A Study on Campus Network Access and Export Management

Anli YAN[1,a], Shan JING[2,b,*], Qi QI [1,c] and Bin XIAO[3,d]

[1] School of Information Science and Engineering, University of Jinan, Jinan, 250022, P. R. China

[2] Shandong Provincial Key Laboratory of Network Based Intelligent Computing, University of Jinan, Jinan, 250022, P. R. China

[3] Information Network Center, University of Jinan, Jinan, 250022, P. R. China

[a] yan-anli@qq.com, [b] jingshan@ujn.edu.cn, [c] ise_qiqi@163.com, [d] nic_xiaob@ujn.edu.cn

* Corresponding author

Keywords: Campus Network, Network Access, Export Management, VLAN, DHCP, Network Security

Abstract. With the improving of the information construction of universities, universities' network construction scale becomes bigger and bigger, it generally has various types of users, multi-exports network, and internal and external network resources distribution and so on. In order to improve campus network management becomes efficient and simplified, we analyze the characteristics of campus network users, the network access requirements and on the basis of export network resources, combining with the characteristics of family residential user type, using the network of campus network by the VLAN and DHCP technology, applying a multiple routing technology export control with NAT technology and strategy, then putting forward the effective solutions to users under the security of network management.

Introduction

With the continuous development of the Internet, companies and universities are beginning to establish their own internal network, universities' network construction scale is becoming more and huger and the structure becomes intricate, the demand for the users' resources is getting diverse. At the same time, the network administrator to manage the remote of campus network also exist security threat. In order to adapt to the size of campus network is bigger, the structure of the network getting complex, the diversity of users demanding for resources, improving the efficient, simplified and secured of campus network management is particularly important.

Analysis of the situation

Universities that the scale of network is large, the structure is complex, and users demand for resources have become diversified, there are all kinds of difficulties that network administrators manage campus network. In university campus network, the entire campus network isn't have certain rules to divide VLAN that brought chaos to manage VLAN in campus network VLAN [1]. Due to the various types of users, and demand for resources is different, universities have adopted different methods to achieve more exports, but the widespread router access control list is huge and having problem about IP address aggregation [2]. Network administrators usually use Telnet to manage the remote equipment in campus network, Telnet is commonly used for terminal access protocol, because most of the latest operating system comes with a built-in Telnet client. But Telnet send all communications on the network in clear text, the attacker using network monitoring software can be read by sending keystroke between Telnet client and switches' Telnet service. So when using Telnet access network equipment, there exists a big danger hidden [3].

Key technology

Internal network by using VLAN and DHCP technology to realize the internal network interconnection and simplify the IP address assignment problem. One VLAN main goal is to limit broadcast of Ethernet's initial problems within a certain range, so as to improve the safety performance of local area network. Its advantage is to make a certain limit for broadcast, making the virtualization of the working party becomes easily to realize the dynamic management of the network [4]. DHCP services allow workstations connected to the network and automatically obtaining an IP address. For each network, server configured the DHCP service that can provide IP address and make subnet mask defaulted gateway, etc.[5].

The problem about network more export in the campus is that using NAT and policy routing technology, simplifying the complexity of exports. Using NAT technology can make the internal private address mapped to the external public address that make internal address be able to access the network resources, and to reduce the consumption of the public IP address[6]. Common problem is the size of the internal users are very big in the campus network. One of the few public address directly allocation to use is not enough. Private address can't transfer in the Internet which need to use NAT technology in internal network boundaries. Traditional routing is based on IP packet forwarding address for the purpose of the road. And policy routing can be the source address, protocol type, packet length, and application type by matching a variety of conditions, such as to determine to send the direction of the data [7]. If IP packets are match a set strategy, which will be according to the strategy to set the next-hop forward; if the match is not successful, then through the normal route forward.

Implementation plan

User IP address assignment. It’s convenient for the network administrator to manage and plan the campus network. The realization of IP address allocation efficiency and reduce the late maintenance costs of the network, it’s important to make reasonable user address coding and allocation scheme.

User address coding mainly contain: VLAN division and the division of naming rules, IP address, port information description of equipment, etc. In this paper, in the above several aspects to encode user address.

The division of VLAN and naming rules: a unit of a building are classified into four VLAN. In order to ensure the compatibility, the management VLAN uses VLAN99. The other VLAN is used to distinguish between the user's choices of Internet service providers. In order to facilitate the memory and management of network administrators, VLAN name code in the form of XXYZ, XX said floor, Y said user network services provide type, Z said the detached wing. For example, VLAN111 represents a unit 1 floor, user pay for Unicom. VLAN121 represents a unit 1 floor, user pay for Telecom. VLAN101 represents a unit 1 floor, user don’t pay for anyone.

The division of IP address blocks: the campus network address is divided into four pieces, 172.19.0.0/16、172.16.0.0/16、172.30.0.0/16 and 172.31.0.0/16. Management address block is 172.19.0.0/16, not payment address block is 172.16.0.0/16, Unicom payment address block is 172.30.0.0/16,Telecom payment address block is 172.31.0.0/16. This principle is mainly to the border router on the road by table design is convenient. Then, that IP address blocks are divided into class C address. Unifying the fourth byte is set to 251 as the gateway of VLAN. Information table for No.1 building is shown in table1.

Table 1 Information table For No.1 Building

Network address	VLAN Number	Annotation
172.16.1.0/24	101	A unit 1 floor only on internal network IP address of the block and VLAN
172.30.1.0/24	111	A unit 1 floor Unicom service IP address of the block and VLAN
172.31.1.0/24	121	A unit 1 floor Telecom service IP address of the block and VLAN

The description of the equipment port information: When the network is running, it will be have the phenomenon of the equipment port breakdown that need change equipment port. If there is no a reasonable port information description rules, it will appear the phenomenon of mixed and managed difficulty. Equipment port description rule is building number - unit number - port number. 11-1-0, for example, describe the information of the 11th floor of a unit, 0 port.

User's address assign mainly through static address allocation and dynamic address assignment. For servers, core routers and other important equipment or user use static address allocation. Ordinary users of campus network who use DHCP dynamically allocated to obtain IP address. This article mainly through the convergence layer multilayer switch Core use DHCP directly, Combined with the division of VLAN and DHCP pool Make different VLAN users get a different IP address, in this way to limit the user's behavior. The user who pay for Unicom that can obtain the IP address of the Unicom address block, the user who pay for Telecom that can obtain the IP address of the Telecom address block, the user who pay for nobody that can obtain the IP address only access to the internal network. Campus network of simple network topology is shown in figure 1.

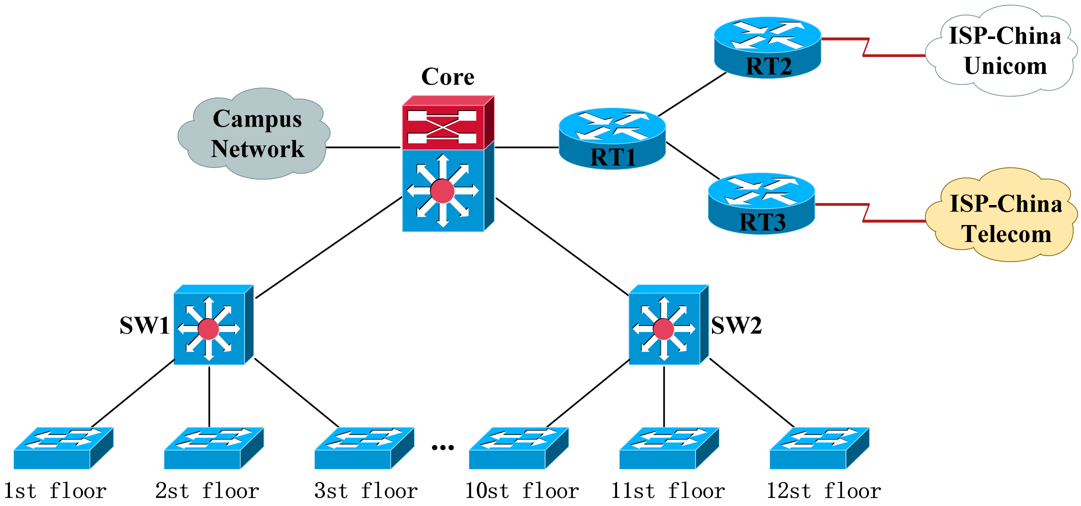

Figure 1 simple network topology

For example, using a building of a unit. Configuration information is shown in table 2.

Table 2 configuration information

DHCP pool	Network Address	gateway	VLAN Number
Campus	172.16.1.0/24	172.16.1.251	101
Unicom	172.30.1.0/24	172.30.1.251	111
Telecom	172.31.1.0/24	172.31.1.251	121

Many export control. The control of more export mainly use NAT and strategy routing in campus network, and packet forwarding path more performed by core routers, there are many problems, although this management way can guarantee the normal operation of the network. Not capture expends users access to internal users that they are not in the same VLAN in campus network, If the packet is also need through the core layer forward routing equipment, it’s undoubtedly that core router add workload and lead to run slow and packet delay. In this article, the core of the multilayer switch Core according to the destination IP address in the network packets in preliminary filter, Access to the campus network resources data directly jump forward to the corresponding next, and access external network packets sent to the core router RT1. RT1 accord to source IP address, confirming its for China Unicom or Telecom users. Who is Unicom user that will send packets to Unicom border router or who is Telecom user that will send packets to Telecom border router?

For not capture expends users in campus network, Its VLAN only access network resources within the campus, the user who pay for Unicom or Telecom that can access to the internal campus network resources and make NAT get public IP address to access external network.

Border router key code RT2 is as follow:

```
Router(config)#ip nat pool Unicom 124.133.254.0 netmask 255.255.255.192
Router(config)#access-list 1 permit 172.30.0.0 0.0.255.255
Router(config)#ip nat inside source list 1 pool Unicom overload
```

Border router key code RT3 is as follow:

```
Router(config)#ip nat pool Telecom  222.175.129.64  netmask 255.255.255.224
Router(config)#access-list 1 permit 172.31.0.0 0.0.255.255
Router(config)#ip nat inside source list 1 pool Telecom overload
```

The safety of the user management. In order to ensure the security of user management in campus network, this article mainly to the Console port, remote management protocol, switch port or interface, DHCP Snooping four aspects to realize the security of user management. Describing as follows:

Switches and routers configuration method usually have two ways: local Console login configuration and remote management. But at the first time, switches and routers configuration must use the Console line connected to the Console port, In order to prevent unauthorized person access device, it should configure passwords for the console and still need to encrypt the password. The reference command code (switch and router configuration code is same):

```
Router (config) # line console 0
Router (config-line) # password words
Router (config-line) # login
Router(config) # service password-encryption
```

Because Telnet is sent as plain text all communication on the Internet, The attacker use network monitoring software can be read each keystroke between Telnet client and Telnet service of switch. Use Telnet access network equipment when there is a big security threats .SSH into the switches for remote access device of choice for virtual terminal lines agreement. At present there are SSHv1 SSH and SSHv2 two versions, in this paper, the implementation of SSHv2, because it uses the stronger than SSHv1 security encryption algorithm and the VTY lines are password encryption. The reference command code:

```
Swtich(config)#ip domain-name ujn.edu.cn
Switch(config)# crypto key generate rsa
Switch(config)#username name secret words
Switch(config)#ip ssh version 2
Swtich(config)#line vty 0 15
Switch(config-line)#transport input ssh
Swtich(config-line)#login local
```

Before the deployment of access layer switches, should protect all switch port or interface, in this paper mainly from the port number of MAC address to protect switch port security. Switch port security to limit the number of valid MAC addresses allowed on port, the distribution of the secure MAC addresses for a port, When the port received packet source address, it is not defined in the group address, Port isn't forwarding these packets. If you limit the number of secure MAC addresses into one, And for the port defines a secure MAC addresses, only the address for the particular security MAC address of the workstation to successfully connect to the switch port, and the workstation will receive the full bandwidth of the port.

In the access layer devices enable DHCP Snooping function, Establish and maintain the DHCP Snooping binding table to filter distrust of DHCP messages. Use this function under the VLAN that can guarantee the user gain legal IP address and avoid being attacked by a DHCP. Specially, when user changes router's WAN port connect to a LAN port, it will not lead to a user gain invalid IP address from the domestic route in local area network. The reference command code:

```
Switch(config)#ip dhcp snooping
Switch(config)#ip dhcp snooping vlan 101， 111,121
```

The uplink switch port is set to trust port, to complete the switch to shield fake DHCP server, to ensure that the client from legitimate DHCP server to obtain IP address. The speed limit on port of the DHCP message and exceed the rate of interface will be shut down that can prevent illegal DHCP request packet radio attack. The reference command code:

```
Switch(config-if)#ip dhcp snooping limit rate 10
Switch(config-if)#ip dhcp snooping trust
```

Summary

Based on the internal network using the VLAN and DHCP technology, in many export control that combined with NAT routing technology and strategy, Optimizing the campus net management and export strategy, realizing the campus network data divide stream. Through reasonable user address coding and effective export control, Network administrators can more clearly understand of the campus network user type, Simplify the complexity of many export administration. At the user security management way, improve the port equipment security, Use reliable SSH protocol instead of Telnet to manage the campus network for remote, Enhanced the security of network management. In this paper, the implementation of the scheme and safety management in the university campus network with self-management ability, not only on the university campus network has the reference value, but also Ordinary residential area of network management have is practical significance of the specific reference.

Acknowledgements

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] LIU Hongyan, "*Application of VLAN technology in campus network*", Computer Era, Vol.2, No.1, pp.14-18, 2012.

[2] MA Liang, JIA Fei, "*Design and Development of IP Address Management System of Campus Network*", Computer & Network, Vol.4, No.23, pp.66-69, 2013.

[3] ZHANG Guofang, "Remote management of Linux based SSH protocol", Computer Security No12, 2014

[4] LIU Xiangdong, LI Zhijie, YAN Dejun, WANG Degao, "Design and Implementation of IEEE 802.1Q VLAN Principal Expeniments", Research and Exploration in Laboratory, Vol.30, No.4, pp.46-49, 2011.

[5] LI Shu, YAO Lei, "Implementing DHCP Service and Security Systems under Complicate Network Enviorment in Lab" Research and Exploration in Laboratory, Vol.30, No.1, pp.143-148, 2014.

[6] Zeng Chuanhuang, Hu Haonan. Analysis of the NAT-PT gateway [J]. 2012 International Conference on Computer Science and Service System, CSSS 2012, IEEE Computer Society, pp.46-49, 2012.

[7] YANG Lin, "Multi-output Configuration Based on Policy Routing in the Campus," Communications Technology, Vol.43, No.06, pp.123-125, June 2010.