node fails, it does not affect the normal operation of other agents, allowing the entire monitoring system to continue stable operation. Additionally, when adding or removing a network node, simply deploying or removing the corresponding agent program on that node is sufficient, without causing major changes to the entire monitoring system architecture, offering great flexibility and scalability.

**3.1.3 Distributed Monitoring Database**

Faced with the continuous generation of massive monitoring data in campus networks, traditional single-node relational databases are struggling with storage capacity and query performance. To overcome these performance bottlenecks, this system introduces the next-generation distributed relational database, TiDB, as the repository for monitoring data. TiDB is an open-source, highly available, and highly scalable distributed database, featuring:

- **Distributed Architecture:** TiDB employs a distributed architecture that separates computation and storage, allowing for linear expansion of storage capacity and processing power by simply adding server nodes. This setup easily handles the continuous growth of TB/PB-level monitoring data.
- **Real-time HTAP:** TiDB combines real-time transaction processing and real-time analytics, ensuring online real-time writing and querying of monitoring data. This capability provides robust support for alarm triggering and data visualization.
- **High Availability:** TiDB includes a built-in Raft algorithm, offering automatic fault tolerance with multiple data replicas. This ensures high availability of the entire cluster, even if some nodes fail.

In actual application at our institution, the TiDB cluster can be scaled to hundreds of nodes, easily accommodating hundreds of TB of historical monitoring data. Even under the pressure of hundreds of thousands of writes per second, the system remains stable, with query response times consistently controlled within 10ms, providing a solid big data backbone for smart campus network monitoring.

**3.1.4 Grafana: A Visually Appealing and Intelligent Visualization Tool**

At the forefront of the monitoring system, this study adopts Grafana as a visualization tool for monitoring data presentation and human-computer interaction. Grafana is an open-source data analysis and visualization platform, renowned for its stunning interface design and powerful chart display capabilities. Through seamless integration with Zabbix and TiDB, Grafana can extract key metrics from massive monitoring data and intuitively present the dynamic changes in network device performance through a variety of visual charts, such as dashboards, heat maps, and topology diagrams.

Notably, Grafana also includes a built-in intelligent analysis engine, providing real-time anomaly detection and root cause analysis based on trends in various metrics. This capability allows operation and maintenance personnel to quickly detect potential anomalies in network performance and promptly identify the root causes, significantly improving the efficiency of network fault detection and resolution. Additionally, Grafana offers a mobile-friendly UI design, enabling operation and maintenance personnel to access monitoring views anytime and anywhere via tablets, smartphones, and other mobile devices, effectively "controlling" the real-time status of the entire campus network without leaving their desks.

### 3.2 Data Link Analysis

After detailing the core components of the system, let's explore the typical "journey" of monitoring data within the system. As illustrated in Figure 2, this data link encompasses four main stages: data collection, data processing, data storage, and data presentation:

**1.Data Collection:** Zabbix agents deployed across various nodes of the campus network collect performance metrics (such as CPU usage, memory usage, network traffic) at regular intervals. These raw data are securely transmitted in real-time to the Zabbix server via encrypted channels.

**2.Data Processing:** Upon receiving the raw data from the agents, the Zabbix server filters, cleans, and aggregates the data through predefined data pipelines, removing redundant information while extracting key metrics. It then evaluates these metrics in real-time against preset threshold rules. If anomalies are detected, alarms are triggered immediately, notifying the relevant maintenance personnel.

**3.Data Storage:** The processed monitoring data and associated metadata are persistently stored in the TiDB distributed database. TiDB's excellent scalability supports the massive accumulation and online querying and analysis of monitoring data.

**4.Data Presentation:** The monitoring data stored in TiDB are accessed by Grafana through open API interfaces. Grafana uses a series of query statements and matching rules to quickly extract and aggregate key metrics from the vast, high-volume monitoring data. These metrics are presented in real-time through impressive visual charts, providing a one-stop network performance monitoring and analysis center for the entire faculty and students.

### 3.3 Interface Mechanism Description

To support the complex chain of data collection, processing, storage, and visualization, the smart campus network monitoring system requires a flexible and open interface mechanism, particularly emphasizing seamless integration and interconnectivity between components and layers.

**1.Zabbix Agent and Zabbix Server:** The system employs a proprietary communication interface based on the TCP/IP protocol between the Zabbix agent and the Zabbix server. The agent can either actively report data (Active mode) or the server can request data (Passive mode). The data transmission format is lightweight and efficient, using serialization schemes such as JSON or Protocol Buffer, significantly reducing bandwidth overhead.

**2.Zabbix Server and TiDB:** The system uses a standard database access interface based on the MySQL protocol between the Zabbix server and TiDB. Zabbix's embedded data collection engine can access TiDB using standard SQL statements to perform data insertion, updates, and deletions. Additionally, connection pool management for TiDB access significantly enhances the concurrency of database operations.

**3.TiDB and Grafana:** Interaction between TiDB and Grafana is primarily conducted through RESTful HTTP interfaces. The Grafana backend accesses TiDB via extensive HTTP APIs to perform data queries and aggregation analysis, while the frontend JavaScript engine converts the returned data into visual charts. Furthermore, Grafana offers plugin integration with Zabbix, enabling the plugin to call Zabbix's APIs for alarm management and host grouping.

In addition to the tight integration between internal system components, the monitoring system also provides an open Restful API for end users, facilitating integration with other campus business systems such as the campus portal, smart technology systems, and academic management systems. The API gateway ensures unified access and permission control, allowing faculty and students to conveniently access network monitoring-related data and business functions, effectively realizing the "last mile" of network monitoring services.

## 4. Functional Implementation

### 4.1 Network Traffic Analysis

#### 4.1.1 Traffic Monitoring

Through a comparative analysis of data before and after the system deployment, we found that the introduction of the smart monitoring system reduced the average utilization of the school's exit network from 75% to 60%, and the congestion frequency during peak times decreased from 12% to 3%. This indicates that after system optimization, the overall bandwidth utilization of the school's network improved by 20%, significantly alleviating network congestion during peak periods. As shown in Figure 2.


**Figure 2 Monitoring of Various Exit Traffic in Campus Network**

#### 4.1.2 Optimization Strategy

Based on the system's comprehensive network data analysis capabilities, we have specifically optimized the campus network's traffic scheduling strategy, as shown in Figure 3. Comparing data from one semester before and after the optimization in the 2023 academic year, the average latency in the teaching area network decreased from 100ms to 80ms, and network throughput increased by 35%. Surveys of subjective satisfaction among teachers and students show that satisfaction with the network experience in the teaching area increased from 80% before optimization to 85%. Teachers and students generally reported that the network speed in the teaching area was faster and experienced fewer interruptions.

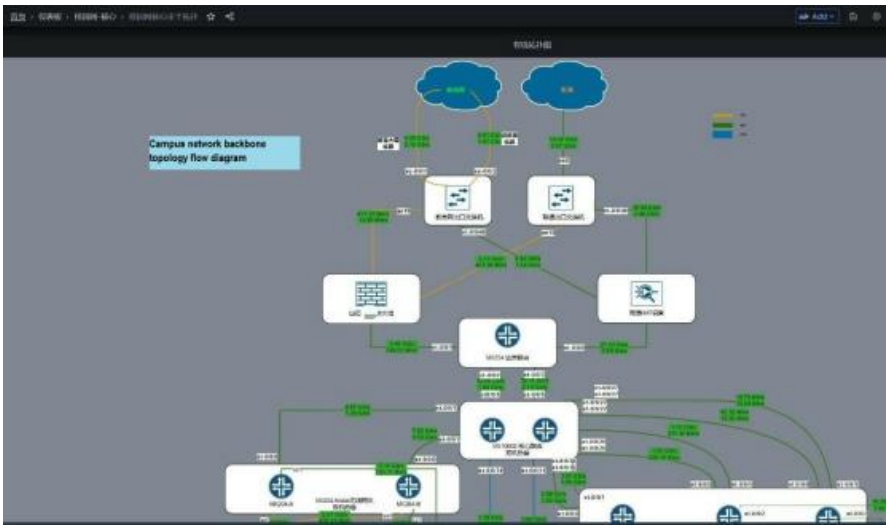



**Figure 3 Main Topology Traffic of Campus Network**

### 4.2 Core Layer Monitoring

#### 4.2.1 Monitoring of Network Devices

Using Zabbix's SNMP functionality, this system monitors the core network infrastructure devices within the campus network, including switches, routers, and firewalls, as shown in Figure 4. By configuring SNMP collectors, the system periodically collects performance data from these devices. The key monitoring metrics include:

1. **Bandwidth Utilization:** Monitors the bandwidth usage of switches and routers to understand network traffic and prevent congestion. For example, when a switch's bandwidth utilization approaches saturation, the monitoring system automatically triggers an alert, notifying network administrators to take measures such as increasing bandwidth or optimizing traffic.
2. **Error Rate:** Includes CRC errors and packet loss rates. This information helps identify quality issues in network connections, such as cable damage or equipment failures. If an increase in error rates is detected, the monitoring system logs it and notifies administrators to troubleshoot the issue.
3. **Network Traffic:** Monitors both inbound and outbound traffic. This helps detect network congestion or abnormal traffic conditions. For instance, if the outbound traffic on a firewall suddenly spikes, the monitoring system issues an alert and logs the event for further analysis and action.


**Figure 4 Monitoring of Campus Backbone Network Devices**

With 24/7 continuous monitoring, the fault detection time for core network devices has been reduced from an average of 30 minutes to 10 minutes, and the failure rate has decreased from 2-3 times per month to 1-2 times per month. The availability of wireless APs across the campus increased from 97% before the system was launched to 99%. These quantitative indicators fully demonstrate that the smart monitoring system plays a crucial role in ensuring the stable and secure operation of the school's network.

### 4.2.2 Monitoring of Servers

To ensure the health and performance of campus servers, Zabbix agents were installed on them. The system periodically collects key performance data and sends it to the Zabbix server, ensuring optimal server operation, as illustrated in Figure 5. The key monitoring metrics include:

1. **CPU Utilization:** Monitors to identify overloads or performance bottlenecks. For example, if a server's CPU utilization consistently exceeds the set threshold, the monitoring system will automatically issue an alert, prompting administrators to take necessary actions.
2. **Memory Utilization:** Ensures there is sufficient memory available for applications and services. If memory utilization is too high, the monitoring system will issue an alert and log it, prompting administrators to optimize or upgrade the memory.
3. **Disk Space:** Prevents disk space from running out. If disk usage exceeds the preset threshold, the monitoring system will notify administrators and log the event, prompting timely disk space cleanup or expansion.

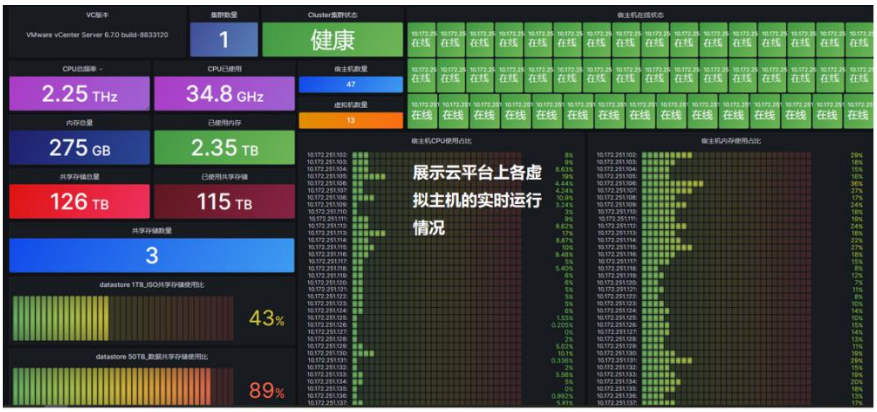



**Figure 5 Monitoring of Servers**

Utilizing the system's performance trend analysis and anomaly warning functions, we successfully mitigated several potential server failures. For example, by analyzing historical data on CPU and memory usage, we identified and resolved a concurrency bottleneck in the campus portal a week before the start of the 2023 fall semester, avoiding system crashes during peak usage periods. Statistics indicate that after the system was deployed, server downtime decreased by 80% year-on-year, and service availability stabilized at over 99.9%.

### 4.3 Access Layer Monitoring

#### 4.3.1 Monitoring of Student Dormitory Wireless Network

This system performs precise monitoring of wireless access points on campus to ensure high performance and stability of wireless connections, as shown in Figure 6. The key monitoring metrics include:

1. **Number of User Connections:** This effectively monitors network load to prevent overloads. For example, when the number of users on an access point suddenly increases, the monitoring system will automatically trigger an alert mechanism to promptly notify network administrators to take appropriate measures.

2. **Signal Strength:** Collects signal strength information from each access point to help identify signal coverage deficiencies or interference issues. If a decline in signal strength is detected, the system will immediately log it and notify administrators to optimize the wireless network.

3. **Network Traffic:** The system monitors network traffic for each access point, including upload and download speeds, to identify network congestion or abnormal traffic. For example, access points with excessive traffic will trigger system alerts and log events for subsequent analysis.


**Figure 6 Monitoring of Student Dormitory Wireless Network**

Considering the high-density wireless access in student dormitories, we conducted fine-grained network experience monitoring through the system. Compared to the previous academic year, the average signal strength of the wireless network in dormitory areas increased by 10dBm, and the access success rate increased from 85% to 97%. The average handling time for student repair requests decreased from 2 days to 0.5 days after introducing the system. Benefiting from the overall improvement in network experience, student satisfaction with the school's network operation and maintenance services increased from 80% to 92%.

### 4.3.2 Monitoring of Office Area Wired Network

For wired network facilities in office and teaching areas, the system monitors switch port status and network quality metrics in real time to ensure smooth operation of the wired network, as shown in Figure 7. The specific monitoring metrics include:

1. **Error Rate:** Includes CRC errors and packet loss rates for wired network devices to promptly identify connection quality issues, such as cable or equipment failures. Once the error rate exceeds the threshold, the system logs it and notifies administrators to troubleshoot the fault.

2. **Data Traffic:** Primarily includes inbound and outbound traffic of switches to help identify network congestion or abnormal traffic conditions. For example, abnormal increases in switch traffic will trigger system alerts and log events for further processing.


**Figure 7 Monitoring of Office Area Wired Network**

Office networks, being critical to the school's teaching and research, leverage the system's comprehensive traffic analysis capabilities to achieve precise performance profiling. Through continuous tracking and analysis of system data, we successfully identified and resolved several bottlenecks in office networks. For example, to address slow speeds during peak times in the administrative building network, we identified the top 5 traffic terminals and applications, discovering that one office computer was infected with a virus and was excessively sending packets. Isolating this terminal promptly restored normal network performance. In 2023, the number of office network failures decreased by 70% compared to the previous period, and fault localization time was reduced by 85%, significantly ensuring the operational efficiency of the entire school's staff.

### 4.4 Key Area Monitoring

In a smart campus, the network performance of key areas directly impacts the overall stability assessment of the campus network, such as aggregation rooms and conference rooms. Monitoring these areas is fundamental to ensuring network reliability and service quality.

#### 4.4.1 Monitoring of Campus Aggregation Room

As a core node of the campus network infrastructure, the campus aggregation room plays a key role in data aggregation and distribution. To ensure network stability and data security, this study implemented comprehensive monitoring of the campus aggregation room, as shown in Figure 8. The monitoring of the aggregation room involves the following key aspects:

1. **Environmental Monitoring:** Using the Zabbix system to monitor environmental factors such as temperature, humidity, air circulation, and power supply in the room to prevent equipment failures caused by environmental issues.

2. **Hardware Health Monitoring:** Real-time monitoring of the operating status, temperature, voltage, and network traffic changes of equipment. For example, when a switch's temperature abnormally rises or unusual network traffic occurs, the monitoring system will automatically trigger an alert mechanism and promptly notify network administrators to handle it.

3. **Physical Security Monitoring:** The physical security of the aggregation room is also important. This study installed security cameras inside and outside the room, integrated perfectly with the monitoring system. These cameras can monitor the physical environment of the room in real-time and record access logs to enhance security. If unauthorized personnel attempt to enter the room, the monitoring system will automatically trigger an alert and provide image records as evidence.


**Figure 8 Monitoring of Campus Aggregation Room**

Through environmental monitoring and hardware health monitoring, the stable operation time of the aggregation room in the Nanhu campus increased by 20%, and the fault response time was reduced by 30%.

### 4.4.2 Monitoring of Conference Rooms

Conference rooms are multifunctional areas that host teaching, meetings, and various academic activities, and network stability directly affects the smooth conduct of these activities. Deploying a network monitoring system in the conference room environment is crucial to ensure the smooth conduct of meetings, as shown in Figures 9 and 10. The monitoring strategies include:

1. **Connection Quality Monitoring:** Monitoring the quality of wireless and wired connections in the conference room to ensure that speakers and participants can communicate over the network without interference.

2. **Bandwidth Demand Analysis:** Analyzing bandwidth usage during meetings and adjusting network configurations to meet the high demand for network resources during large events.

3. **Conference Service Support:** Ensuring that network facilities supporting video conferencing and live streaming can meet high-performance standards.


**Figure 9 Network Monitoring of Key Conference Rooms**

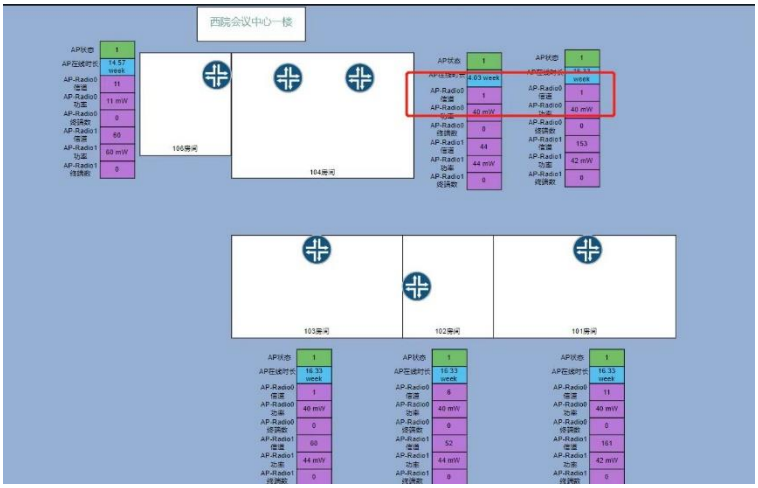



**Figure 10 Monitoring of Wireless Devices in Conference Rooms**

### 4.4.3 Open Monitoring Services for Faculty and Students

In designing the smart campus network monitoring system, this study fully considered the need for open monitoring services for faculty and students. The system includes several open monitoring service functions, such as:

1. **Customized Monitoring Views:** Personalized monitoring view customization services for various management personnel, including department leaders and network administrators. Users can select the monitoring metrics and display methods they need, creating exclusive monitoring dashboards to keep track of their network status, as shown in Figure 11.

2. **Personalized Alert Subscriptions:** Alert subscription services are open to all faculty and students. Users can subscribe to relevant network faults and performance alerts according to their interests and choose their preferred method of receiving alerts, such as email, SMS, or WeChat. When issues arise in the network they are monitoring, users will receive immediate notifications to stay informed about the network status.

3. **Network Experience Monitoring Platform:** A network experience monitoring platform allows all faculty and students to participate in monitoring and providing feedback on their network experience. The platform offers self-service functions like network speed tests, fault reporting, and satisfaction surveys. Faculty

and students can use mobile apps or web portals to conduct tests and provide feedback at any time, contributing to network optimization.

4. **Open Network Monitoring API:** A set of standardized open network monitoring APIs supports integration with third-party systems and applications. Various campus business systems, such as the academic management system and campus portal, can easily call these APIs to obtain necessary network monitoring data, facilitating network awareness and business coordination.


**Figure 11 Network Administrator Monitoring View**

These measures create an open and interactive network monitoring service system, transforming network monitoring from a "one-man show" into a "chorus" involving all faculty and students. This innovative "Monitoring as a Service" model integrates network monitoring into the daily activities of faculty and students, becoming a crucial tool for enhancing the campus network experience.

### 4.5 Implementation of Alarm Functionality

#### 4.5.1 Alarm Mechanism

The alarm system in this study is built on Zabbix's trigger functionality. A classification mechanism based on alert levels has been designed, categorizing alerts into four levels according to the severity and impact: Information, Warning, Error, and Disaster. Each level has clear criteria and handling procedures to ensure the timeliness and effectiveness of the alerts.

Here is an example of how the alarm mechanism works for monitoring server CPU utilization:

1. **Monitoring Item Setup:** Server CPU utilization.
2. **Threshold Settings:**
   - Information Level: CPU utilization exceeds 70%
   - Warning Level: CPU utilization exceeds 80%
   - Error Level: CPU utilization exceeds 90%
   - Disaster Level: CPU utilization exceeds 95%

In this setup, a monitoring item for server CPU utilization is configured. When the CPU utilization exceeds the set thresholds, Zabbix triggers alerts based on the corresponding levels. These thresholds are derived from a comprehensive evaluation of system performance and business needs and can be dynamically adjusted according to actual conditions.

3. **Alarm Notification Mechanism:** Different handling methods are adopted based on the alert level:

- Information Level: Log the event without sending notifications.
- Warning Level: Log the event and send alert notifications to system administrators.
- Error Level: Log the event, send alert notifications to system administrators and relevant technical staff, and require immediate action.
- Disaster Level: Log the event, send alert notifications to all relevant personnel, trigger the emergency response plan, and execute fault recovery procedures.

The system adopts differentiated alert handling strategies for different alert levels. For severe alerts (Error and Disaster), the system immediately notifies relevant personnel for handling. For minor alerts (Information and Warning), the system logs the events and sends moderate notifications to avoid alert storms.

Alert notifications can be sent through various channels such as SMS, email, and instant messaging tools to ensure timeliness and reachability. For example, for Disaster-level alerts, the system quickly notifies on-duty personnel via SMS and phone calls to initiate the emergency response plan.

**4.5.2 Alert Handling Process**

The alert handling process mainly includes the following steps:

1. **Alert Trigger:** For example, if CPU utilization exceeds the critical alert threshold (90%), the trigger is activated, and an alert is generated.
2. **Notify Relevant Personnel:** The system immediately notifies system administrators and relevant operations personnel via SMS or other means, e.g., "Error Alert! Server CPU utilization exceeds 90%, please address promptly!"
3. **Fault Handling:** Relevant personnel diagnose and address the fault based on the alert information and predefined procedures, such as checking for abnormal processes consuming CPU resources and attempting to restart affected services.
4. **Tracking and Verification:** After fault handling, personnel track and verify that the issue is resolved and the system has returned to normal operation.
5. **Alert Clearance:** When the monitoring item returns to normal range, the alert is automatically cleared. For instance, when server CPU utilization drops below 85%, the alert is cleared.
6. **Summary and Optimization:** Analyze and summarize the causes of major alert events and develop targeted optimization plans, such as resource expansion and parameter tuning, to prevent similar issues from recurring.

Through the above alert handling process, system faults can be quickly detected and located, and effective measures can be promptly taken to minimize the impact on business operations. Additionally, continuous tracking and optimization enhance system stability and reliability.

We have also established comprehensive on-duty and emergency response mechanisms to ensure that major alerts are properly handled promptly. Detailed duty plans and schedules are developed, and regular emergency drills are conducted to improve the fault handling capabilities and coordination level of operations personnel.

Furthermore, regular statistics and analysis of alert data, including the number, types, frequencies, and handling efficiency of alerts, are conducted to evaluate the performance of the monitoring system and provide data

support for subsequent optimization and adjustments. Continuous data analysis and feedback optimization enhance the accuracy and effectiveness of the monitoring system.

## 5. Conclusion

This paper addresses the urgent needs for building a smart campus and proposes a network monitoring system based on Zabbix, TiDB, and Grafana, overcoming the limitations of traditional campus network monitoring systems. The system features the following innovations and characteristics:

1. **Comprehensive Monitoring System:** A three-dimensional monitoring system covering the access layer, aggregation layer, and core layer was built. It enables comprehensive awareness and centralized management of various ICT resources within the campus network, especially showing significant results in access layer monitoring and network experience optimization.
2. **Introduction of TiDB:** TiDB, a time-series database, was innovatively introduced as the monitoring data storage engine. This effectively resolves the storage and real-time computation bottlenecks of massive monitoring data, achieving second-level multi-dimensional analysis of millions of monitoring metrics.
3. **Integration of Zabbix and Grafana:** The integration of Zabbix and Grafana capabilities achieved intelligent diagnosis, tracing, and automated handling of network faults, significantly improving the efficiency of detecting, locating, and addressing campus network issues.
4. **"Monitoring as a Service" Model:** A new network monitoring service model called "Monitoring as a Service" was pioneered. By opening various monitoring service functions, it allows faculty and students to conveniently participate in network monitoring and optimization processes, enhancing the quality of network services and user experience.

The research results of this paper provide new ideas and methods for the field of smart campus network monitoring and are of great value in promoting network management reform and improving network service quality in higher education institutions. However, we also recognize that to meet the future development needs of smart campus networks, further improvements and enhancements are needed in areas such as comprehensive awareness, dynamic optimization, and intelligent operation and maintenance.

In the future, we will continue to focus on improving the automation and intelligence levels of the monitoring system. On one hand, we will explore intelligent operation and maintenance and big data analysis technologies to achieve automatic detection, intelligent location, and prediction of network anomalies. On the other hand, we will deepen the capabilities of intelligent diagnosis and tracing of network faults, driving the transformation of campus network management from passive response to proactive optimization. Only by doing so can we build a solid foundation for smart campus network governance, supporting the educational foundation with the strength of a powerful network nation.

## References:

[1] Wang Jian, Li Kangkang, Yang Xianmin. Exploration of New Generation Network Architecture Model for Smart Campus in Universities [J]. China Educational Informationization, 2023, 29(2): 93-100.

[2] Xu Shibo, Zhang Lin, Guo Yanhong, et al. Design and Research of Comprehensive Network Operation and Maintenance Management Platform in the Context of Smart Campus [J]. Network Security Technology & Application, 2021(08): 98-101.

[3] Yin Wenhao. Research on the Construction of Smart Operation and Maintenance System for Universities in the New Situation [J]. Smart China, 2023(06): 81-82.

[4] Villegas-Ch W, Molina-Enriquez J, Chicaiza-Tamayo C, Ortiz-Garcés I, Luján-Mora S. Application of a Big Data Framework for Data Monitoring on a Smart Campus. Sustainability. 2019; 11(20): 5552. https://doi.org/10.3390/su11205552

[5] Minea M, Dumitrescu CM, Minea VL. Intelligent Network Applications Monitoring and Diagnosis Employing Software Sensing and Machine Learning Solutions. Sensors. 2021; 21(15): 5036. https://doi.org/10.3390/s21155036

[6] Udo, Edward & Isong, Etebong & Nyoho, Emmanuel. (2020). Software Defined Networking Framework for Campus Network Management. https://www.researchgate.net/publication/350186945_Software_Defined_Networking_Framework_for_Campus_Network_Management

[7] Li, Nan & Xu, Xiaofei & Sun, Qi & Wu, Jie & Zhang, Qiao & Chi, Gangyi & I., Chih-Lin & Sprecher, Nurit. (2023). Transforming the 5G RAN With Innovation: The Confluence of Cloud Native and Intelligence. IEEE Access. PP. 1-1. 10.1109/ACCESS.2023.3234493. https://www.researchgate.net/publication/366912463_Transforming_the_5G_RAN_with_Innovation_The_Confluence_of_Cloud_Native_and_Intelligence

[8] Du Zhiguo. Building a Smart Campus Oriented to Serving Teachers and Students at South China Agricultural University [J]. China Educational Network, 2023(06): 41-44.

[9] Sun, Long & Li, Yan & Memon, Raheel. (2017). An open IoT framework based on microservices architecture. China Communications. 14. 154-162. 10.1109/CC.2017.7868163. https://www.researchgate.net/publication/314201600_An_open_IoT_framework_based_on_microservices_architecture

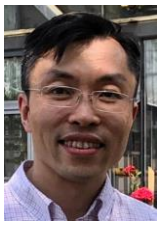
[10] Zhao Zhe, Tan Haibo, Zhao He, Wang Weidong, Li Xiaofeng. Network Monitoring System Based on Zabbix [J]. Computer Technology and Development, 2018, 28(01): 144-149.

[11] Xie Chaoqun. Research on the Construction of Operation and Maintenance Monitoring Platform for University Data Centers Based on Zabbix [J]. Journal of Changchun University, 2018, 28(12): 44-47.

[12] Huang Huachao, Xu Chuan. TiDB: A Highly MySQL-Compatible Distributed HTAP Database [J/OL]. Big Data, 2021, 7(3): 130-143.

[13] Zheng Hang, Zhang Duo, Wang Yuanyuan, Li Xiang, Wu Xiaomin. Application of Grafana in Web System Monitoring [J]. Electronic Technology & Software Engineering, 2019(22): 161-162.

## ABOUT THE AUTHOR



Fangming Guo was born in Guizhou, China in 1974. He obtained a Ph.D. degree from Huazhong University of Science and Technology in China. He is currently working at the Network Information Center of Wuhan University of Technology. His main research interests include systems integration, network management, network security, and machine learning.

E-mail: yangjie.xit.cs@gmail.com

Caijun Chen was born in Henan, China in 1970. He obtained a master's degree from Wuhan University of Technology in China. He is currently working at the Network Information Center of Wuhan University of Technology. His main research interests include digitalization of education, information governance, and related areas.

E-mail: ccj_nic@163.com

Ke Li was born in Wuhan, China in 1979. He obtained a Ph.D. degree from Wuhan University in China. He is currently working in the Information Management Department at Zhongnan University of Economics and Law. His main research interests include network operations and maintenance, big data processing, network security, and related areas.

E-mail:like@zuel.edu.cn