

Research on Management Platform Construction of Users and Recourses Based on Multi-export Campus Network

Qi QI^{1, a}, Shan JING^{1, b, *}, Runyuan SUN^{1, c}, Bo YANG^{2, d}

¹ School of Information Science and Engineering, University of Jinan, Jinan, 250022, China

² Shandong Provincial Key Laboratory of Network Based Intelligent Computing, University of Jinan, Jinan, 250022, China

^aemail:qiqi@mail.ujn.edu.cn, ^bemail:jingshan@ujn.edu.cn, ^cemail:sunry@ujn.edu.cn, ^demail:yangbo@ujn.edu.cn

* Corresponding author

Keywords: multi-export; campus network; users and resources; management; proxy technology; policy based routing

Abstract. The campus network users have many kinds of types, and the network resource they access to is not certain. In order to improve the flexibility of the different needs for campus network users to access external resources, so campus network access multiple ISP network. This paper based on the multi-export campus network environment, according to analyze the characteristics of campus network users, network access requirement of the campus network and the network export resources, put forward the user and resource management platform by using proxy technology, policy base routing and NAT technology, and studies the manageability, security and reliability of the platform. The construction schemes of the platform provides a reference for other campus network.

Introduction

With the continuous development of the Internet, the major companies and universities gradually began to establish their own internal network. The internal network began to access multiple ISP [1]. The speed of access to resource which is very fast in same ISP, but the speed is greatly reduced by cross ISP access. This phenomenon is particularly prominent in many enterprises and universities [2].

Campus network is the most representative of internal network, it not only accesses to CERNET (China Education and Research Network), but also accesses to China Unicom, China Telecom and other ISP. Because the complexity of users in the campus, it is more practical to classify and manage users and network resources under the environment of multi-export. Therefore, this paper takes the campus network as the model to study.

Situation Analysis

With the development of information technology in universities, the types of campus network users are increasing, and the need to access the network resources is also expanding, many universities use CERNET and also access to the other ISP together. However, some problems still exist after the multi-line access. Which users access to the Internet through China Unicom? Which users access to the Internet through China Telecom? The users which default route is China Unicom want to access the resources of the CERNET, how to do? This problem is common in most of the multi-export campus network. Most of the campus network use proxy or set up the default route to solve the problem.

Proxy pattern: After the user has configured the corresponding agent, users' data packets will be sent to the proxy server and the proxy server will help users request network resources. Proxy server will usually have the function of cache resources. The requested resources will be cached in the local. When a user requests the resources which in the cache of proxy server, the proxy server

can send the buffer data directly to the user, which greatly improves the user's access speed. However, the proxy pattern is opaque to users. This increases the cost of access to network resources for users, and is not friendly enough for some application without support agent.

Set default route: Boundary device will select interface to send data packets according to pre-set policy based routing. When data packets arrive at the device, the packet will be matched with the routing policy. When data packets matched the routing policy, they will be sent out according to the corresponding rules. Other data packets will sent out by default routing interfaces. When the number of users is very large, the system resource utilization ratio of boundary equipment will grow rapidly. This is not conducive to the normal operation of the device and will affect the entire campus network.

Key Technology

NAT (Network Address Translation)

NAT technology can map the internal private IP address to external public IP address, and it can make users which use the internal IP address access to network resources, to reduce the consumption of public IP address [3]. On campus network, the size of the internal user is very large. If the public IP address directly allocated to users, it is not enough. Private IP address cannot be transmitted in the Internet, so it is required to use NAT technology in the internal network boundaries.

Proxy Technology

Proxy technology is a solutions accessing to the external network based on bypass mechanism, proxy servers simultaneously access both internal and external networks, default route of server's points to the external network. When users want to access Internet resources, local program is not directly access to the data provider, but do it by the proxy server, then the program accesses the data from the proxy server [4]. When there is the corresponding information in the buffer of the proxy server, the proxy server can directly echo the data to client. In this way, access speed is improved.

Policy based Routing

The traditional route is based on the destination address of IP packet in the forwarding of packets. The policy based routing is a more flexible forwarding mechanism. The groups could select a different path according to the source address, protocol type, or application type by using policy based [5]. If the IP packets and the relevant strategies of policy based routing match, data packet will be forwarded according to the specific next hop in policy based routing. If the match fails, data packet will be forwarded according to the traditional routing based on destination address. Policy based routing can be used to provide a more flexible routing approach for multi-export campus network.

User-Resource classification

There are many different needs of users in the campus network, some users may only need the resources under a certain ISP and they are not concerned about the speed of access to resources in other ISP. However some other users may need to access the resources in different ISP frequently. For CERNET users, when accessing CERNET resources, they may also need visit other network resources at the same time. In order to guarantee the universality of the research, this paper mainly discusses the situation of the campus network, which is connected with China Unicom, China Telecom and CERNET. Resources also include: China Unicom resources, China Telecom resources, CERNET resources, local resources and other resources.

In order to optimize the user's resource access efficiency, enhance user access to network resources, build a more secure and stable campus network. We must fully understand the characteristics and needs of the campus network users, classify users with the appropriate encoding, clear access authority to different types of users. Through the above analysis, we have designed the user resource classification table, as shown in Table 1. Among them, the Class code using tri-bit encoding. The first encoding said the default type of user access to ISP, with U, T, C respectively

represent China Unicom, China Telecom and CERNET. The second encoding said the payment status, with 0 representatives unpaid, 1 representatives have been paid. The third encoding said the user types, with 1 representatives of the office network users, 2 of the teachers' apartment users, 3 of the students' apartment users, and with 0 of all users.

Table 1 User-Resource classification table

ISP	Payment Status	User Type	Class Code	Network Resources
China Unicom	paid	office network users	U11	Internal network / Internet
China Unicom	paid	teachers' apartment users	U12	Internal network / Internet
China Unicom	paid	students' apartment users	U13	Internal network / Internet
China Telecom	paid	office network users	T11	Internal network / Internet
China Telecom	paid	teachers' apartment users	T12	Internal network / Internet
China Telecom	paid	students' apartment users	T13	Internal network / Internet
China Unicom	unpaid	all users.	U00	Internal network
China Telecom	unpaid	all users.	T00	Internal network
CERNET	unpaid	office network users	C01	Internal network / CERNET
CERNET	paid	office network users	C11	Internal network / Internet/ CERNET

Management Platform Construction of Users and Recourses

The management platform construction of user and recourses based on the analysis of the campus network users and export resources. Combining with the campus network multi export access strategy, reasonable dispatching the export resources, so that the campus network users can access to the variety of resources more secure and efficient.

Network Architecture

In order to make the users obtain the required resources more fast through the best path. The platform needs to set up the reasonable export strategy, according to the analysis of the user and the export resources. The campus network is mostly used in two-wire, three-wire or even five-wire access, including China Unicom, China telecom, China Mobile, CERNET, etc. Therefore, this paper uses the three-wire access network infrastructure, which is China Unicom, China telecom and CERNET, making this research more universal significance. The users and resources management model is shown in Figure 1.

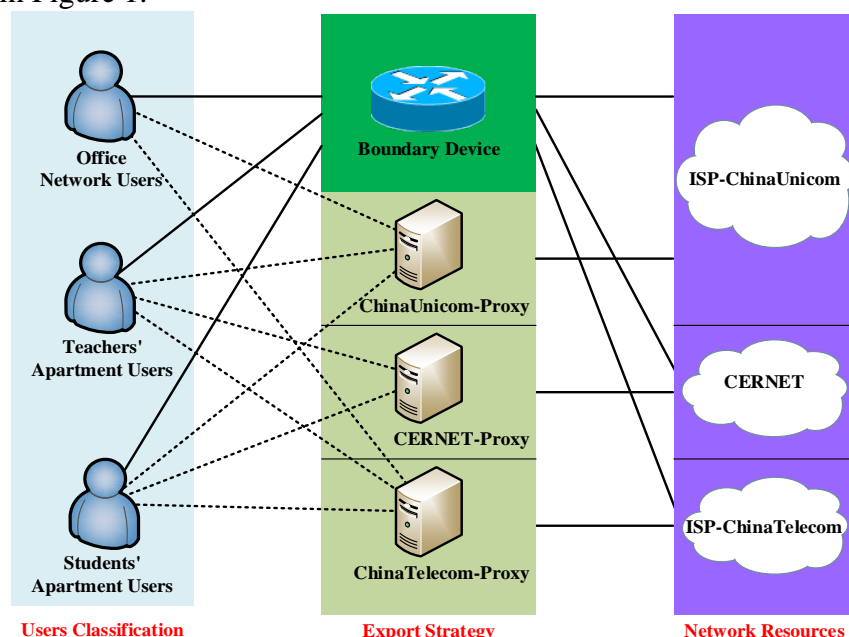


Figure 1 Users and resources management model

Taking into account the stability of the network, and to minimize the basic principle of network changes, this paper designed two sets of export strategies proxy mode and NAT mode, and they can be used in parallel. When using the proxy mode, the campus network needs to reserve the proxy server resources corresponding to different ISP. When accessing to network resources, the users need to configure the proxy server address in the local browser and access to different network resources by configuring different proxy addresses. This approach requires that the campus network users have a certain knowledge of the network and they can configure the corresponding proxy server address according to their own network access needs. In this mode, the users are only divided into two categories, which have already been paid and not paid. Network administrators can distinguish these two types of users through different VLAN and configure corresponding access control policy on the proxy server for different VLAN. These can achieve the payment users can access recourse and through the proxy server, unpaid users cannot access the Internet even if they configure the correctly proxy server address. In this mode, when the user is not configured any of the proxy, the CERNET users can access the education network resources and the internal resources of the campus network. Non education network users are only allowed to access the internal resources of the campus network.

In NAT mode, the user will not rely on the proxy server to access resources, but through the use of NAT technology on the network export device. Users can access the network resource without configuration, and adjust the default network exports according to their own needs. Administrators need configure the core of the campus network equipment and export equipment by the corresponding security control strategy, allowing the paid users to access the Internet and deny legitimate users access to the Internet. The unpaid users can only access the internal resources of the campus network. In this mode, the users' request data is analyzed by boundary device and get the information of the source, destination address and protocol type, and then match the routing policy. After a successful match the data will be sent to the suitable interface according to the corresponding strategy. Matching failures, the data will be sent by default routing. By default, the segment of data packages received from the China Telecom address will be sent from the China Telecom interface, received from China Unicom address will be sent from China Unicom interface. The matching unsuccessful packets will be sent through the default route.

Manageability

In the campus network, which has the complex export environment, the large user groups, kinds of users, how to allocate the resources reasonably and improve the access efficiency of different users to the network resources is a key problem to be considered by the network administrator. In this paper, we propose a network line selection platform based on multi-export by analyzing the types of users and the diffident export resources.

Users can adjust their default ISP by the platform. Legitimate users use the identification account login in the platform and adjust their default network exports. The process of campus network users apply to adjust the export line is as follows:

- ① Users login in the platform register (the first login) and submit the application for line switching.
- ② Network administrator login in platform to check the application information or the platform and push the relevant information to the administrator.
- ③ Administrator approval, and login the network equipment user's equipment uplink connected to, switch user's access port to the VLAN which represent network export resource of user request.
- ④ Administrator entering result in the platform.
- ⑤ Users login in the platform to see the application results or the platform push the relevant information to users.

Reference models are shown in Figure 2.

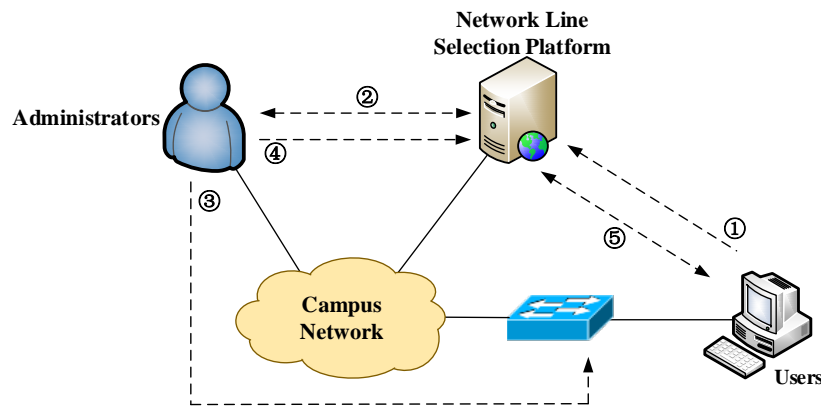


Figure 2 Schematic diagram of network line selection platform

Through this platform, the network administrators can more easily view all the user's network connection information, and switch their export line based on the user's resource access habits or user's initiative request to enhance the efficiency of user access to network resources.

Security

Security is a key factor to build users and resources management platform, this paper studies from two aspects of DHCP security and export security.

① DHCP Security. The network administrator can enable the DHCP Snooping function on the access layer device, filtering unsafe DHCP information by establishing and maintaining the DHCP Snooping binding table. In this way, users can obtain legitimate IP address, and avoid DHCP attacks. Individual, when a user connect the cable which should be connected to the WAN port to the LAN port, The other users in the same local network will not access to that route's invalid IP address.

② Export Security. When the user uses the proxy server to access the network resources, the user will send the request to the proxy server in fact, the proxy server help the user to obtain the corresponding resources, and then return the resources to the user. In this mode, the proxy server acts as a "middleman" role, users hide behind the proxy server. This can protect the user's privacy, and the proxy server can filter some unsafe network connection request, and to protect the user's network security. When the user uses the NAT mode, it is actually using the NAT function on the campus network boundary device, which realizes the transformation of the public IP address and internal private IP address or the IP address of the education network, and maintains a mapping relationship. This mode also allows the user to hide behind the boundary device, and to enhance the user's network access security.

Reliability

With the development of information technology, people increasingly rely on the variety of network resources provided by Internet. This requires that the campus network must have a strong fault-tolerant ability to ensure the normal operation of the network. When the proxy and NAT mode both in the campus network, network administrator can use the NAT mode as main way, and use the proxy mode as supplement.

When the boundary equipment failure, the users who use NAT approach to network may appear network connection failure. At this time, users can use the proxy mode reconnect to the Internet by configure the corresponding proxy server address. This can effectively avoid the network paralysis caused by the failure of individual equipment and enhance the stability and availability of the campus network.

Conclusion

This management platform based on the application needs of the multi-export campus network, and has a certain practical significance for the design and deployment of the general multi-export campus network solution. The program, integrated policy based routing, proxy technology and NAT technology, optimized the export strategy of campus network, realized the campus network data diversion, and made the campus network more security and reliability. Through the classification of users and resources, this paper propose a network line selection platform based on multi-export, which can enhance the flexibility of user access to the network resources. By this, campus network administrators can manage users more easily. The successful implementation of the project can provide effective reference for the construction of other multi-export campus network user management platform.

Acknowledgment

This work was supported by the Technology Development Program of Shandong Province (2011GGX10116), and the Next Generation of Internet Technology Research and Development, Industrialization and large scale commercial projects (CNGI-12-03-017).

References

- [1] Zhang Zhicheng, ZOU Renming, ZHANG Xiaoquan and ZHU Junjun, Design and Realization of Multi-Export Campus Network Based on Redundancy Architecture [J]. Computer Science, 2012, 39(10).219-222.
- [2] Wang Zirong, HU hao, YIN Shaofeng, WANG Yuke. Research of multi-homed network service deployment based on strategy DNS and HTTP Proxy [J]. Computer Engineering & Science, 2014, 36(2).238-243.
- [3] Zeng Chuanhuang, Hu Haonan. Analysis of the NAT-PT gateway [J]. 2012 International Conference on Computer Science and Service System, CSSS 2012, 2012.46-49.
- [4] Sysel Martin, Doleal Ondej. An educational HTTP proxy server [J]. Modern Trends and Techniques in Computer Science - 3rd Computer Science On-line Conference, CSOC 2014, 2014, 285(1).541-547.
- [5] Yang Lin, "Multi-output Configuration Based on Policy Routing in the Campus," Communications Technology, 2010, 43(06).123-125.