TELKOMNIKA Indonesian Journal of Electrical Engineering
Vol.12, No.4, April 2014, pp. 3040 ~ 3045
DOI: http://dx.doi.org/10.11591/telkomnika.v12i4.4776

Based on the RADIUS and AAA Authentication of the Campus Networks Security System Design and Implementation

Yuyang Lu*[1], Xiang Zhang Chen[2], Wenjie Wang[3], Yong Yang[4]
School of Information Management Technology, College of Industrial Technology,
Xuzhou, Jiangsu, 221000, China
*Corresponding author, e-mail: luyy@mail.xzcit.cn[1], chenxz@mail.xzcit.cn[2], wangwj@mail.xzcit.cn[3], handanyangyong@126.com[4]

Abstract

As the work of digital campus construction, the function of network became more and more important. The kernel of digital campus is fast speed, function formidable, resource widely. The campus network is a special network, which face special user community, it is thought ,technology of active, and it adopt access layer access ,so the network security is lower, Vulnerable to illegal users and virus attacks. This text use RADIUS and AAA authentication technology in the campus, through user authentication, strengthen the network access restrictions, the log service, campus network management more systematic and safe.

Keywords: *AAA, RADIUS, network security, campus network*

Copyright © 2014 Institute of Advanced Engineering and Science. All rights reserved.

1. Introduction

Campus network (CN) is the comprehensive information service network for teachers and students teaching, researching. There are all different kinds person in campus in the net. So it is hard to avoid the hack by someone with net technology when connecting the net. If they enter into CN and modify the configuration of network equipment, the CN will be destroyed and paralysis. The paper makes the purpose of building safety CN by using Cisco AAA set the certification, award, billing safety function configuration.

Cisco AAA architecture has three independent safety function, which realizes the safety access control. The AAA safety model can control some user visiting the net recourse intelligently by using relevant award strategy and audit service condition. The comprehensive safety service can make the efficient net management and safety net visiting into together. Turning on the network equipment AAA function such as router can make the connection with the Cisco security service by these protocols.

Cisco AAA includes three basic contents: Authentication, Authorization, and Accounting. They are depended on each other. It can be authenticate without authorization and accounting, but it can not be authorized and accounted without authentication. The protocols in AAA authentication are RADIUS protocol, Tacacs protocol and HWTACACS protocol.

2. CN AAA Authentication Security Development

Next, through a section of net security setting of some college network topology proves AAA authentication system enhancing the net safety. We set the example as from college central apparatus room to dormitory. Among these central apparatus room arranges an AAA server, which is imitated by virtual machine with 2003 server operation system. And in the student dormitory, we use another common virtual imitating student client. The intermediate equipment is Cisco 3700 series router. In the right part student dormitory we use a router with switching module as dormitory floor switchboard (this can be simulated switchboard in GN33). The ISP internet can be simulated by a router named ISP in the Figure 1 the cloud means net in the Figure 1. AAA server adopts DAGIUS authentication. The switchboard adopts 802.1X authentication system. Figure 1 is the dynamic IP address distribution topology network.

Received September 10, 2013; Revised November 23, 2013; Accepted December 3, 2013

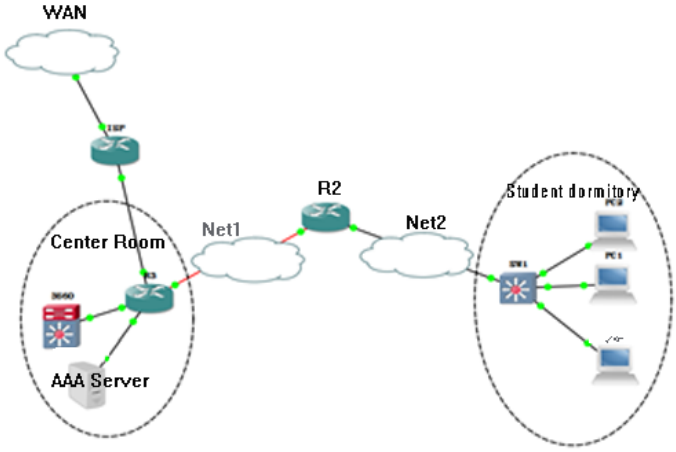

Figure 1. The Dynamic IP Address Distribution Topology

2.1. Network Equipment Related Configuration (Some Part)

SW1 configuration:

SW1(config)#hostname SW1 //Switch name:SW1

SW1(config)#enable password cisco

AAA configuration:

SW1(config)#aaa new-model //overall open AAA, the default condition is close.

SW1(config)#aaa authentication login default group radius local

SW1(config)#aaa authentication login LOCAL1 local //set login list's local enter name is "LOCAL1"

SW1(config)#aaa authentication login NOACS line none //offline protect, keep entering into router after login failture.

SW1(config)#aaa authentication dot1x default group radius local

SW1(config)#aaa authorization exec cisco group radius local

SW1(config)#aaa authorization network default group radius local //after authentication successfully, the authorized users by RADIUS can enter into the net.

SW1(config)#aaa accounting exec cisco start-stop group radius ///Accounting the exec mode users, recording the start and end time.

SW1(config)#aaa accounting commands 15 cisco start-stop group tacacs+

DHCP address pool configuration:

SW1(config)#ip dhcp excluded-address 10.10.10.1 10.10.10.5 /Except the address section 10.10.10.1 10.10.10.5 all the address are ready for reserve. Dividing the connecting users port into relevant VLAN:

SW1(config)#ip dhcp pool AAA

SW1(dhcp-config)#network 10.10.10.0 255.255.255.0

SW1(dhcp-config)#default-router 10.10.10.1

SW1(dhcp-config)#domain-name www.cisco.com

SW1(dhcp-config)#lease infinite

将连接用户的接口划入到相应的VLAN:

SW1(config)#interface FastEthernet1/0

SW1(config-if)# switchport access vlan 2

SW1(config-if)# spanning-tree portfast

SW1(config-if)#interface FastEthernet1/1

SW1(config-if)# switchport access vlan 2

SW1(config-if)# dot1x pae authenticator

SW1(config-if)# dot1x port-control auto

SW1(config-if)# spanning-tree portfast

SW1(config)#dot1x system-auth-control //open then dot1x authentication function overall

```
SW1(config)#vlan 2
SW1(config-vlan)#name AAA
SW1(config)#int vlan 2
SW1(config)#ip address 10.10.10.1 255.255.255.0
SW1(config)#router ospf 1          //use ospf
SW1(config-router)# router-id 1.1.1.1
SW1(config-router)# network 10.10.10.1 0.0.0.0 area 0
SW1(config)#line vty 0 4
SW1(config-line)# authorization exec cisco
SW1(config-line)# accounting commands 15 cisco
SW1(config-line)# accounting exec cisco
SW1(config-line)# login authentication LOCAL1
SW1(config)#line console 0
SW1(config-line)#login authentication NOACS
R2(config-if)#interface Serial1/0
R2(config-if)# ip address 12.1.1.2 255.255.255.0
R2(config-if)#no sh
R2(config)#interface FastEthernet0/0
R2(config-if)# ip address 10.10.10.2 255.255.255.0
R2(config-if)#no sh
R2(config)#router ospf 1
R2(config-router)# router-id 2.2.2.2
R2(config-router)# log-adjacency-changes
R2(config-router)# network 10.10.10.2 0.0.0.0 area 0
R2(config-router)# network 12.1.1.2 0.0.0.0 area 0
```

Use the same interface and OSPF protocol on the R3：

```
R3(config)#interface FastEthernet0/0
R3(config-if)# ip address 192.168.123.3 255.255.255.0
R3(config-if)#no sh
R3(config)#interface Serial1/1
R3(config-if)# ip address 12.1.1.1 255.255.255.0
R3(config-if)#no sh
R3(config-if)#router ospf 1
R3(config-if)#router-id 3.3.3.3
R3(config-if)#network 3.3.3.3 0.0.0.0 area 0
R3(config-if)#network 12.1.1.1 0.0.0.0 area 0
R3(config-if)#network 34.1.1.3 0.0.0.0 area 0
R3(config-if)#network 192.168.123.3 0.0.0.0 area 0
R3(config)# ip nat inside source list 100 interface Loopback0 overload
R3(config)#access-list 100 permit icmp any any
R3(config)#interface s1/1
R3(config-if)#ip nat inside
R3(config)#interface f3/0
R3(config-if)#ip nat outside
```

2.2. Sever-Side Configuration

(1) As Figure 2, create a count with name snc15 in ACS sever, then fill the username and password (user setup), where the user will be connected by switcher in future.

(2) As Figure 3, adding the AAA client-side and sever-side information (network configuration): AAA client IP address is the VLAN2's IP address among the switcher. Shared secret is the passwords of switcher setting passwords 'cisco'. Authenticate Using is RADIUS.

(3) As Figure 4, next step is setting the group authentication. After authenticating user can enter into net (Group Setup). In the option of IETF RADIUS Attributes choose all the selected option .Attention: 064 is the authentication only for the user under VLAN. 065 is the 802.1x authentication mode.081 sets as VLAN ID (here is VLAN 2). That is because the pre-plan for switcher authentication belongs to VLAN 2. After all these settings, click Submit+Restart.

(4) After all these above steps, we can test the defined name and passwords in

switcher whether can be authenticate completely. Figure 5 shows authentication completely. SW1#test aaa group radius snc15 cisco new-code

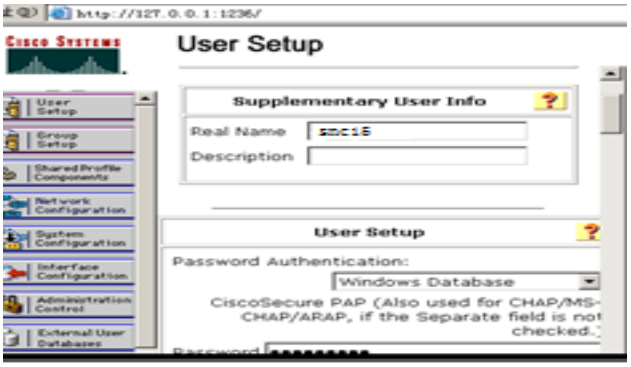

Figure 2. Add User

Figure 3. Adding Client-Side Information

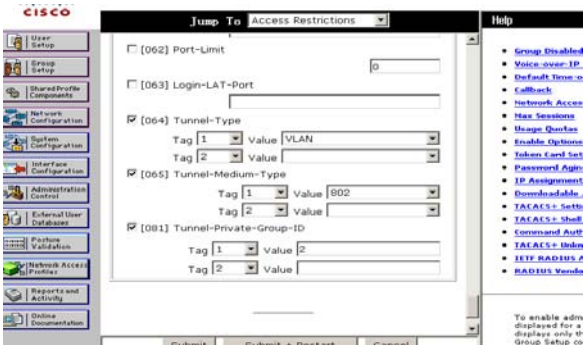

Figure 4. IETF RADIUS Attributes Setting

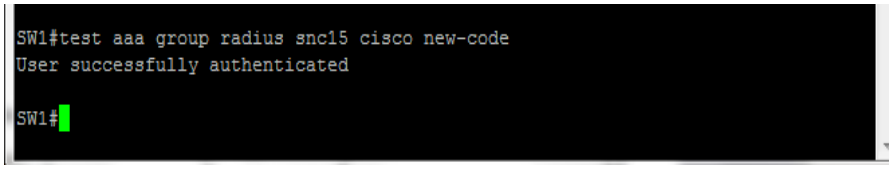

Figure 5. Authentication Test

2.2. Test Result

(1) To client-side to certificate whether the common user can enter into net. According to Figure 6 hints click the place.

(2) As Figure 7, input the username and passwords just test in pop-up dialog, then click ok waiting authentication completely.

(3) Waiting a moment, it will display authenticate successfully as Figure 8.

(4) As Figure 9, in client-side we open the CMD command line and try to login SW1 with just the username and passwords.

(5) The client-side can connect with the outside campus net as Figure 10. We can try to ping one some address 4.4.4.4 among the ISP topology, and then connect with the router belonging to outsides net to see the network address translation information as Figure 10.

(6) As Figure 12, we check the user login time in accounting data base on sever-side. Click Reports and Activity, and then choose RADIUS Accounting:

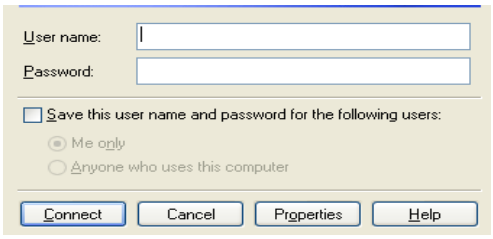

Figure 6. The Client-Side Hints

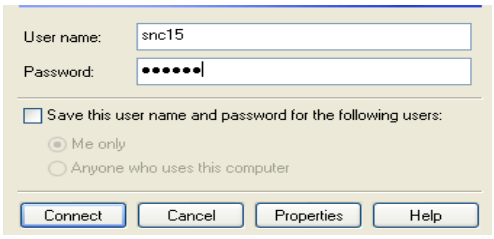

Figure 7. Local Login Hints

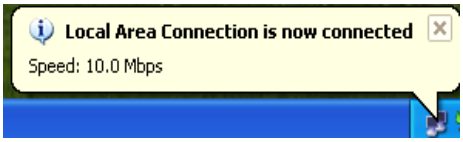

Figure 8. Authentication Successfully

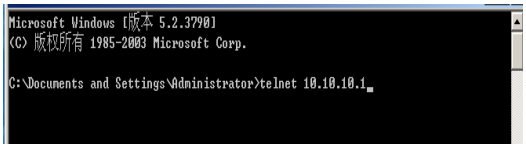

Figure 9. Try To Loginsw1

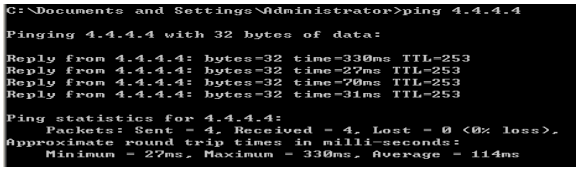

Figure 10. Client Computer Visit Outside Net

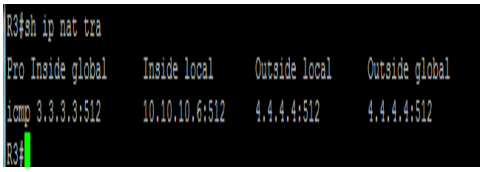

Figure 11. R3 NAT Translation Table

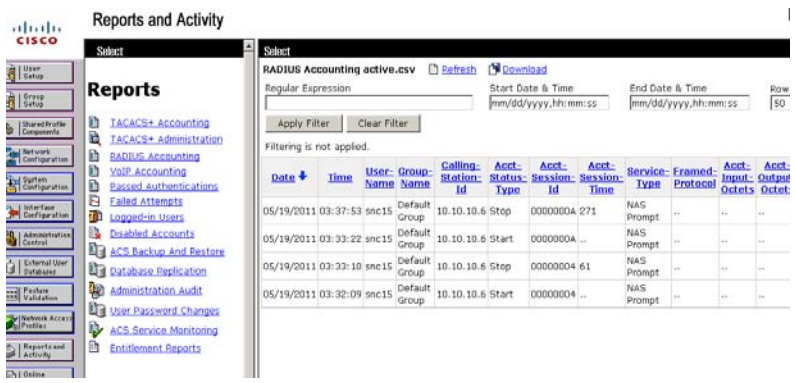

Figure 12. Accounting Data Base Displays

Through above operation we can check the authentication users who can get useful IP address and visit outside net, besides can find the user login time.

Cisco AAA is a authentication mechanism for checking user in remote security sever. It offer authentication, authorization, accounting three basic functions for managing mess net users to network manager, which makes legal users visit all kinds net resource safely. The cisco AAA authentication can account the legal user login time and restrict the action. At present stage of internet management the highest authority is not belong to every administrator. It always depends on the level of the ability or position of the high and low respectively with different levels of permissions. One hand is making the internet management much more normalization, on the other hand to avoid the newcomer internet manager‘s fail settings to paralyze the network.

References

[1] Yusufbhaiji. Network security technologies and Solutions. Beijing: Post &Telecom Press. 2009: 203-217.
[2] Brandon Carro. *Cisco Access Control Security: AAA Administrative Services.* Syngress Publishing. 2004: P58-73.
[3] Greg Bastien, Christian Abera Degu. CCSP Cisco Secure PIX Firewall Exam Certification Guide. Beijing: Post & Telecom Press. 2003: 9-18.
[4] Wayne Lewis, Ph.D, Cisco Systems, Cisco Networking Academy program: CCNP4.fault clearance. Beijing: Post & Telecom Press. 2005: 23-33.
[5] Rajesh. *Cisco Security Bible.* John Wiley & Sons INC Publishing. 2002: 21-29.
[6] Joe Harris. *Cisco Network Security Little Black Book*. *PARAGLYPH PR Publishing.* 2002; 19-28.
[7] James Macfarlane. *Network Routing Basics: Understanding IP Routing in Cisco Systems*. John Wiley & Sons INC Publishing. 2006: 12-24.
[8] http://baike.baidu.com/view/2951218.htm