ATLANTIS PRESS
Advances in Social Science, Education and Humanities Research, volume 350
International Conference on Advanced Education Research and Modern Teaching (AERMT 2019)

The Construction Thought of DNS System under the Background of Education Informatization

Liang Zhao
Jilin Institute of Chemical Technology
Jilin City, Jilin Province, China

***Abstract*—The degree of information construction in colleges and universities is an important criterion for educational reform and innovation. Under such an information background, how to build a safe and efficient DNS system has become a key point. From the technical point of view of the security and reliability of domain name system, this paper puts forward the design idea of DNS system which is more in line with the current level of education informatization construction. Multi-DNS deployment, internal and external network separation, static or dynamic adjustment of analytical results, and application-level disaster recovery technology are important components of this design idea. The work draws experience from the application of traditional domain name technology in colleges and universities, and innovates construction ideas.**

***Keywords*—Education Informatization; DNS System; Network Security; Internet; Disaster Recovery**

I. BACKGROUND OF DNS SYSTEM CONSTRUCTION

China's economic and social development is very fast, which can not be separated from the support of information-based talents in the new era. Only more advanced educational concepts can provide sufficient talent support for China's socialist modernization. In order to achieve this goal, we must deepen educational reform and gradually establish a new educational system to meet the needs of economic and social development and modernization in the 21st century. Among them, education informationization, with the comprehensive application of information technology in the field of education as the core, provides favorable opportunities and conditions for promoting the reform and development of education.

Information network is an important part of the construction of educational informatization, and also the material basis and prerequisite for the realization of educational informatization. At present, China Education and Research Network (CERNET) and China Satellite Broadband Distance Education Network, which have been built and launched in our country, are all important contents of information network infrastructure construction in education informatization. The construction of these infrastructures not only lays a foundation for the informationization of education in China, but also creates conditions for the implementation of informationization education.

Since 2012, policies in the field of education informatization have been promulgated. The Ten-Year Development Plan of Education Informatization (2011-2020) in March 2012 provides guidance and general direction for the construction of education informatization in the next 10 years. In April 2012, Liu Yandong's teleconference on national education informationization determined the development orientation of "Three links and two platforms" for education informationization.

With the implementation of educational informationization, colleges and universities rely more and more on information systems. Once it can not be used, there will be many problems in daily teaching, office and even life, so the high availability of information systems is also put forward higher and higher requirements. The guarantee of high availability of information system needs to be strengthened and strengthened from many aspects such as application system, network, security and so on. The design of availability guarantee is carried out in every link to support the normal operation of information system.

II. THE CONSTRUCTION DEMAND OF DNS SYSTEM UNDER THE BACKGROUND OF EDUCATION INFORMATIZATION

When using various information systems, from the user client to the application system in the chain access link, at the application system level, there are cluster, application load balancing and other technical means to improve the availability of the application system. Network and security devices can enhance their availability through link redundancy and device virtualization.

However, the reliability of network services has not been paid attention to. This also makes it an obvious weak link. In order to be easy to use, the application system usually publishes by domain name. When users access the business system, they first need to parse the domain name and obtain its corresponding IP address for accessing through the network. The service of resolving domain name into IP address is domain name resolving service, commonly referred to as DNS.

A. High Reliability of Domain Name System

In the 1980s, DNS protocol came into being. Due to the limitation of computer performance and network bandwidth at that time, DNS was designed as a large global system with layered and distributed deployment. Each layer was responsible for maintaining the root domain, the top domain, the second domain and so on. However, since the birth of DNS protocol, domain name resolution function has always been the focus of construction. In terms of reliability, it only depends on the way of synchronization between primary and secondary, let alone the lack of its security function running on UDP protocol.

Copyright © 2019, the Authors. Published by Atlantis Press.
This is an open access article under the CC BY-NC license (http://creativecommons.org/licenses/by-nc/4.0/).

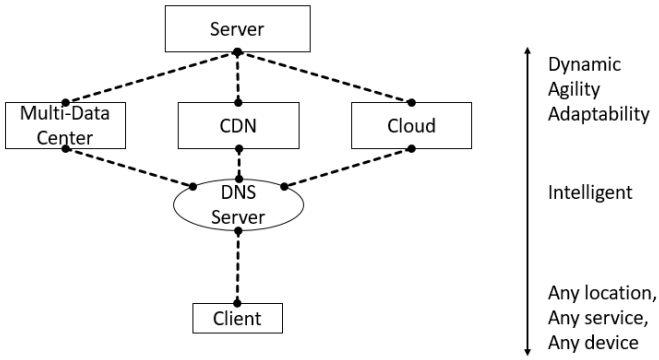

Fig. 1. Characteristics of DNS System

Nowadays, with the highly developed information technology, the reliability of domain name system is not enough to meet the needs of high availability and high security of information system. As can be seen from Fig.1, in today's highly informationized application which is issued by domain name, the domain name system can actually be regarded as the gateway to the Internet. Therefore, the availability of domain name system directly affects the availability of information systems. Many of the network failures and application failures in our daily use are actually caused by the problems of domain name system. It is imperative to build a strong and reliable domain name system (DNS).

B. Security of Domain Name System

DNS protocol was born in the 1980s. Due to the performance and security awareness of computers at that time, DNS was designed as a global distributed + UDP transmission architecture, leaving many security risks. In recent years, network security threats emerge endlessly. DNS protocols with simple protocols and much vulnerability have become disaster areas, such as DNS hijacking, cache poisoning, DDos attacks and Serverfail attacks, which are all security threats against DNS. Once DNS has problems, data security is difficult to be guaranteed. How to strengthen the security of DNS system itself needs to be considered.

C. Multi-export Traffic Optimization Based on Domain Name System

Unlike foreign countries, China's Internet is composed of three major operators, education network, radio and television and many other operators, which are independent and interconnected. Because of the cost of traffic settlement, the bandwidth of interconnection between operators is far from enough to meet the demand. The speed of cross-network access and available bandwidth are very limited, and the experience is very poor. In order to provide better services for users, we often use self-built or rented CDN to build mirror resources in multiple operators'networks at the same time, and guide users of different operators' networks to access the corresponding resource mirror to ensure users'experience. Fig. 2 is its flow chart. Taking the Tencent video as an example, the user's network environment is identified by identifying the source IP when the user parses the domain name of Tencent video, and the user is guided to access the network image resources through the parsing results.

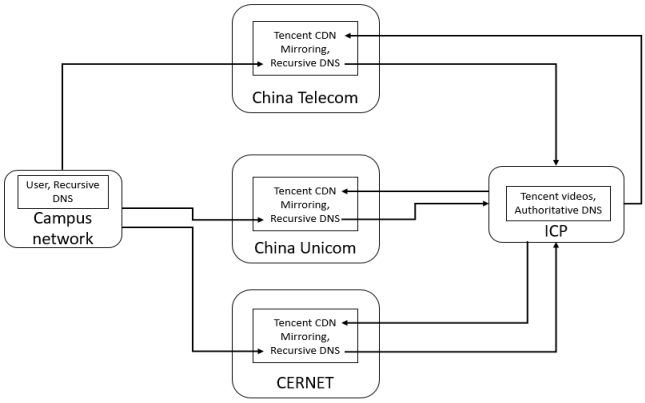

Fig. 2. Access mirror resources

Because universities need to use "edu.cn" domain name, they must access the education network as an Internet export. Considering the bandwidth and stability of the education network, we often choose the route of another or several operators as the Internet export. However, due to its own DNS or the use of public DNS, it is often impossible to use the bandwidth resources of multiple outlet lines at the same time, resulting in traffic concentrated on an Internet outlet line, resulting in idle resources and waste.

When using policy-based routing to boot, such as load balancing, it only solves the problem of idle bandwidth resources, and users'experience can not be guaranteed stably.

Therefore, we must consider the source of this problem, that is, DNS, to solve this problem, which means that the construction of DNS system needs to have the function of guiding users' Internet traffic through domain name resolution service.

D. Application Disaster Recovery Based on Domain Name System

The domain names of colleges and universities are all "edu.cn" suffixes, and the domain names of business systems (such as home page, VPN, enrollment, employment, etc.) are often all published on the public IP of the educational network, whose availability is restricted by the availability of the educational network lines. In the event of such incidents as the fire in the computer room of Beijing University of Posts and Telecommunications, the university business system will not be able to be used by users even though it is still in operation.

In addition, with the development of information technology in Colleges and universities, more and more business systems are online, and from the original chimney structure to a large number of business systems in horizontal series. Once a business system has problems, it may affect other businesses besides the business. Therefore, in the information construction, the requirements for disaster recovery will also change from data-level disaster recovery to application-level disaster recovery.

Nowadays, domain name technology is the most widely used technology route for disaster recovery in the financial industry with the fastest development of informationization. It realizes the overall application load and disaster preparedness through domain name resolution, which is also one of the construction requirements of DNS system under the background of educational informationization.

III. NEW THOUGHTS ON THE CONSTRUCTION OF DOMAIN NAME SYSTEM

With the further development of education informationization, besides the basic domain name resolution function, domain name system also needs to add such characteristics as outbound and inbound scheduling, intelligent resolution, security, reliability and easy operation and maintenance. Realize business experience optimization, automation, security and compliance, and provide data support for large data analysis of user behavior.

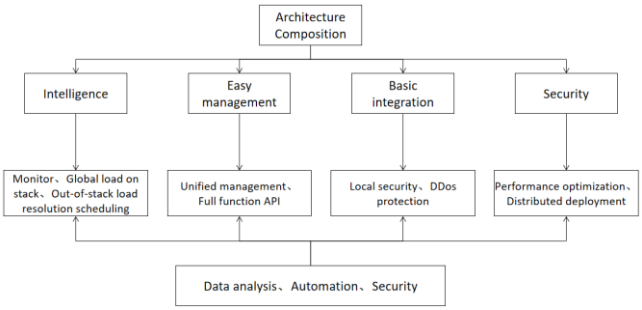

Fig. 3. New Domain Name System Function

As shown in Figure 3, the new domain name system should have the following functions to meet the needs of DNS in the context of educational informatization：

- High reliability
- Safety
- Optimal Guidance of Outward Flow
- Application-level disaster recovery based on the domain name

A. High-Reliability Design

Since the traditional primary and secondary modes no longer meet the availability requirements of DNS, deployment using primary and secondary modes and multi-active modes becomes a better choice. Following the principle of not putting eggs in one basket, deploying multiple DNS independently and ensuring data consistency can significantly improve the availability of the domain name system.

Considering the structure of the network, the master-standby mode is suitable for authoritative DNS deployment, while the multi-active mode is more suitable for recursive DNS deployment because it can use the same IP to provide services.

In order to ensure data consistency, when deploying multiple DNS, centralized management can be considered, that is, DNS in the network can be managed in a unified system without separate management, which can effectively reduce the risk of data inconsistency and reduce the pressure of administrators'operation and maintenance.

B. Safety design

In addition to the traditional technologies such as 0x20, random port, random ID, IP and domain name speed limit to deal with the cache poisoning and DDoS attacks on domain names, we should also change the architecture to realize the separation of internal and external networks, so as to avoid the vulnerable DNS system being exposed to the Internet without affecting the normal publication of authoritative domain names.

Traditional DNS is basically deployed based on open source software and Linux + Bind is the most widely used architecture. In this framework, in addition to the hidden dangers of DNS protocol itself, the vulnerability of open source software itself has become a disaster area. Once illegally controlled or tampered with data, such as the domain names of gambling websites or illegal overseas domain names, the impact is wide and nature will be very bad. Therefore, we can consider using DNS software with non-BIND architecture to provide authoritative DNS services. Internet publishing of authoritative domain names in schools uses cloud-based DNS services, and in-school publishing uses authoritative DNS servers deployed in schools to achieve the purpose of separating the internal and external networks of DNS. It can significantly improve the security of authoritative DNS (recursive DNS does not need to provide services to Internet users, and faces fewer security threats, which can be protected by traditional security technology).

C. Optimal Guidance Design of Outward Flow

In the case that universities generally have two or more Internet exports, it is necessary for DNS itself to have the ability of static or dynamic adjustment of the analytical results to optimize traffic guidance and enhance users'online experience based on domain name resolution. According to the pre-determined strategy, different analytic results are returned to different users, and users' traffic is guided to use different Internet outlet routes from the source to avoid the problems of traffic aggregation and experience decline.

Considering the network structure of universities and the factors of authentication and accounting, DNS system should have the following types of strategies, and support the combination of strategies to provide more choices to adapt to the different environments of schools and meet their needs.

- User grouping: Grouping according to user source IP corresponds to different outlet lines.
- Domain library: Use the built-in domain name library to group application types and correspond to different export routes.
- Time strategy: Traffic scheduling is carried out in different time periods.
- Bandwidth ratio: Flow guidance is automatically carried out according to the ratio of the bandwidth of the outlet line.

- Third-party linkage: Linkage with Internet export equipment to guide traffic according to bandwidth usage.
- Linkage with Internet export equipment to guide traffic according to bandwidth usage.

D. Application-level Disaster Recovery Design Based on Domain Name

If domain name technology is used for disaster recovery at the application level, besides physical facilities and application system architecture (from IP connection to domain name connection between servers), domain name system also needs to have application health detection and global application load function.

Applying health detection function can real-time detect the availability of distributed deployed application system servers. Once an exception is found, the server IP can be automatically shielded from the parsed results to ensure the availability of the returned results.

The global application load function can guide the inbound traffic of users or clients according to the strategy and health test results, and realize the disaster tolerance mode of backup, dual-activity and even multi-activity of the application system. When problems arise in the application system or data center, business can be switched to standby system or standby data center in time to deal with them, so as to minimize the duration of business failure and improve the availability of educational informatization system.

IV. CONCLUSION

As one of the important pillars of education information construction, the security of DNS system is the most important. The rising security of domain name system is of great significance to the security of the Internet system in Colleges and universities. This paper puts forward a new design idea for the construction of DNS system from the aspects of high reliability, security, optimal guidance of outgoing traffic and disaster recovery at the application level. It is of great help in leading the improvement of business value and IT capability, and also conducive to reducing the cost of university informatization construction and the risk of system operation. Based on the traditional DNS system, this paper lists some important system security issues to provide theoretical reference for the construction of DNS system under the background of education informationization.

REFERENCES

[1] Song Suxuan, Yang Xianmin, Song Ziqiang. Research on the Construction of the New Generation of Intelligent Campus Foundation Platform under the Background of Educational Informatization 2.0 [J]. Modern Educational Technology, 2019 (08): 18-24.(In Chinese)

[2] Yuan Pengpeng, Wang Changqing. Research on DNS Security Threats and Response Measures [J].Cyberspace Security, 2018, 9(05): 50-54. (In Chinese)

[3] Liu Quan. Research and Application of Internet DNS Oriented Optimization Technology [J]. Telecommunication Technology, 2017 (12): 48-52. (In Chinese)

[4] Hu Ning, Deng Wenping, Yao Su. Research status and challenges of Internet DNS security [J].Journal of Network and Information Security, 2017, 3(03): 13-21. (In Chinese)

[5] Sui Yi. Discussion on the Construction of Operational DNS Protection System [J]. Information Communication, 2015 (08): 215-216. (In Chinese)

[6] Zhang Rongrong. Design and prototype implementation of load balancing scheme for DNS system [D]. Beijing University of Posts and Telecommunications, 2011. (In Chinese)

[7] Wujiang, Feng Wen, Jiang Shaojie. Research and Implementation of Intelligent DNS System in Campus Network [J]. Microcomputer Information, 2010, 26 (09): 102-104. (In Chinese)

[8] Li Jingmei, Wu Peng. Design and Implementation of Intelligent DNS System [J]. Computer Engineering and Application, 2007 (11): 157-160. (In Chinese)

[9] Ren Mian. DNS Security and Protection [D]. Beijing University of Posts and Telecommunications, 2007. (In Chinese)

[10] Akamai Technologies Inc.; Patent Issued for Countering Security Threats with the Domain Name System (USPTO 9467461)[J]. Computer Weekly News, 2016.