The design of AAA server for Wireless LAN with 802.1x

YoungHwan Ham and ByungHo Chung
Wireless Internet Security Research Team, Information Security Research Division
Electronics and Telecommunications Research Institute
161 Gajeong-Dong, Yuseong-Gu, Daejeon, 305-350, KOREA
Tel. +82-42-860-5432, Fax.: +82-42-860-5611
e-mail : yhham@etri.re.kr, cbh@etri.re.kr

Abstract: The importance of security in WLAN(Wireless LAN) service is very critical, so IEEE organization has made the IEEE 802.1x standard. The IEEE 802.1x standard uses the EAP as authentication protocol which requires AAA(Authentication, authorization, and Accounting) server for authentication & accounting. For the reliable and scalable AAA service, the Diameter protocol has more advanced characteristics than existing radius protocol. So the Diameter protocol can be used for WLAN service provider who has large scale WLAN system and a large number of subscriber. This paper proposes the design of Diameter AAA server for the authentication and accounting of WLAN system which is adopting IEEE 802.1x standard.

1. Introduction

Because people want more stable and high bandwidth wireless internet service, the need for wireless LAN is growing explosively recently. Nowadays many ISP(Internet Service Provider) are going to service the wireless LAN. The security problem in WLAN service is very critical, so IEEE organization has made the IEEE 802.1x standard. The IEEE 802.1x standard defines the port based access control method, and uses the EAP(Extensible Authentication Protocol) as an authentication protocol. The radius protocol has been used world-widely by many ISP and corporations, but has many limit in scalability and security aspect for supporting current rapidly increasing network environment.

This paper proposes the design of Diameter AAA server for the authentication and accounting of WLAN system which is adapting IEEE 802.1x standard. The proposed Diameter system is mainly focused on Diameter base protocol which provides an AAA framework for applications such as network access or IP mobility. The WLAN system generally consists of the WLAN terminal(i.e. note book, pda, computer with wireless land card), ap(access point) and authentication server. This paper shows the interaction with these three components, and describes the each component about the function and adoption of diameter protocol.

2. The Structure of Diameter System

2.1 Diameter protocol requirements

The Diameter protocol allows peers to exchange a variety of messages. The Diameter base protocol provides the minimum requirements needed for an AAA transport protocol which is used by Diameter applications, such as NASREQ, Mobile IP, and CMS. The base protocol provides the following facilities for the applications.

- Delivery of AVP
  : All data delivered by the protocol is in the form of AVP Some AVPs are used by base protocol, and others are used by the application. For the purpose of delivery of such AVP base protocol manages the peer connection between Diameter peer. Also it supports the relaying, proxying and redirecting of Diameter message.

- Capability negotiation
  : When Diameter peers are connected to each other, they exchange the capability information ,such as protocol version, extenson list by the CER/CEA(Capability Exchange Reqeust/Answer).

- Error notification
  : When the error happen in the receiving server, it send the Hop-by-Hop .error notificiation to the peer or End-to-End error notification to the message-originating end server.

- Handling of user session and accounting
  : For the application's session management and the accounting of the service user, the Diameter server provides the management of user session and user accounting.

- Transport failure detection
  : As system can discover the failure of the transport layer as soon as possible, so it reduce the cost of recover and messages which are discarded. By using the DWR/DWA(Device-Watchdog-Request/Answer) system can check the error state of the peer Diameter server.

2.2 The structure of Diameter System

We proposed the block diagram for Diameter base protocol and application. The proposed Diameter block diagram consists of 7 main modules of block, each block is necessary for the operation of base protocol. The modules are main controller, message handler, agent manager, peer manager, session manager, accounting manager and applications.

The following picture shows the architecture of the proposed system and the arrow between the block indicates the flow of Diameter message & event. The system requires two data bases which are used for accounting & user authentication, and also requires three information table(peer, session and routing table) which are necessary for the function of Peer Manager, Session Manager and Agent Manager[8,9,10].

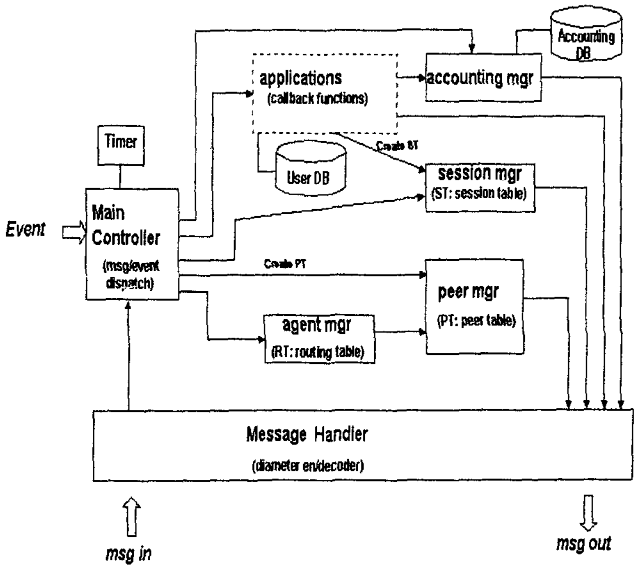

Figure 1. Diameter system block diagram

The functions of each block are as follows.

- Main Controller
  - event/communication dispatcher function
  - event & time management
  - application callback function invocation

- Message Handler
  - Diameter base message header decoding & handler
  - Diameter message scheduler (message queue management)
  - application message encoding/decoding function

- Agent Manager
  - manage and perform 4 different agent function
  - realm based routing table management
  - reference function on peer table
  - message forwarding by routing table

- Peer Manager
  - manage the Peer State Machine
  - maintain the peer table
  - encode/decode the peer related message(CER/CEA, DWR/DWA, DPR/DPA)

- Session Manager
  - manage the Session State Machine
  - end-to-end session state maintenance by session table
  - session establishment for the application
  - manage the session stop, termination

- Accounting Manager
  - accounting state machine management
  - accounting related message (ACR/ACA) en/decoding
  - store the accounting information to the DB
  - send accounting DB data to the backend billing server

- Applications
  - real program which executed on the Diameter base protocol
  - application message processing (NASREQ, Mobile IP, CMS message)
  - uses callback API framework

The proposed system can provide the framework for diameter application and it can manage each state machine(Session State, Peer State, Accounting State and Application State Machine), table and timer for the performing of Diameter protocol operation. The Peer Manager, Session Manager and Accounting Manager need timer which produces event periodically for each finite state machine.

The Agent manager, Peer Manager and Session Manager also need information table(routing table, peer table, session table). They maintain necessary state information & related information in the table and update it whenever state transition occurs. The table 1 shows the each information table's component, manager and description.

Table 1. Diameter information table

	Peer Table	Session Table	Routing Table
Component	Peer host id, State, Static/Dynamic, expiration time, TLS enabled	Session id, session state	Realm name, application id, local action, Server id Static/Dynamic expiration time
Manager	Peer Manager	Session Manager	Agent Manager
Description	Peer connection related info.	Session related info.	Routing related info.

2.3 The Diameter Message Sequence between Diameter peers

The Main Controller module parses the message header, and dispatch the message to the appropriate module. Also the controller dispatches the event and timer event. By the way of analyzing the sequence diagram of message, the role and action of each module can be understood more comprehensively. Especially we will focus on the peer connection establishment and session establishment by application.

Firstly sequence diagram on peer connection establishment is as follows.

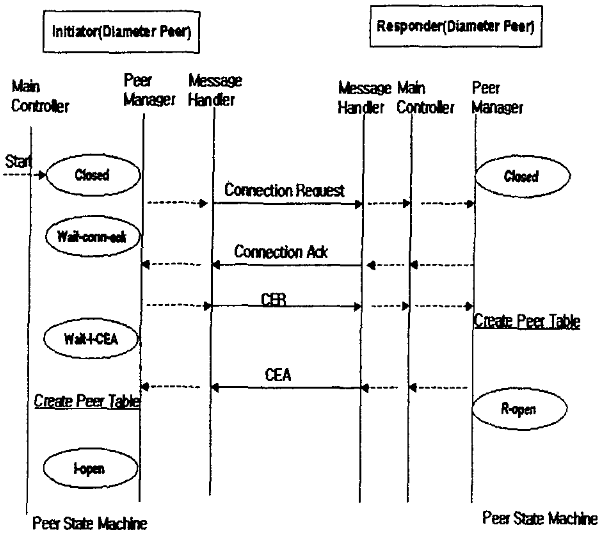

Figure 2. Diameter Connection Establishment

The peer connection establishment is mainly controlled by the Peer Manager. The Main Controller starts the connection request, and the Message Handler encodes & decodes the connection establishment related Diameter message.

The sequence diagram on session establishment is as follows.

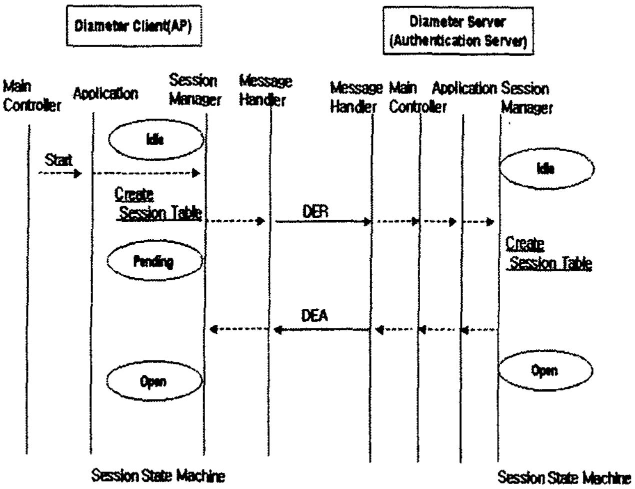

Figure 3. Diameter Session Establishment

The Session Manager controls the session establishment. But there is no session-initiation Diameter message, the session is initiated only when the Applications start. When the any Diameter application starts, the Session Manager creates the session table and session state machine.

3. The Diameter system for WLAN with 802.1x

The WLAN authentication system with IEEE 802.1x standard consists of supplicant(wireless terminal), authenticator(AP), authentication server. The authenticator and authentication server support Diameter protocol to use Diameter authentication & accounting.

The supplicant requests authentication to the AP, and AP relay the requests to the authentication server. The AP plays a role as Diameter client, and authentication server plays a role as Diameter server. But the Diameter client can process the server-initiated request, such as re-auth request because basically Diameter protocol is a peer-to-peer protocol. The protocol stack of each entity(supplicant, authenticator AP, authentication server) is as follows.

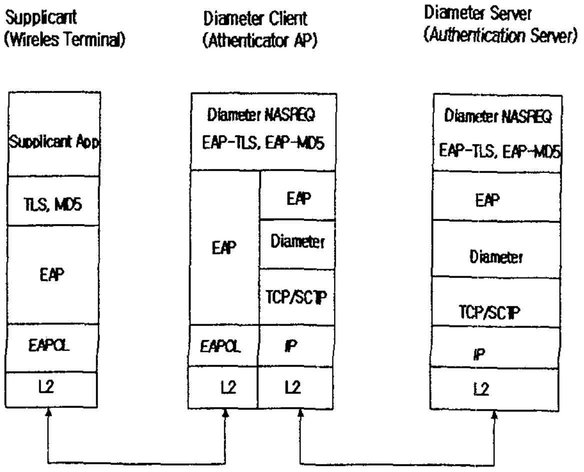
Supplicant (Wireles Terminal)
Diameter Client (Athenticator AP)
Diameter Server (Authentication Server)
Supplicant App
TLS, MD5
EAP
EAPOL
L2
Diameter NASREQ EAP-TLS, EAP-MD5
EAP
EAP
Diameter
TCP/SCTP
EAPOL
IP
L2
L2
Diameter NASREQ EAP-TLS, EAP-MD5
EAP
Diameter
TCP/SCTP
IP
L2

Figure 4. Protocol Stack in WLAN system with Diameter

The protocol operation of IEEE 802.1x is comparatively simple. Firstly the supplicant send EAP-start message to the authenticator AP. Then the authenticator AP requests subscriber ID information to the supplicant. The subscriber ID must have the form of NAI(Network Access Identifier), such as user@realm. This NAI is necessary for subscriber global authentication & accounting. If the "realm" of the NAI is not matched with the domain of Diameter server, then the message is routed to the appropriate home Diameter server by the agent manager of current Diameter server. The supplicant's eap message is encapsulated into eap attribute of DER message. Then the DER message is transferred to the authentication server(Diameter server). When the authentication succeeds, the authentication server send the DER message to the authenticator with Result-Code attribute whose value is "success". It is the end of the IEEE 802.1x authentication with Diameter server.

When the Diameter NASREQ application uses EAP-MD5 as an authentication algorithm, the message sequence diagram is as follows.

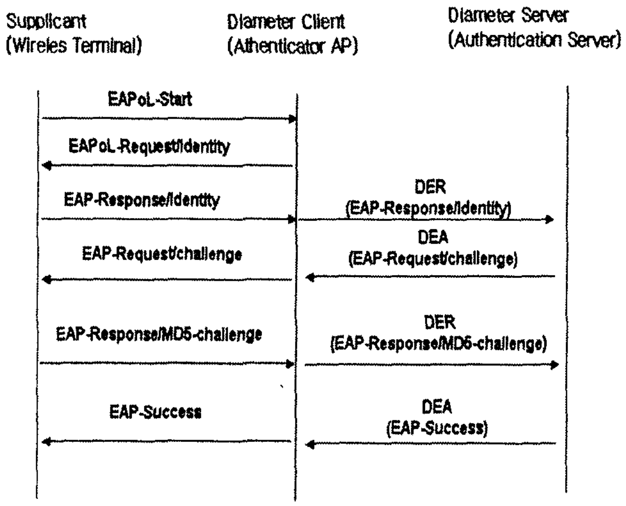

Figure 6. Message Sequence in WLAN system with Diameter

4. Conclusions

We have proposed the AAA server system for the support of secure authentication and accounting of WLAN system which includes the 802.1x supplicant and authenticator. Because the proposed AAA server can provide EAP authentication method which was defined in IEEE 802.1x standard, it can be used with the WLAN systems which support 802.1x standard.

We adapted the Diameter protocol for the AAA service, the design of the proposed system mainly focused on Diameter base protocol because it provides the framework for the Diameter applications. The proposed structure of the Diameter server follows the Diameter-related standard and provides the common API for Diameter server and client for the WLAN service. The proposed Diameter server system can be used in any other network access authentication & accounting. We are going implement the proposed system in the near future on WLAN test network.

References

[1] IEEE 802.1 Working Group, "Port-Based network Access Control", *IEEE Std 802.1X-2001*, June 2001.

[2] L. Blunk, J. Vollbrecht, "PPP Extensible Authentication Protocol (EAP)", *RFC 2284*, March 1998

[3] C.Rigney, S.Willens, A. Rubbens, "Remote Authentication Dial In User Service(RADIUS)", *RFC 2865* March 1998

[4] Pat R. Calhoun, Jari Arkko, Erik Guttman, Glen Zorn, "Diameter Base Protocol", *Draft-ieft-aaa-diameter-10.txt,* April 2002

[5] Pat R. Calhoun, William Bulley, Allan C. Rubbens, "Diameter NASREQ Application", *Draft-ietf-aaa-diameter-nasreq-09.txt,* March 2002

[6] Pat R. Calhoun, Tony Johansson, Charles E. Perkins, "Diameter Mobile IPv4 Application", *Draft-ietf-aaa-diameter-mobileip-10.txt,* April 2002

[7] Pat R. Calhoun, Stephen Farrel, William Bulley, "Diameter CMS Security Application", *Draft-ietf-aaa-diameter-cms-sec-04.txt,* March 2002

[8] C. Metz, "AAA Protocols: Authentication, Authorization, and Accounting for the Internet", *IEEE Internet Computing, November-December*, 1999

[9] C.Perkins, "Mobile IP Joins Forces with AAA", *IEEE Personal Communications,* August 2000

[10] J.Macker, V.Park, M. Corson, "Mobile and Wireless Internet Services: Putting the pieces Together", *IEEE Communications Magazine,* June 2001