AAA Based on 802.1x Authentication

Jiange Zhang*, Yuanbo Guo, Yue Chen and Jun Ma

State Key Laboratory of Mathematical Engineering and Advanced Computing, China National Digital Switching System Engineering and Technological Research Center, Zhengzhou Information Science and Technology Institute, Zhengzhou, China

jiangezh@126.com

Keywords: 802.1x authentication; EAP protocol; RADIUS protocol; configure; analysis of these messages

Abstract. It has obvious advantage to adopt 802.1x authentication for network access control, which is an ideal and low-cost scheme and is usually used for those enterprises and campuses which run and manage simply or have simple business. This paper analyzed 802.1x protocol, EAP protocol and RADIUS protocol, configured switch, FreeRADIUS Server and MySQL, constructed AAA management framework which is based on 802.1x authentication at the end, and showed the whole authentication flow. Using software the messages of the whole authentication process have been captured. The brief analysis of these messages provides technology strongly for particular research and further improvement, and has important value for research and application.

1. Introduction

802.1x authentication has many characteristics such as higher efficiency of message, better supporting ability of multicast, lower requirement of equipment and simpler supporting for increment application.

Hence, the advantage of 802.1x is obvious, and it is an ideal and low-cost scheme, which is applied to point-to-point connection mode between access equipment and access port, realizes the authentication and management of users who are authorized to access LAN, and is usually used for those enterprises and campuses which run and manage simply or have simple business.

2. Related protocols about authentication

2.1 802.1x protocol

802.1x defines a protocol which is called port based network access control[1]. The port may be physical port, and may be also logical port. The protocol provides a scheme of users' identity authentication, but it is not able to realize this scheme only depending on 802.1x, and managers of access equipment should also configure AAA, select RADIUS or local authentication method to finish users' identity authentication.

The purpose of 802.1x authentication is ensuring that the port would be usable, that is to say, for a port it will be opened if authenticated successfully and allow all messages to pass, but it will be closed if not successfully and only allow EAPOL which is the authentication message of 802.1x to pass. EAPOL frame format includes PAE ethernet type, protocol version, packet type, packet body length and packet body, whose size is respectively 2 bytes, 1 byte, 1 byte, 2 bytes and variable.

2.2 EAP protocol

EAP (Extensible Authentication Protocol)[2] is mostly used between client and switch. This authentication mode alleviates the burden of switch to a certain extent because the challenge and computing process are accomplished by server. EAP supports many authentication methods[3] such

as Eap-Md5, Eap-TLS, Eap-TTLS, PEAP and so on. EAP packet format includes code, identifier, length, type and data, whose size is respectively 1 byte, 1 byte, 1 byte, 1 byte and variable.

2.3 RADIUS protocol

RADIUS (Remote Authentication Dial In User Service)[4] is a protocol of C/S which is mostly used between switch and authentication server. This protocol is used to identify users' name and password, if users are authenticated successfully they will be able to use authorized resources, and will pay for their Internet fee according to the using record which is saved. That is to say, this protocol includes 3 functions which are authentication, authorization and accounting or AAA for short. RADIUS packet format includes code, identifier, length, authenticator and attribute, whose size is respectively 1 byte, 1 byte, 2 bytes, 16 bytes and variable.

3. Authentication flow

The AAA system has three parts which are client, switch, authentication server (FreeRADIUS2.1.10). The authentication process is as follows.

Step1: client requests for switch.

Step2: switch collects users' name and password and transmits to AAA server.

Step3: AAA server matches them with its own database according to given algorithm, then returns result which is accepted, rejected or other (for example, challenge) to switch.

Step4: switch opens or closes client according to returned result.

If client authenticated successfully the following procedure will go on.

Step5: server authorizes client, and switch configures client' Internet environment according to authorization results.

Step6: if accounting is needed switch will collect client' using Internet resources and transmit them to accounting server.

The transmitted messages of the whole process are showed in Figure 1.

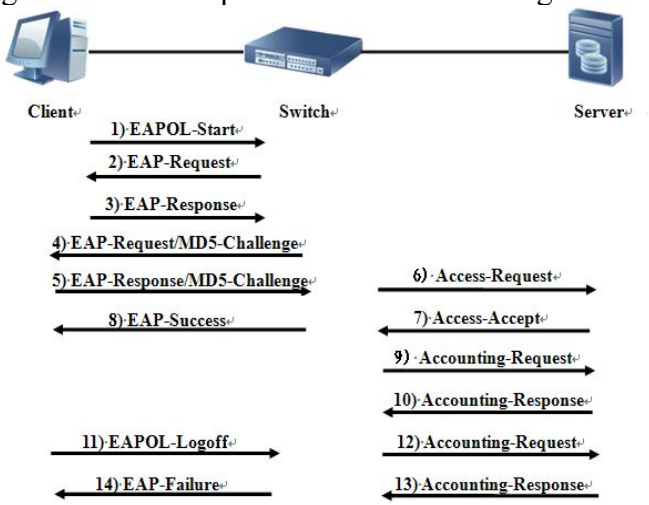

Fig.1: Tansmitted messages

4. The configuration of authentication system

4.1 The configuration of switch

RADIUS protocol lies on UDP protocol. The authentication port is 1812, and the accounting port is 1813, moreover, it adopts key to ensure network safety. Supposing the IP address of authentication server is 192.168.0.83, and the key is testing123, the configuration shall be as follows.

[Quidway]radius scheme xy

[Quidway-radius-xy]primary authentication 192.168.0.83 1812

[Quidway-radius-xy]primary accounting 192.168.0.83 1813
[Quidway-radius-xy]key authentication testing123
[Quidway-radius-xy]key accounting testing123
[Quidway-radius-xy]user-name-format without-domain
[Quidway]domain xy
[Quidway-isp-xy]radius-scheme xy
[Quidway]domain default enable xy

4.2 The configuration of FreeRADIUS server

FreeRADIUS is based on RADIUS protocol and it realizes AAA function[5]. Its operation system is Linux, and the process of its compile and installation is as usual.

After installation the FreeRADIUS server should be configured.

Step1: client IP address and key should be added at the end of the file clients.conf

Step2: the symbol "#" before the line $INCLUDE sql.conf should be canceled in the file radiusd.conf in order to use SQL database.

Step3: the name and password in the sql section of the file sql.conf is the name and password of SQL database which is root and dove in the test.

Step4: the lines files should be added symbol "#" and the lines sql should be canceled symbol "#" in the files default and inner-tunnel of the directory sites-enabled in order to use SQL database.

Step5: the lines files should be added symbol "#" and the lines sql should be canceled symbol "#" in the files default of the directory sites-available in order to use SQL database.

4.3 The configuration of FreeRADIUS Client

It can use FreeRADIUS Client to authenticate, if most users use Linux system. The process of its compile and installation in Linux system is as usual.

After installation the FreeRADIUS Client should be configured.

Step1: the IP address of authentication server and authorization server should be configured in the file radiusclient.conf, and the value is 192.168.0.83 here.

Step2: the IP address of server and the key should be configured in the file servers, and the value is 192.168.0.83 and testing123.

It can use the following methods to authenticate, if most users use Windows system.

One method is making use of Cygwin software. It is a simulation platform of Linux system which can run on Windows system, and it is also seen as the terminal of Linux. After installing completely there will be a new directory whose name is cygwin in system disk, and the directory is same as the directory of Linux. If users want to use the software of FreeRADIUS Client, they should open the software of Cygwin in Windows system, and input the command of installation. This solution has a little difficulty, and suits with those users who are familiar with the command of Linux.

The other method is adopting authentication mode supporting 802.1x protocol, and don't use the software of FreeRADIUS Client to authenticate. The authentication mode based on 802.1x protocol can realize authorization, authentication and accounting and it can realize effective control for network access of LAN's users also. Moreover, the software supporting 802.1x protocol can be downloaded easily in the Internet.

4.4 The configuration of MySQL

If there are scores of users or more the database should be used. If the number of users is below myriad the MySQL will be right selection.

Step1: create database radius.

Step2: create tables of the database radius.

Step3: add testing user.

5. Test

The procedure of test in Linux system is as follows.

Step1: (Start server) radius –X

Step2: (Start client) radlogin

The username is test and the password is test here, and it will show successful information after inputting them correctly.

If using the software which is supported by 802.11, the message of authentication successfully will be showed when user input the right name and password. Using software (the software of server is wireshark and the software of client is sniffer) the messages among client, switch and server will be showed in Table 4 according to Figure 1. In the test client' IP address is 192.168.0.73 and MAC address is 001E90611045, switch' IP address is 192.168.0.224 and MAC address is Huawei6D825E, and server' IP address is 192.168.0.83 and MAC address is 00188b540032. The messages between client and switch are EAP and the numbers are 1, 2, 3, 4, 5, 8, 11 and 14, the frame-type of these messages is 0x888e, and the protocol version is 0x01. The messages between switch and server are RADIUS and the numbers are 6, 7, 9, 12 and 13, the frame-type of these messages is 0x0800.

Table 4: Messages among client, switch, server

No.	Message	Source	Destination	Type	Code	Id.
1	EAPOL-Start	001E90611045	0180C2000003	0x01		
2	EAP-Request	Huawei6D825E	001E90611045	0x00	0x01	2
3	EAP-Response	001E90611045	Huawei6D825E	0x00	0x02	2
4	EAP-Request/MD5-Challenge	Huawei6D825E	001E90611045	0x00	0x01	3
5	EAP-Response/MD5-Challenge	001E90611045	Huawei6D825E	0x00	0x02	3
6	*Access-Request*	*192.168.0.224*	*192.168.0.83*		*0x01*	*108*
7	*Access-Accept*	*192.168.0.83*	*192.168.0.224*		*0x02*	*108*
8	EAP-Success	Huawei6D825E	001E90611045	0x00	0x03	3
9	*Accounting-Request*	*192.168.0.224*	*192.168.0.83*		*0x04*	*244*
10	*Accounting-Response*	*192.168.0.83*	*192.168.0.224*		*0x05*	*244*
11	EAPOL-Logoff	001E90611045	Huawei6D825E	0x02		
12	*Accounting-Request*	*192.168.0.224*	*192.168.0.83*		*0x04*	*245*
13	*Accounting-Response*	*192.168.0.83*	*192.168.0.224*		*0x05*	*245*
14	EAP-Failure	Huawei6D825E	001E90611045	0x00	0x04	4

6. Conclusions

The 802.1x authentication realizes authorization, authentication and accounting and it realizes effective control for network access of LAN's users. Hence, the configuration of AAA system supporting 802.1x authentication provides technology strongly for particular research and further improvement, and it is very important for research and application.

References

[1] IEEE standard for local and metropolitan area networks-port-based network access control[S]. IEEE Std, 802.1x, 2001.

[2] Blunk L, J Vollbrecht. PPP Extensible Authentication Protocol(EAP)[S]. IETF RFC2284.

[3] Chiornita, Alexandra. A practical analysis of EAP authentication methods [J]. 2010 9th Roedunet International Conference (RoEduNet), 31-35, 2010.

[4] Remote authentication dial in user service(RADIUS)[S]. IETF RFC2865, 2000.

[5] Shujuan Wang, Mangui Liang. A Network Access Control Approach for QoS Support Based on the AAA Architecture [J]. 2010 International Symposium on Intelligence Information Processing and Trusted Computing (IPTC), 507-511, 2010.