Asian Journal of Information Technology 6 (1): 47-53, 2007

Design and Implementation of an AAA-Enabled Access Management System for Wireless Networks

[1]Fu-Min Chang, [2]Chih-Mou Shih and [2]Shang-Juh Kao
[1]Department of Finance, ChaoYang University of Technology,
168 Jifong E. Rd., Wufong Township Taichung County, Taiwan
[2]Department of Computer Science, National Chung-Hsing University,
250 Kuo-Kuang Rd. Taichung City, Taiwan

Abstract: In the current wireless network environment, Remote Access Dial-In User Service (RADIUS) protocol was mainly adopted to provide the services of Authentication, Authorization and Accounting (AAA), which was proposed by IETF. With this protocol support, a secure environment for wireless users is provided while the usage of network resources can also be monitored and managed by system administrator. However, not all wireless access points support the RADIUS protocol, which causes the difficulty of building a universal wireless security environment. Furthermore, the accounting policy of RADIUS protocol takes into account the idle time of a wireless user whenever he is in the connection state, which is obviously unfair to the user. To overcome these deficiencies, in this study, we propose a wireless network access management system which directs the processes of authentication, authorization and accounting to back-end servers. In the system, by employing the approach similar to the webpage authentication, the wireless access point is not necessary in verification of legal access but simply transfers the messages to the back-end authorization and authentication server. Consequently, the AAA features are satisfyingly accomplished with a better accounting strategy. Specifically, the NetFlow protocol is applied to collect the wireless network usage for each user. Based on the collection, the time or the traffic each user actually utilizes is accounted for. Four accounting alternatives, which are time-prepaid, flow-prepaid, time-postpaid and flow-postpaid, are proposed and demonstrated.

Key words: AAA, radius, wireless network, access management, netflow

INTRODUCTION

Wireless Internet access has become more and more popular. The widespread use of wireless network environment creates a strong demand for the service of Authentication, Authorization and Accounting (AAA) (De Laet *et al*., 2000; Metz, 1999; Voll Brecht *et al*., 2002). In order to provide a secure Internet access management and assure the revenue of service providers, several AAA protocols are proposed, such as Terminal Access Controller Access Control System (TACACS, http://www.ciso.com/warp/public/614/7.html),(TACACS+ http://www.ciso.com/warp/public/614/7.html), Remote Access Dial In User Service (RADIUS and Jonathan Hassell); Rigney *et al.* (2000) and DIAMETER http://www.diameter.org/. Among these AAA protocols, TACACS+ is usually adopted in Cisco products. It is an enhancement of the original TACACS, which is the first AAA protocol developed by Cisco Systems. Although many features can be found in TACACS+, it is a proprietary protocol that is only available in Cisco's products. Another AAA Protocol is DIAMETER, which is newly developed by IETF. DIAMETER has several improvements over RADIUS such as failover, transmission-level security and agent support. However, this project is still in its infancy. Hence, currently management requirements of AAA are mostly accomplished through the RADIUS.

Even though RADIUS protocol was frequently adopted to provide the services of AAA for wireless networks, there still exist several shortages. First of all, to enable AAA features under RADIUS, all Access Points (APs) must also support the RADIUS protocol. This requirement is impractical. For accounting in RADIUS, time duration since connecting to the Internet until logout is taken into account, no matter how a user uses the Internet resources. In several occurrences, an idle user is also charged without consuming any network traffic. Many Internet Service Providers (ISPs) disconnect an idle user when he is inactive for a long time. However, the length the inactive time is not easy to determine and different types of users may have different criteria. Some

Corresponding Author: Fu-Min Chang, Department of Finance, ChaoYang University of Technology, 168 Jifong E. Rd., Wufong Township Taichung County, Taiwan

type of users may occupy the network for a large volume of data communication, while others may consume only a little of network bandwidth. Consequently, providing an accounting management to allow alternatives of either time or traffic consumption could be favorable to various application users.

An Internet user could require several application services provided by different ISPs. For instance, he may access an Internet game by logging in to an ISP, while goes through another ISP to download a movie. Since ISPs have their own IP address scopes, how to migrate from one ISP to another ISP without logging out and logging in again causes a challenge to AAA implementation. A user friendly Internet access management system is supposed to provide users the best choice to utilize the resources transparently.

In this study, we present a practical, flexible and user-friendly access management system to implement AAA features for wireless networks. Our implementation carries out authentication, authorization and accounting via the redirection module, authentication module and accounting module, together with the cooperation of web server, NAT server, DHCP server and DNS server. As AAA features being processed at powerful computing servers in the backend, the loads at APs can be significantly reduced and the functions of AAA can also be flexibly customized. According to the deficiencies mentioned above, we adopt NetFlow, http://www.ciso.com/. protocol to collect user connection information at the NAT server. A regular AP, which is not necessary to have the RADIUS support, is adequate for transferring communication messages to accomplish the AAA requirement. We also propose four accounting alternatives for end users' selection according to their preferences.

Related AAA protocols

TACACS and TACACS+: TACACS (Terminal Access Controller Access Control System) is an industrial standard protocol specification, which provides on authentication scheme forwarding username and password information to a centralized server. The centralized server can either be a TACACS database or a database like the UNIX password file with TACACS protocol support. TACACS is now somewhat dated and is not used as frequently as it once was. A later version of TACACS was called XTACACS (Extended TACACS). These two versions have generally been replaced by TACACS+ and RADIUS in newer or updated networks. TACACS+ allows a separate access server (the TACACS+ server) to provide the services of authentication, authorization and accounting independently. Each service can be tied into its own database or can use the other services available on that server or on the network. TACACS+ is courtesy of Cisco routers and network access servers.

Radius: RADIUS use the client-server model and the Network Access Server (NAS) plays the role as a RADIUS client. RADIUS servers receive the request from the user connection, authenticate the user and then reply all necessary configuration information for the client (NAS) to deliver service to the user. If accounting is used, the RADIUS server is also used to receive and store accounting information in a suitable way. Transactions between the server and client are authenticated by a shared secret. If the server receives a packet that the server cannot authenticate, the server discards the packet. RADIUS uses UDP as its transmission protocol. This requirement differs from retransmission timers defined in the TCP protocol. RADIUS does not require the detection of lost data. The user will wait for few seconds until the authentication is complete. The operation of RADIUS is shown in Fig. 1.

Diameter: The newly developed DIAMETER protocol is intended to provide an AAA framework for applications such as network access or IP mobility. DIAMETER is a network protocol that provides AAA services for roaming users. It was designed by Pat Calhoun of Black Storm Networks in 1996 as a replacement for the outdated RADIUS protocol. Its open base protocol provides transport, message delivery and error handling services to applications that need them to function in broader, multi-domain environments. With DIAMETER's last call issued by the Internet Engineering Task Force (IETF) on October 22, 2002, it has become a proposed standard on January 27, 2003. It will serve as an alternative to older protocols like RADIUS or the proprietary TACACS+.

The proposed system architecture: The AAA-enabled access management system consists of DHCP server and DNS server together with three main modules: Redirection module, authentication module and accounting module, as shown in Fig. 2. In between redirection module and authentication module is the authorization agent.

Fig. 1: Operation of radius

Fig. 2: The architecture of the AAA-enabled access management system

Physically, these modules are located at NAT server, web server and accounting server. Specifically, the redirection module is installed in the NAT server. When a user is trying to access to the Internet, he is first connected to the DHCP server through an AP for a temporary IP address, 10.0.0.*. Before the user can actually use the Internet resources, AP forwards the request to the redirection module, which is redirected to the web server and RADIUS server for authentication. Once the user is authenticated, a public IP address is assigned and scope of ports are authorized. Since then, he can legally access the Internet.

AP acts as an interface between a user and the access management system for entering the internet. Its main role is to consult with DHCP and DNS server and to forward the message to the redirection module. Both DHCP and DNS servers are cooperated to distribute IP addresses and to provide the domain name lookup service during the initiation phase of a connection session.

Redirection module, which contains the policy executor, is the first security entry for guarding the system entrance. It provides the message filtering and determines the redirection. Before a user has been granted to access the Internet, redirection module ensures that only the authentication necessary information is made available. The targets of redirection can be classified into three categories: Authentication server, authorized access and restricted access. An unauthenticated user will be redirected to the authentication module. An already authenticated user will be authorized to access the Internet. If the authentication fails, the access request is rejected and the requesting user is prompted to the web server for another sign-in.

Authentication module is composed of RADIUS server, web server and a database. RADIUS server plays the key role of authentication. It incorporates with browsers having SSL, (Kipp Hickman *et al*., 1994) support to accomplish the verification procedures. Authentication request is issued from the web server, which encapsulates the request using SSL protocol and forwards to the RADIUS server for verification. An authenticated request is then processed by the authorization agent for access right association. The procedures that a user starts to issue an Internet connection request until the occurrence of authorized use are summarized in Fig. 3.

Inside the accounting module is the NetFlow agent, accounting server and a database. This module monitors and controls the resource usage. Unlike the traditional accounting management using RADIUS, we gather NetFlow data at the NAT server for all Internet connection once a user is authenticated. Since we monitor the consumption of all Internet resources of users, we are able to analyze the data collection to accurately and flexibly implement the accounting management. The accounting procedures involve AP, NAT server, accounting server and the database, which can be summarized as in Fig. 4.

System implementation and management applications: In order to demonstrate the system's feasibility, we implement an experimental wireless network system. We adopted the Host AP, http://hostap.epitest.fi/. a

Fig. 3: Workflow of redirection, authentication and authorization

Fig. 4: Accounting procedures

programmable device of wireless access point and set it as in the bridge state. Meanwhile, we chose the Apache Tomcat, http://hostap.hostap.epitest.fi/. for the web server and used Java servlet to write the authentication program. FreeRADIUS http://www.freeRADIUS.org/. was deployed for the RADIUS server in a Linux host and MSSQL Server 2000 was used for the database for both accounting and authentication purposes. We also used fprobe http://sourceforge.net/projects/fprobe. to collect NetFlow packets and applied iptables (Gregor, 2004). http://iptables-tutorial.frozentux.net/iptables-tutorials.html. for redirection and authorization. Accounting server, which is a Windows PC, receives and analyzes the NetFlow packets and records into the database. Various accounting mechanisms can be implemented according to the data logged in the database. The physical layout of the experimental system is depicted in Fig. 5.

Redirection and authentication management applications: As redirection module plays the security entry for guarding the system access, we implement policy executor at the NAT server to verify user's identity. Before a user is verified, he can only lookup the domain names without actually connecting to the Internet. Only when he has passed the authentication, can he obtain the access right to external world. An unauthenticated user is redirected to the web server, which is at 10.0.0.1, for authentication procedure. The web server prompts user name and password for verification purpose as shown in Fig. 6. We use Password Authentication Protocol (PAP Loyd and Simpson, 1992.) and MD5 Rivest, 1992. encryption mechanism to manipulate the shared secret and authenticator. The results are XORed with user's password, encapsulated using UDP packets and then transferred to the RADIUS server. RADIUS server performs the examination using the information stored in the database to determine whether the requesting user is legal or not.

Authorization management applications: Once a user has passed the authentication, authorization agent scans the NAT data table for available IP address and the range of available port numbers. Each authenticated user is allocated one public IP address and a scope of port numbers, usually 1024 ports are assigned. Port numbers

Fig. 5: The experimental wireless network system

Fig. 6: The webpage for unauthorized user

from 0 to 1023 are reserved by the system. The names and data types of attributes in NAT data table are included in the followings: (IpIndex, int), (Public_IP, char), (Public_StartPort, int), (Public_EndPort, int), (UserId, int), (Private_IP, char), (AuthTime, datetime), (Status, char) and (Idle, int). Authorization agent establishes the corresponding public IP and available ports using SNAT protocol http://iptables-tutorial.frozentux.net/iptables-tutorial.html. and it also registers the allocated public IP and available ports for the authenticated user. For example, as shown in Fig. 7, both internal IP address 10.0.0.15 and 10.0.0.16 are assigned from the DHCP server. Once they passed the authentication, both addresses are associated with the same public address, 140.120.15.50, but with separate port numbers 2048-3071 and 1024-2047.

As multi-homing service has becoming popular, many ISPs are cooperated to offer convenient applications for the user. Other than simply relying on AP to transmit account/password to RADIUS server for verification, we are able to carry the extra information, such as for ISP's migration, by embedding the information into the packets at web server. When a user submits his account and password, he may be assigned an IP which is not in the range of his subscribed scope. By redirecting

Target	Prot opt source	Destination	
Accept	All -10.0.0.16	0.0.0.0/0	
Accept	All -10.0.0.15	0.0.0.0/0	
Dnat	All -10.0.0/24	10.0.0.0/24	to: 10.0.0.1
Chain postrouting (policy accept)			
Target	Prot opt source	Destination	
Snat	udp-10.0.0.16	0.0.0.0/0	to: 140.120.15.50:2048-3071
Snat	tcp -10.0.0.16	0.0.0.0/0	to: 140.120.15.50:2048-3071
Snat	tcp -10.0.0.15	0.0.0.0/0	to: 140.120.15.50:1024-2047
Snat	upd -10.0.0.15	0.0.0.0/0	to: 140.120.15.50:1024-2047

Fig. 7: Public IP address ports assignment for each private IP

Recvtime		Srcip	Srcport	Desip	Desport	Octets
2006/1/4	0721:18	203-187.48.77	21	1400120-15.50	3072	5190
2006/1/4	0721:56	140-120.15.50	3072	203.187-48.77	1055	2571848
2006/1/4	0722:07	203-187.48.77	3072	203.187-48.77	1058	3621632
2006/1/4	0722:20	203-187.48.77	1032	140-120-15.50	3072	647
2006/1/4	0722:50	203-187.48.77	1047	140.120-15.50	1024	604
2006/1/4	0726:01	203-187.48.77	1103	140.120-15.50	3072	186490
2006/1/4	0726:25	140-120.15.50	3072	203.187-48.77	1086	168
2006/1/4	0726:29	140-120.15.50	3072	203.187-48.77	1088	3033559
2006/1/4	0726:33	203-187.48.77	21	140.120-15.50	3072	1130

Fig. 8: A sample netflow data table

UserId	Private_IP	Public_IP	Public_StartPort	Public_EndPort	Acc_StartTime		Acc_EndTime		Octets
10.0.0.15	140.120.1550	1024	2047	2006/1/4	07:22:00	2006/1/4	07:22:50	2006/1/4	604
10.0.0.16	140.120.1550	2048	3071	2006/1/4	07:22:00	<NULL>		<NULL>	<NULL>
10.0.0.17	140-120.1550	3072	4095	2006/1/4	07:22:00	2006/1/4	07:22:20	2006/1/4	3622279

Fig. 9: A sample accounting data table

the authentication procedure to the backend web server and RADIUS server, authorization of alternative ISP choices can be automatically accomplished in a multi-homing environment.

Accounting management applications: By installing fprobe http://sourceforge.net/project/fprobe.at the NAT server, we deploy the NetFlow agent to collect all traffic passing through the NAT server. The NetFlow packets are transferred to the accounting server for resource consumption computation. When the accounting server receives these packets, it extracts the source IP, destination IP, source port number, destination port number, time and amount of data transferred and writes to the NetFlow data table. The table contains the following attributes: recvtime, srcip, srcport, desip, desport, octets. A sample NetFlow data table is shown in Fig. 8.

For calculating the exact resource usage, another table, the accounting data table, is necessary. The accounting table records all necessary information for each perspective user. The accounting data table includes the attributes of UserId, Private_IP, Public_IP, Public_StartPort, Public_EndPort, Acc_StartTime, Acc_EndTime and Octets. By comparing the data in both NetFlow data table and Accounting data table, we are able to figure out how much the Internet resource is consumed by each user. Part of an Accounting data table can be shown in Fig. 9.

In our system, four accounting alternatives are available for users based on their preferences. They are time pre-paid, time post-paid, traffic pre-paid and traffic post-paid billing systems. Both pre-paid billing choices are to deduct the amount of time or data flow periodically from the user's pre-paid quota, while the amount is adding to the user's resource consumption table in the post-paid counterpart. By taking into account the Acc-StartTime, Acc_EndTime and Octets of corresponding UserId, both pre-paid and post-paid billing alternatives in either time-based or data flow-based becomes possible. Consequently, an end user has the flexibility in determining his most favorite accounting system.

CONCLUSION

RADIUS is the most commonly used protocol for AAA implementation. However, it works only with the APs that support the RADIUS protocol. Even though with RADIUS, the accounting management is short of

flexibility and fairness. Moreover, RADIUS supported access management could be insufficient to cope with a multi-homing environment. In this study, we presented an efficient but flexible AAA-enabled wireless access management system. Without the requirement of RADIUS support at APs, we can freely customize the packets for authentication purpose. In our proposal, authentication processing is executed at the backend web server and RADIUS server. Using this approach, it is easy to adopt authentication mechanisms other than the commonly used EAP/MD5 Rivest, 1992, Blunk and Vollbrecht, 1988, Jyh-Chng Chen and Yu-Ping Wang, 2005. such as EAP/TLS (1999) and EAP/TTLS (2003) proposed in IEEE 802.1x (2001) Aruncesh and William, 2002. without extra hardware installations.

To provide a better choice for end users to determine which criteria the accounting will be based, the system offers four accounting alternatives for end users. An Internet application user may choose either connection time or data transfer volume for his accounting basis. By analyzing the statistics of NetFlow packets at the NAT server, we are sure the time and volume that a user exactly consumes. And, we can effectively rule out the problem of disconnecting from the Internet due to the long idle time and prevent the re-authenticating procedures from repetitive logins. To make the system friendlier, in both pre-paid billing systems, some sort of alert generation could be favored whenever the left amount of time or data is below a predefined threshold. Nevertheless, the proposed access management system is powerful enough to practically provide all the AAA features without equipping all APs with RADIUS for wireless networks.

REFERENCES

Arunesh Mishra and William A. Arbaugh, 2002. An initial security analysis of the IEEE 802.1X Standard, Department of Computer Science, University of Maryland College Park, CS-TR-4328.

Aboba, B. and D. Simon, 1999. PPP EAP TLS Authentication Protocol, RFC 2716.

De Laat, C.G. Gross, L. Gommans, J. Vollbrecht and D. Spence, 2000. Generic AAA Architecture, RFC 2903.

DIAMETER Base Protocol, http://www.diameter.org/

Funk, P. and S. Blake-Wilson, 2003. EAP tunneled TLS authentication protocol, IETF Internet Draft, Draft-ietf-pppext-eap-ttls-05.txt.

FreeRADIUS, http://www.freeRADIUS.org/.

Fprobe, http://sourceforge.net/projects/fprobe.

Gregor, N. Purdy, 2004. LINUX Iptables Pocket Reference, O'Reilly, ISBN: 0-596-00569-5.

IEEE Std, 2001, 802.1X-, Port-based network access control, Institute of Electrical and Electronics Engineering, Inc.

Iptables Tutorial 1.1.19, http://iptables-tutorial. frozentux. net/iptables-tutorial.html.

Jyh-Cheng Chen and Yu-Ping Wang, 2005. Extensible Authentication Protocol (EAP) and IEEE 802.1x: Tutorial and Empirical Experience, IEEE Radio Communications, pp: 26-32.

Jonathan Hassell, RADIUS and O'Reilly, 2002. ISBN:0-596-00322-6 .

Jouni Malinen, Host AP, http://hostap.epitest.fi/.

Kipp, E.B., 1994. Hickman, The SSL Protocol, Netscape Communications Corp.

L. Blunk and J. Vollbrecht, 1998. PPP Extensible Authentication Protocol (EAP), RFC 2284.

Lloyd, B. and W. Simpson, 1992. PPP Authentication Protocols, RFC 1334.

Metz, C. 1999. AAA protocols: Authentication, authorization and accounting for the Internet, IEEE Internet Computing, pp: 75-79.

NetFlow, http://www.cisco.com/.

Rigney, C., S. Willens, A. Rubens and W. Simpson, 2000. Remote Authentication Dial In User Service, RFC 2865.

Rivest, R., 1992 The MD5 Message-Digest Algorithm, RFC., 1321.

Tomcat, http://tomcat.apache.org/.

TACACS+ Protocol, http: //www. cisco. com/ warp/ public/614/7.html

Vollbrecht, J., P. Calhoun, S. Farrell, L. Gommans and G. Gross *et al*., 2000. AAA Authorization Framework, RFC 2904 .