Journal of Computer Science and Frontier Technologies
ISSN Print: 3104-4204
ISSN Online: 3104-4212
CD ISSN: 3104-4220
https://doi.org/10.63313/JCSFT.2001

Design of Deep Service Awareness and Analysis System for International Education Park Network

Hongyan Luo
School of Integrated Circuits and Communication, Suzhou Vocational Institute of Industrial Technology, Suzhou 215104, China

How to cite this paper: Luo, H. (2025). Design of Deep Service Awareness and Analysis System for International Education Park Network. Journal of Computer Science and Frontier Technologies, 1(2), 11-17. ISSN Print: 3104-4204; ISSN Online: 3104-4212.
https://doi.org/10.63313/JCSFT.2001
Published: 2025-10-16

Abstract

Given the characteristics of the International Education Park network, such as a large user scale, complex services, and high quality requirements, this project aims to achieve a "visible, manageable, controllable, and trustworthy" network. It plans to build a centralized-distributed data storage and sharing system, collaborate with CDN/Cache to optimize resource scheduling, and construct a full-process security monitoring and big data performance management platform to meet eight core functional requirements, including multi-dimensional visualization, resource analysis, and quality evaluation. By comparing IP Account, Flow, and DPI/DFI technologies, DPI/DFI is selected as the core technology. A four-layer architecture (Application Layer, Sharing Layer, Decoding Layer, and Collection Layer) is designed, and its technical maturity, industrial chain completeness, and deployment feasibility are analyzed. The equipment deployment and interface design schemes are clarified to provide support for the digital transformation and efficient operation of the Education Park network.

Keywords

Deep Service Awareness; DPI/DFI Technology; Four-Layer System Architecture; Network Security Monitoring

1. Project Overview

As a core educational scenario gathering universities, colleges, faculty and students, the International Education Park network carries diversified services including teaching and research, daily life of faculty and students, and management services—such as online courses, academic resource access, cloud laboratories, campus office systems, and video conferences. It features a large user scale, complex service types, and high requirements for network stability and quality. Establishing a deep service awareness and analysis system to achieve a "visible, manageable, controllable, and trustworthy" network is not only an inevitable choice to address the current pain points in network management, but also a core measure to support the digital transformation of the Education Park and improve service quality and operational

efficiency.

Starting from the network construction and management needs of the International Education Park, this project intends to build a centralized-distributed integrated data storage and sharing system. It will optimize content distribution strategies through refined resource analysis, deepen the intelligent analysis of Internet resources, and collaborate with CDN/Cache to achieve efficient scheduling. Centering on the requirements of security compliance and risk controllability, a full-process security monitoring platform covering attack protection, content management, and audit traceability will be constructed; meanwhile, a big data-driven performance management platform will also be built to realize the full-process security monitoring of network data, thereby providing decision support for different roles such as operation and maintenance personnel, operators, and decision-makers.

2. Functional Requirements

To meet the operation requirements of the International Education Park network and support the efficient development of core services such as teaching and research, as well as faculty and student services, the system needs to be equipped with the following eight overall functions. These functions cover full-scenario needs including basic management and control, data presentation, resource optimization, and security protection:

1) Basic Functions

It can accurately identify network protocols and service types, conduct traffic control and scheduling as well as feature marking, block non-compliant content in real time, intelligently divert traffic to optimal nodes, and support traffic mirroring for analysis and auditing.

2)Multi-Dimensional Visualization Presentation Function

From the user dimension, it displays access distribution and behaviors; from the link dimension, it presents load and quality; from the service dimension, it shows type proportion and trends; and from the traffic direction dimension, it presents interaction rankings. This function intuitively displays the network status.

3)Internet Resource Analysis Function

It analyzes the popularity and distribution of resources, evaluates access efficiency and costs, conducts special optimization for key resources, collaborates with CDN/Cache to improve distribution efficiency, and realizes intelligent resource scheduling.

4) Internet Quality Evaluation, Analysis and Monitoring Function

It monitors user experience through active and passive methods, evaluates network indicators such as latency and jitter, analyzes the quality of services (e.g., websites, games), and monitors DNS resolution efficiency in real time.

5) Green Security Monitoring Function

It detects and blocks abnormal attacks and harmful information, records security

incidents for auditing, conducts compliant management of IDC/ISP information, and ensures the green and secure operation of the network.

6) Data Sharing Function

It opens interfaces for raw packets, session data and statistical data, supports permission-based data sharing, meets the collaborative analysis needs of multiple systems, and realizes efficient data reuse.

7) Service Management and Control Function

It manages and controls P2P and abnormal traffic, identifies and restricts the "one-to-N" non-compliant behavior, supports custom traffic rules, and precisely regulates the bandwidth and access permissions of various services.

8) Traffic Billing and Allocation

Based on traffic data from interconnection and network access, it conducts statistics in accordance with protocols and rules, realizes accurate calculation and allocation of costs among multiple entities, and supports fair billing.

3. Core Technologies

Considering that the main requirement of the deep service awareness system for the International Education Park network is to provide decision support for the configuration of network egress interconnection links. The system needs to analyze the traffic volume and direction of the network egress to understand the access of internal network users to other external networks, identify application hotspots, and reduce settlement costs. In addition, the system is required to analyze the types of network service traffic to guarantee high-value service traffic and provide value-added services. It also needs to conduct user behavior analysis and establish user portraits to provide basic data for big data applications. Furthermore, the system should be equipped with security protection capabilities to enhance network robustness, comply with laws and regulations, and provide users with a healthy internet environment. Therefore, when constructing this traffic collection and analysis system, the mainstream technologies to be adopted include the IP Account-based method, Flow-based method, and DPI/DFI-based method. The main characteristics of these three mainstream technologies are detailed in Table 1.

Table 1. List of Characteristics of Three Mainstream Technologies

Traffic Collection and Analysis Technology	IP Accounting Method	Flow-based Method	DPI/DFI-based Method
Traffic Collection Granularity	Single Packet	Data Flow	Single Packet/Flow
Traffic Collection Accuracy	Only counts the traffic passing through the router	The lower the sampling rate, the higher the accuracy	Accurately identifies service flows and application types
Implemented Functions	Traffic collection and partial traffic flow direction analysis functions	Traffic collection and partial traffic flow direction analysis functions Full traffic flow direction collection and analysis	Traffic collection and partial traffic flow direction analysis functions Full traffic flow direction collection and analysis
Implementation Difficulty	Requires the router to enable the IP Accounting function and access statistical values via the SNMP protocol. No new hardware devices are added, but the configuration is complex	When high precision is required, corresponding function boards need to be configured on the router, and the implementation is relatively complex Needs to deploy DPI/DFI systems in the existing network, and the implementation is complex	When high precision is required, corresponding function boards need to be configured on the router, and the implementation is relatively complex Needs to deploy DPI/DFI systems in the existing network, and the implementation is complex
Applicable Scenarios	Suitable for small-traffic billing scenarios	Suitable for traffic flow direction analysis scenarios Wide range of applicable scenarios, full-traffic collection billing, application layer analysis	Suitable for traffic flow direction analysis scenarios Wide range of applicable scenarios, full-traffic collection billing, application layer analysis

Through the comparative analysis of the above technical characteristics, it can be concluded that the IP Accounting-based method and the Flow-based method can only meet the functions of traffic collection and partial traffic direction analysis, and do not perform in-depth detection of packet content information for the collected traffic. Therefore, considering the actual requirements of this project design, the DPI/DFI-based method is intended to be adopted for the system design.

4. System Architecture Design

The design of the system’s data processing and application system mainly includes a four-layer core architecture. Each layer has a clear division of responsibilities and collaborates interactively to jointly support the efficient end-to-end operation of network data from collection to application. Its specific functions are as follows:

1)Application Layer: It covers various application systems such as network management, service management, and user management. Through standardized interfaces, it queries and subscribes to required data from the Sharing Layer, supports services like network optimization, planning, and design, and meets diverse data application needs.

2)Sharing Layer: It stores and queries log data, and provides real-time/near-real-time sharing services. It supplies raw data to the Application Layer via flexible interfaces and is also equipped with a log reporting gateway to support log data subscription by more application systems, facilitating data reuse.

3)Decoding Layer: It receives single-interface log file data reported by the Collection Layer, generates target log files through processes including analysis, correlation, supplementation of key information, and synthesis, and outputs them to the Sharing Layer, laying a foundation for subsequent data applications.

4) Collection Layer: It accesses and collects raw data from the live network, completes data parsing and accurate DPI service identification, and simultaneously performs XDR synthesis and generation of corresponding raw code streams to provide high-quality data input for the Decoding Layer.

The system architecture design is shown in Figure 1.

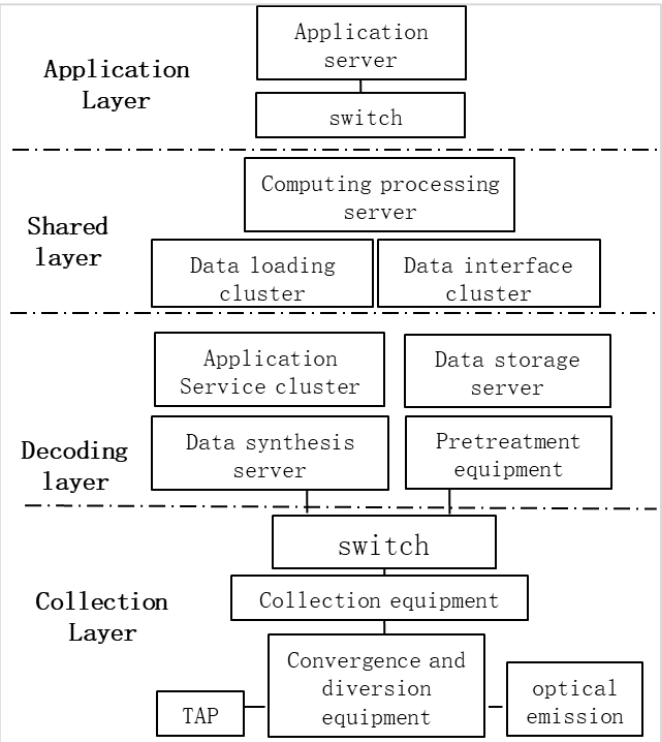

Figure 1. System Architecture Diagram

5. System Function Implementation

1)Feasibility Analysis

Traffic collection and analysis based on DPI/DFI technology through packet-by-packet parsing and pattern matching, the DPI/DFI-based traffic collection and analysis method can accurately identify specific application types and protocols in traffic, conduct in-depth analysis of traffic behaviors, and complete application classification. As new protocols and emerging applications emerge, this method enables dynamic updates to the backend application database, supporting full-scenario functions such as multi-dimensional visualization of network-wide traffic, Internet resource analysis, quality evaluation and monitoring, green security protection, data sharing, service management and control, and traffic billing and allocation.

Current application practice of DPI/DFI technology at present, telecommunications operators have deployed DPI/DFI-based traffic collection and analysis systems on a large scale at core nodes of broadband networks. These systems can realize functions including network-wide traffic visualization, Internet resource analysis, quality evaluation and monitoring, green security protection, data sharing, service man-

agement and control, and traffic billing and allocation. From a practical perspective, both the application maturity of DPI/DFI technology and the operational experience accumulated by operators are sufficient to meet the deployment requirements of this project.

Industrial Chain and Compatibility of DPI/DFI systems in addition, the industrial chain layout of DPI/DFI systems—covering upstream and downstream sectors such as chips, general-purpose servers, dedicated equipment, software development, network equipment, and storage equipment—has been highly improved, with a sufficient number of participating manufacturers. These systems have been deployed and applied on a large scale in multiple scenarios, including telecommunications operator networks and enterprise networks. Meanwhile, the system interfaces are continuously enriched, enabling effective connection with big data analysis platforms, traffic billing systems, content billing systems, log retention systems, as well as CDN, Cache, and various value-added service application systems, thus featuring excellent compatibility and scalability.

2)System Deployment

As the front-end component of the system, collection devices are deployed in the network architecture in series or parallel mode. Based on preset configuration rules, these devices can conduct in-depth detection and real-time parsing of network traffic and application protocols, and transmit the analyzed and processed data to the back-end data analysis and application support system, thereby providing data support for comprehensive analysis in dimensions such as users, services, and traffic.

The system interfaces are divided into two categories: external and internal. External interfaces are responsible for connecting with systems such as log retention, network management, traffic billing, CDN, and Cache. Internal interfaces link front-end collection devices with the back-end data processing platform, undertaking the transmission of service management strategies and analysis results, including data information and control information. The data processing platform acquires and stores the analyzed source data from collection devices, completes the analysis of full-service data, user behaviors, and security information through preset functional modules, and outputs service statistics, user application preferences, as well as displays and reports related to specified application traffic management and illegal user detection.

The devices can be deployed in series. Although this mode has higher requirements for DPI device capabilities, it offers strong control capabilities. For traffic collection, if the priority is analysis, one-way upstream traffic monitoring can meet the functional requirements; if equal emphasis is placed on analysis and control, two-way upstream and downstream traffic monitoring is required. The system requires 100% link coverage for all network links. The core network interfaces need to collect full traffic as the basic data for billing and settlement. Since bidirectional incoming and

outgoing traffic is involved, the traffic billing functional module requires 100% bi-directional link coverage.

Considering the deployment scope of the International Education Park network, its traffic collection and analysis system includes front-end collection and analysis devices and data processing platform devices. In addition, the traffic collection and analysis system at the data center egress is required to support the corresponding capabilities of the IDC/ISP information security management and analysis system.

6. Integration Requirements and Core Value of the Project

The system architecture of this project requires the integration of DPI and the IDC/ISP information security system, with the IDC/ISP information security management serving as a functional module of the DPI system. Whether more actual live network cases can be collected in the early stage to support the deployment and implementation of the project remains to be verified through more extensive research.

The functional requirements of the entire system are highly comprehensive. According to the data from the early technical research, mainstream manufacturers in the industry can basically provide support for the eight functional modules of the project architecture. However, a small number of functions—such as user perception—have been rarely applied in fixed networks in the past, and the reliability of the equipment functions requires further verification.

The core value of establishing a deep service awareness and analysis system for the International Education Park network does not lie in technical upgrading, but in transforming the traditional basic network that only bears traffic into an intelligent platform supporting education and scientific research through a closed loop of "service awareness → data analysis → decision optimization".

Therefore, the practical significance of this project's implementation will ultimately be reflected in the following aspects: improving the quality of teaching and scientific research, reducing operating costs, ensuring security and compliance, supporting digital decision-making, realizing the transformation of the network from passive operation and maintenance to active service, providing solid network support for the high-quality development of the International Education Park, and achieving a key leap from a basic network to an intelligent education support platform.

References

[1] WangXin,ZhangXiaojun.Enabling Anonymous Authorized Auditing over Keyword-Based Searchable Ciphertexts in Cloud Storage Systems [J].IEEE Transactions on Service Computing,2023,16 (6):10252041.

[2] ZhangHaiyang，ZhangXiaojun.Blockchain-based proxy-oriented data integrity checking mechanism in cloud-assisted intelligent transportation systems [J].IEEE Transactions On Intelligent Transportation Systems,2024,25 (10):10618924.

[3] Shi Meilin, Li Juanzi, Niu Zhisheng, et al. Design and Implementation of a Flow-based IP Billing System [J]. Computer Engineering and Applications, 2000, 36(8): 123-124, 128.