Journal of Theoretical and Applied Information Technology
31st October 2012. Vol. 44 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

# RESEARCH ON AUTHENTICATION AND ACCOUNTING SYSTEMS BASED ON 802.1X

[1]YUE FUQIANG
[1]School of Automotive and Electronic Engineering, Xichang College, Xichang, China

## ABSTRACT

The user authentication and billing are important elements in the network management in particular. It is a normal and continuous operation of the campus network that guarantees the universal access based on traffic charges CERNET's campus network, billing. In this paper, we propose a campus network authentication and billing systems designed based on the 802.1x protocol, and give a more detailed description of the system.

**Keywords:** *Network Billing; 802.1x; The RADIUS; AAA*

## 1. INTRODUCTION

The CERNET scale of construction continues to expand, universities and secondary schools in succession through CERNET access the Internet. CERNET-sharing traffic costs for vast majority of schools, in addition, you also need to pay the substantial costs of the DDN lines, and network systems operation and maintenance. Therefore, the billing system is to guarantee normal operation of the campus network [1-4].

IEEE 802.1x protocol has complete user authentication and management capabilities to support broadband networks, billing, security, operations and management. 802.1x authentication mode and authentication architecture are optimized to solve the problems brought about by the traditional PPPoE and Web/Portal. The authentication method has a great advantage of broadband IP MAN, carrier-grade network operations and management, and is more suitable for the use in broadband Ethernet. Therefore, this article proposes a campus network authentication and accounting system based on the 802.1x protocol implementations [5-9].

## 2. AUTHENTICATION AND ACCOUNTING SYSTEM ARCHITECTURE DESIGN AND IMPLEMENTATION

Campus network users generally fall into two categories, one is not charging, the other is charging. According to the needs of different user groups within the campus network can only provide access authentication does not provide billing, or both to provide access authentication and billing functions. But whether it is billing or not billing, accurate identification of user identity not only needs accurate billing, but also network security management [10].

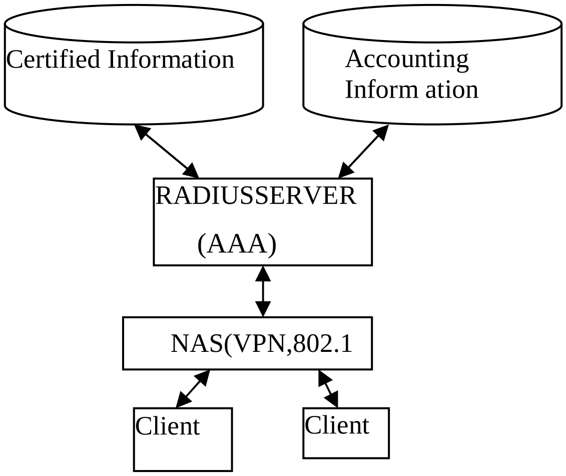

*Figure 1 System Architecture of CNAS*

Figure 1 depicts the logical structure of a new design of the campus network authentication and accounting system CNAS (Campus Network AAA System), the system can be extended IEEE 802.1x and RADIUS protocols, and using the free open source JBoss server software to build the certified meter. The fee system of management control platform. The IEEE 802.1x standard defines the limit of a Client/Server mode is not authenticated users access to the network; 802.1 x users can expand by binding IP or MAC, automatically assigns IP to limit user access, the extension is completely compatible with IEEE 802.1x standards. The majority of brand switches are realized 802.1x, and extend it, you can force the user requirements certified to use a fixed IP [11]. Safety interlocks in order to better implement IDS and other network components. You can choose to use the switches of the same brand as the NAS [12].

### 2.1 Realization of Authentication and Accounting Server

CNAS authentication and accounting server can used the most commonly used RADIUS server, it can use Windows Server 2003 operating system platform, using Free RADIUS server software to support the 802.1x protocol; can use the SQL Server database for user billing, user billing the raw data provided by the management module by the RADIUS service has been treated; can use the Sun ONE Directory Server for user authorization, user attributes and expanded to the IP, MAC and other properties. Standard RADIUS server is made to expand and modify the new user authorization and authentication modules, added a new traffic accounting module [13].

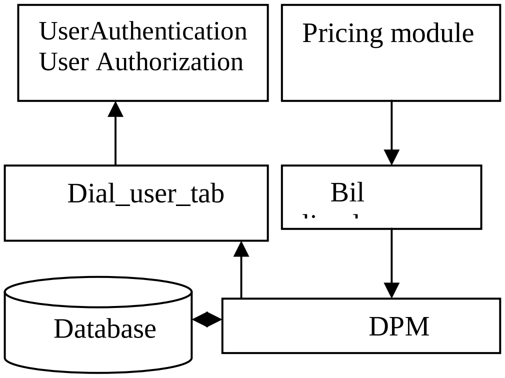

*Figure 2 Implementation Model of RADIUS Server*

Expanded RADIUS server was shown in Figure 2. It can complete the following: use for a radius server to achieve authorization for dial-in user authentication, only authorized authenticated users to use the dial-in service; recorded when the user dials the dial-in time, when the user disconnects, recorded off open time, and calculate the user total time-line; notified when the user dials the IP traffic accounting server which has been credited to the user traffic accounting server, and record traffic on the IP, notified when the user disconnects the flow accounting server, the user has to release the IP traffic accounting server of the IP traffic on the record to the user account.

The CNAS authentication server provides three basic functions, respectively Certification (Authentication), authorization (Authorization) and accounting (Accounting), namely, the AAA services. User authentication and authorization based on user-supplied user name and password, confirm the identity of the user legitimate, as well as to confirm whether the user has permissions to access the dial system. The newly designed user authentication and authorization modules use the existing RADIUS user authentication and authorization interface to access to the user-supplied user name and password, according to the database processing module the DPM (the Database Processing, Module,) generated by the user table Dial_user_tab first compare the user name and password to judge user identity is legitimate, and then determine whether users have permission to dial, and return success otherwise returns failure, so you can achieve the management and control of dial-up users.

New user billing module is to expand on the original RADIUS server. When the user through the authentication and authorization, access server (NAS) to accept a user's access to the RADIUS server sends accounting start information. Billing module obtain this information, recording time and IP address of the user access and communication function is called to register the user and IP address, so users can normally network traffic accounting module. When users take the initiative or outside disconnect a dial-up connection, the access server to the end of the RADIUS server sends billing information, so the traffic accounting module records the user's session ends, calculate online time; and call the communications function from the billing module access to the user's IP traffic, cancel the use of users IP.

### 2.2 Realization of Network Access Server

The 802.1x protocol is based on Client/Server access control and authentication protocol. It can restrict unauthorized users/devices to be accessed through the access port LAN/WLAN. The network access server (NAS) is a switch or AP before the switch or LAN provides a variety of business, 802.1x on the switch port connected to the user/device authentication. Prior to the adoption of the certification, 802.1x allows EAPoL (LAN-based Extensible Authentication Protocol) data through the device connected to switch port; certification through the normal data can pass through the Ethernet port.

A client makes a request to the NAS, the state is not certified, it cannot access the network; NAS sent to the client response package requires the user to provide a legal identity, such as username/password; client response to the authentication server access request, the authentication server bind the LDAP/Windows AD server, only the specified group or the specified domain user and password is correct, the system returns the user's authorization and IP to the NAS, only has authorized the user using the IP and returning the IP, the corresponding port of the NAS for this user open the user's state to certificate status, you can use the network resources.

In standard 802.1x, according to the certification status of the port, the port on the user is allowed access to the network. A non-controlled port under all users can use the network resources; only in a controlled port has certification status before they can access the network. Taking into account the device not in the campus network can support the 802.1x protocol. There are usually two deployment scenarios:

A.802.1x authentication in the access layer

The program calls for:

1) The user support for 802.1x user host is equipped with the 802.1x client software (Windows XP comes with the Star-the supplicant or the IEEE802.1x standard client software);

2) Access switches support the IEEE 802.1x (play a certification role);

3) At least one support standard RADIUS server as the authentication server.

The program's configuration points:

1) Access switch and the Radius Server, connected to the port and uplink port configured as a non-controlled port, so that users can communicate properly and severely, so that the authenticated user access to network resources through the uplink ports;

2) Set the user to connect the switch ports for the controlled port to access the user's control, the user must be authenticated to access network resources.

The program features:

1) Each supports the 802.1x switch responsible client, authentication speed. Independent of each other, switch to restart operation between the switch does not affect the other switches connected users;

2) Allows administrators to network management to the access layer device.

B.802.1x authentication in the convergence layer

The program calls for:

1) User-host support 802.1x, that is equipped with 802.1x client software (Windows XP comes with the Star-the supplicant or other IEEE802.1x standard client software);

2) Access layer switch cannot support the 802.1x protocol, but can support the transparent transmission of the IEEE 802.1x frame (EAPoL);

3) Aggregation layer switches support 802.1x;

4) At least one support standard RADIUS server as the authentication server [14-18].

The program's configuration points:

1) Connected with the Radius Server, switch ports and uplink ports, configured as a non-controlled port in order to switch to normal the server communications, so that authenticated users access to network resources through the uplink ports;

2) Set the access layer switch port connected to the controlled port to access the user's control, the user must be authenticated to access the network resources.

The program features:

1) Due to the convergence layer device, the network size is large, then under the number of users, equipment requirements, because if the layer of equipment failure will lead to a large number of users cannot access to the network;

2) Access layer devices can use cheaper unmanaged switch;

3) The administrator cannot be directly over a network management to the access layer device.

## 3. TNC SUPPORT TECHNOLOGY

This includes the network access technology, secure message transmission technology, and user authentication.

TNC network access layer is based on the existing network access technologies, including 802.1X, virtual private network VPN, and Point to Point Protocol PPP [19-22]. 802.1X port-based access control, network connection control through the controlled port and uncontrolled port for LAN, this application is currently the most widely used network access methods. VPN uses the Internet Key Exchange protocol IKE and IPsec protocol, Secure Sockets SSL or Transport Layer Security TLS on the Internet to establish a secure tunnel to ensure the security of data transmission. The PPP protocol point-to-point connection is the transmission standard method of multi-protocol datagrams.

Extensible Authentication Protocol for 802.1X architecture. EAP can not only transmit authentication information, but by the EAP method can also pass the terminal integrity measurement information. HTTP protocol and HTTPS for information related to the transfer application. TLS can pass the integrity of the report and the integrity check message handshake.

In network access control, user authentication, the TNC does not force the use of any agreement, but you can use the existing RADIUS protocol and Diameter protocol.

It can be seen in the Trusted Network Connect architecture, the underlying network access layer is basically follows the existing network access control technology, especially in the authentication protocol. TNC is an open support for heterogeneous environments, network access control architecture built on top of industry standards and specifications of the TCG specifications and other widely used. During the design process, it is necessary to consider the security of the architecture, and consider the compatibility with existing standards and technologies, to some extent, a compromise to consider, therefore, the TNC has certain advantages and also has some limitations. The following are its advantages and limitations of the analysis.

## 4. THE ADVANTAGES OF THE TNC

(1) The TNC architecture for interoperable, all norms are open to the public, researchers free access to the specification document. In addition, it uses a lot of existing standards and specifications, such as EAP, 802.1X, making the architecture be adapted to the needs of a wide range of environmental, not bound to a specific product. Its NAC architecture, the interoperability of the NAP architecture also illustrates the openness of the architecture.

(2) TNC is an extension of the traditional network access control technology based on the basis of user authentication, platform authentication and integrity verification. This will access the network terminal demanding higher and in turn enhanced the security of the network to provide access.

(3) The TNC specifications detailed considered a comprehensive interface definition specification and provided a specific message flow, XML Schema and the operating system and programming language bindings, such as IF-IMC and IF-IMV and IF-TNCCS, etc., easy to guidance products.

(4) TNC specifications for a complete architecture, each interface sub-specifications defined in detail, about the integrity of metrics, reporting and core issues such as set up a special Integrity Working Group (Integrity Working Group, IWG) to develop appropriate specifications and reference model, and compute the overall specification of both the association and its own system.

## 5. THE LIMITATIONS OF TNC

Although TNC has the above advantages, but it also has some limitations, some of the limitations are related to the Trusted Computing.

(1) The current situation exists in the field of trusted computing technology ahead of the theory of the TNC is no exception. How the chain of trust extends from the terminal to the network, the Internet has become a trusted computing environment; this is an urgent need to study the theoretical issues. TNC from a technical means of trusted computing technology is applied to network access control, but this access is still the lack of credible support of theory.

(2) The TNC verification of the credibility of the terminal based on integrity. Integrity can only be credible sources of information and has not been modified, and cannot guarantee that the information is credible. Moreover, credible validation of the integrity only ensure software static credible, is not yet sure the software is dynamic credible. TNC cannot guarantee a credible platform of access terminals. In addition, the TNC architecture based on integrity verification is more complicated and difficult to extend, achieve the high cost.

(3) TNC's starting point is to ensure network security; the framework does not consider how to protect the security of the terminal. Terminal prior to the access network, in addition to provide a platform for the credibility of evidence, but also should have a credible assessment of the access network, or cannot guarantee that access to credible service from the network.

(4) TNC architecture, multiple entities need to exchange information, such as TNCC and TNCS, TNCC and IMC, TNCS IMV between the IMC

and IMV need a lot of information exchange, but the TNC architecture itself does not given the appropriate security protocols, only a simple message passing.

(5) TNC just in the process of terminal access network terminal platform authentication and integrity verification, there is no appropriate measures to protect the network and terminal after the terminal access network. State changes may occur after the access terminal platform, it is necessary to increase the access control mechanism of the process. TNC1.3 architecture increases the security dynamic information sharing, to some extent, enhances the dynamic control functions.

(6) TNC application is currently limited to the enterprise network; it is difficult to provide distributed, multi-level, carrier-grade, and cross-network domain network access control architecture.

## 6. CONCLUSIONS

Most colleges and universities have implemented authentication and accounting system in order to improve the level of network management. Tsinghua University, Beijing has begun the original implementation of LAN computing network traffic earlier by IP address, MAC address authentication identity. The improvement of the account/password for authentication, according to the IP address was used to calculate the network traffic billing. With this 802.1x-based authentication billing, it will not only save the network resources and cost, ensure the controllable of school for all Internet users, improve network and information security, but also inevitably increase the difficulty of the user's Internet access.

## REFERENCES

[1]Scott Stark. JBoss Administration and Development 3.2.x Third Edition. Scott Stark and the JBoss Group, June, 2003.

[2] M.P.Vani, Computer Aided Interactive Process of Teaching Statistics Methodology–III Evaluation Questionnaire for LearnersThrough statistical display using Bar chart, IEIT Journal of Adaptive & Dynamic Computing, 2011(4), Oct 2011, pp:9-14. DOI=10.5813/www.ieit-web.org/IJADC/20114.2

[3] Ye Y.H., Liu W.P., Dao B, BIM-Based Durability Analysis for RC Structures, IEIT Journal of Adaptive & Dynamic Computing, 2011(4), Oct 2011, pp:15-24. DOI=10.5813/www.ieit-web.org/IJADC/20114.3

[4] R. Sandhu, K. Ranganathan and X. Zhang, Secure information sharing enabled by trusted computing and PEI models, Proceedings of. ACM Symposium on Information, Computer, and Communication Security, ACM Press. 2006.

[5] R. Krishnan, R. Sandhu, K. Ranganathan. PEI models towards scalable, usable and high-assurance information sharing. Proceedings of the 12th ACM symposium on Access control models and technologies. ACM Press. 2007. pp:145-150.

[6] Tian W.C., Cao Y.R, HFSS Simulation of Reconfigurable Multi-band Antenna Bands Based on RF Switch, IEIT Journal of Adaptive & Dynamic Computing, 2012(1), Jan 2012, pp:1-4. DOI=10.5813/www.ieit-web.org/IJADC/2012.1.1

[8] Zhao Z.L., Liu B., Li W, Image Classification Based on Extreme Learning Machine , IEIT Journal of Adaptive & Dynamic Computing, 2012(1), Jan 2012, pp:5-11. DOI=10.5813/www.ieit-web.org/IJADC/2012.1.2

[9] Zhao Z.L., Liu B., Li W, Image Clustering Based on Extreme K-means Algorithm, IEIT Journal of Adaptive & Dynamic Computing, 2012(1), Jan 2012, pp:12-16. DOI=10.5813/www.ieit-web.org/IJADC/2012.1.3

[10] Zheng L.P., Hu X.M., Guo M, On the q-Szasz Operators on Two Variables, IEIT Journal of Adaptive & Dynamic Computing, 2012(1), Jan 2012, pp:17-21. DOI=10.5813/www.ieit-web.org/IJADC/2012.1.4

[11] Hu G.P., Wang H.Y, Research on Similarity between Generalized Molecular Graphs, IEIT Journal of Adaptive & Dynamic Computing, 2012(1), Jan 2012, pp:22-27. DOI=10.5813/www.ieit-web.org/IJADC/2012.1.5

[12]Chen L., Zhao S.G., ZhangL.J., Zhang W.B, Real-time Large-deformation Cloth Simulation, IEIT Journal of Adaptive & Dynamic Computing, 2012(1), Jan 2012, pp:28-34. DOI=10.5813/www.ieit-web.org/IJADC/2012.1.6

[13]R. Sandhu, X. Zhang. Peer-to-peer access control architecture using trusted computing technology. SACMAT05. ACM Press. 2005. pp:147-158.

[14]Wenbo Mao, Fei Yan, Chunrun Chen, Daonity: grid security with behaviour conformity from trusted computing, Proceedings of the first ACM workshop on Scalable trusted computing, 2006, pp:43-46

[15]Shen Changxiang, Zhang Huanguo, Feng Dengguo, Cao Zhenfu, Huang Jiwu. Survey of Information Security, Science in Chian Series F,Vol.50,No.3,Jun.2007, pp：273-298.

[16]Wu H., Xu J.B., Zhang S.F., Wen H, GPU Accelerated Dissipative Particle Dynamics with Parallel Cell-list Updating, IEIT Journal of Adaptive & Dynamic Computing, 2011(2), Apr 2011, pp:26-32. DOI=10.5813/www.ieit-web.org/IJADC/2011.2.4

[17]Zhou J.J, The Parallelization Design of Reservoir Numerical Simulator, IEIT Journal of Adaptive & Dynamic Computing, 2011(2), Apr 2011, pp:33-37. DOI=10.5813/www.ieit-web.org/IJADC/2011.2.5

[18] Zhao Z.L., Liu B., Li W, Image Classification Based on Extreme Learning Machine , IEIT Journal of Adaptive & Dynamic Computing, 2012(1), Jan 2012, pp:5-11. DOI=10.5813/www.ieit-web.org/IJADC/2012.1.2

[19] Zhao Z.L., Liu B., Li W, Image Clustering Based on Extreme K-means Algorithm, IEIT Journal of Adaptive & Dynamic Computing, 2012(1), Jan 2012, pp:12-16. DOI=10.5813/www.ieit-web.org/IJADC/2012.1.3

[20] Zhao C.H., Zhang J., Zhong X.Y., Chen S.J., Liu X.M, Analysis of Tower Crane Monitoring and Life Prediction, IEIT Journal of Adaptive & Dynamic Computing, 2012(2), Apr 2012, pp:12-16. DOI=10.5813/www.ieit-web.org/IJADC/2012.2.3

[21] Zhao C.H., Chen S.J., Liu X.M., Zhang J., Zeng J, Study on Modeling Methods of Flexible Body in ADAMS, IEIT Journal of Adaptive & Dynamic Computing, 2012(2), Apr 2012, pp:17-22. DOI=10.5813/www.ieit-web.org/IJADC/2012.2.4

[22] Chen G.Q., Jiang Z.S., Wu Y.Q, A New Approach for Numerical Manifold Method, IEIT Journal of Adaptive & Dynamic Computing, 2012(2), Apr 2012, pp:23-34. DOI=10.5813/www.ieit-web.org/IJADC/2012.2.5