Path Authorization Technique in Diameter Base Protocol

Hui-Jong Yu* and Hyun-Gon Kim**
* AAA System team, ETRI, Korea
Tel : +82-42-860-5382 Fax : +82-42-860-5611 E-mail: anny5@etri.re.kr
** AAA System team, ETRI, Korea
Tel : +82-42-860-5428 Fax : +82-42-860-5611 E-mail: hyungonkim@ etri.re.kr

Abstract
Diameter base protocol is intended to provide an AAA framework for applications such as IP mobility. Currently Diameter base protocol is standardized to RFC 3588, but there are some problems. One of them, path authorization is already argued at IETF WG Mailing List. According to RFC 3588, path authorization function causes inefficient data traffic and conflicts with RFC 3588 itself. In this paper, we analysis these problems about path authorization function and propose more improved solution.

1. INTRODUCTION

Authentication, Authorization and Accounting (AAA) protocols such as TACACS [7] and RADIUS were initially deployed to provide dial-up PPP [8] and terminal server access. Over time, with the growth of the Internet and the introduction of new access technologies, including wireless, DSL, Mobile IP and Ethernet, routers and network access servers (NAS) have increased in complexity and density, putting new demands on AAA protocols. Network access requirements for AAA protocols are summarized in [6]. These include Failover, Transmission-level security, Reliable transport, Agent support, Server-initiated messages, Transition support, Capability negotiation, Peer discovery and configuration, Roaming support.

In the decade since AAA protocols were first introduced, the capabilities of NAS devices have increased substantially. As a result, while Diameter is a considerably more sophisticated protocol than RADIUS, it remains feasible to implement within embedded devices, given improvements in processor speeds and the widespread availability of embedded IPsec and TLS implementations. Currently, some parts of Diameter standardization are just completed and other parts are going on. Diameter gives various services through Diameter Base Protocol and many Applications as follows.

o Diameter Base Protocol[1]
o Diameter Credit Control Application[2]
o Diameter NASREQ(Network Access Server REQiurement) Application[3]
o Diameter Mobile IP Application[4]
o Diameter EAP Application[5]

The Diameter base protocol provides many facilities as Delivery of AVPs (attribute value pairs), Capabilities negotiation, Error notification, Extensibility, through addition of new commands and AVPs (required in [6]), Basic services necessary for applications, such as handling of user sessions or accounting.

In this paper, we discuss Path Authorization, analysis its problems and solve them.

2. DIAMETER PATH AUTHORIZATION

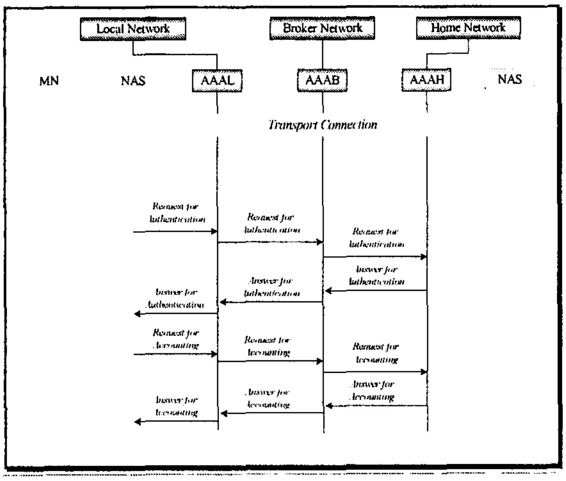

Fig. 1. Diameter Protocol

Figure 1 shows authentications, authorization and accounting of user (MN: Mobile Node) move to local network. MN can be a user of Diameter Mobile IP application or Diameter EAP application. In this paper, we use this environment. MN accesses to NAS for authentication by Home AAA server (AAAH) in local network. NAS operating as Diameter client sends authentication request message to Local AAA server (AAAL). This message is forwarded to AAAH through Broker AAA server (AAAB) in broker network. AAAH processes this message and return authentication response message to NAS through AAAB and AAAL. If NAS confirms authentication success, NAS opens accounting session and exchange accounting messages with AAAH. Path authorization is to check Route-Record AVPs to make sure that the route traversed by the message is acceptable. Route-Record AVP contains host information the message passed. Path authorization can be applied to every Diameter message and operates as follows.

- Path authorization at AAAH

AAAH, prior to authorizing a session, MUST check the Route-Record AVPs to make sure that the route traversed by the request is acceptable. For example, administrators within the home realm may not wish to honor requests that have been routed through an untrusted realm. By authorizing a request, the AAAH is implicitly indicating its willingness to engage in the business transaction as specified by the contractual relationship between the server and the previous hop. A DIAMETER_AUTHORIZATION_REJECTED error message is sent if the route traversed by the request is unacceptable.

- Path authorization at AAAL

AAAL, on receiving a Diameter response authorizing a session, must check the Route-Record AVPs to make sure that the route traversed by the response is acceptable. At each step, forwarding of an authorization response is considered evidence of a willingness to take on financial risk relative to the session. AAAL may wish to limit this exposure, for example, by establishing credit limits for intermediate realms and refusing to accept responses that would violate those limits. By issuing an accounting request corresponding to the authorization response, the local realm implicitly indicates its agreement to provide the service indicated in the authorization response. If the AAAL cannot provide the service, then a DIAMETER_UNABLE_TO_COMPLY error message must be sent within the accounting request. A NAS receiving an authorization response for a service that it cannot perform must not substitute an alternate service, and then send accounting requests for the alternate service instead.

3. PATH AUTHORIZATION PROBLEMS AND SOLUTIONS

3.1. Path authorization Problems

- Path authorization at AAAH

Though the path authorization of authentication request message fails by AAAH, AAAL may retry of authentication request message through the same path because AAAL can't know the failure of path authorization. It is caused from using same error code of path authorization failure and other failure reasons. DIAMETER_AUTHORIZATION_REJECTED is returned when service requested is not permitted to the user. In this case, several authentication request messages and authentication response messages can be exchanged uselessly.

- Path authorization at AAAL

This case is more complex, and raises contradiction in Diameter protocol. First, Result-Code AVP is contained in accounting request message if path authorization is conducted. Currently, RFC 3588 specifies every request message don't contain Result-Code AVP. It is very awkward that request message carries Result-Code AVP. Second, though every authentication request message is exchanged and AAAH authenticates the user successfully, the session is failed at AAAL. So, AAAL sends accounting request message. Accounting messages normally are created after user session starts. It is also very odd that accounting messages are exchanged without user session. Third, if AAAL failed to verify path authorization, there are no ways to inform that to NAS. Because accounting request message is created at NAS, AAAL must inform the failure of path authorization to NAS when successful authentication response message is received. But RFC 3588 does not specify any method about this.

3.2 Improved Path Authorization

- Improved path authorization at AAAH

We define new error code for path authorization. Path authorization failure can be solved if AAAL send authentication request message through other path. Therefore the new error code can be classified into Transient Failures. According to RFC 3588, Transient Failures are identified by fourth thousands digit in the decimal notation (4xxx). Currently, there are three Transient Failures. So, we define as follows.

DIAMETER_PATH_AUTHORIZATION_FAILURE 4004

AAAH, prior to authorizing a session, check the Route-Record AVPs to make sure that the route traversed by the request is acceptable. If it fails, A DIAMETER_PATH_AUTHORIZATION_FAILURE error message is sent if the route traversed by the request is unacceptable.

If AAAL receives this authentication response message, re-sends authentication request message through other path without informing NAS of the failure.

- Improved Path authorization at AAAL

There are some considerations to solve the problems about path authorization at AAAL as follows.

° It is desirable that request message do not contain Result-Code AVP.

° It is proper that accounting request message without normal user session is not created.

° It is reasonable that NAS operates regardless of path authorization.

We propose improved path authorization applies these considerations in this paper. Also, this path authorization can solve problems in Path authorization at AAAH at once.

We define new AVP. This AVP is of type grouped and contains host or realm name not acceptable at AAAL.

Unvalid-Path AVP
(AVP Code – defined in each Application)

AAAL send authentication request message within Unvalid-Path AVP. Diameter broker nodes receive Diameter message usually add or check Route-Record AVP and decide routing path. Now Diameter broker nodes must check not only Route-Record AVP but also Unvalid-Path AVP. They decide routing path that the message is not forwarded to the realms or hosts in Unvalid-Path AVP. Therefore there is no accounting request message caused by path authorization failure. It means also that request message do not contain Result-Code AVP and NAS can operate independently to path authorization. Figure 2 shows our path authorization.

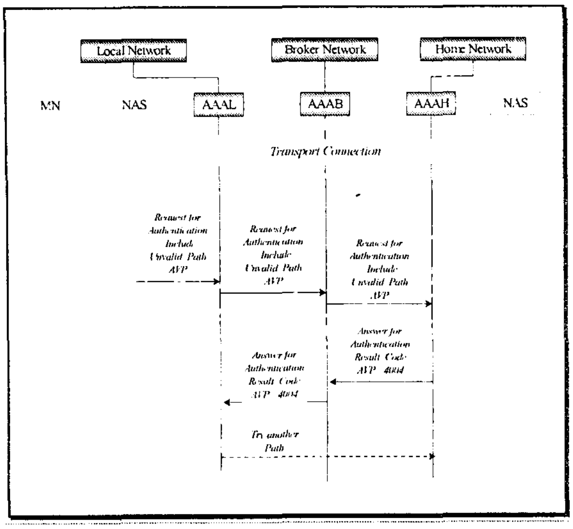
Local Network
Broker Network
Home Network
MN
NAS
AAAL
AAAB
AAAH
NAS
Transport Connection
Request for Authentication Include Unvalid Path AVP
Request for Authentication Include Unvalid Path AVP
Request for Authentication Include Unvalid Path AVP
Answer for Authentication Result Code AVP 4004
Answer for Authentication Result Code AVP 4004
Try another Path

Fig. 2. Improved Path authorization at AAAH

This AVP can be contained in authentication request message. AAAH can inform AAAL of unacceptable path in AAAH by using Unvalid-Path AVP. This method is more efficient than definition of new Result-Code AVP value because AAAL can know unacceptable path in AAAH certainly.

4. CONCLUSION

Diameter protocol can provide user authentication, authorization and accounting service in various applications. Diameter base protocol make Diameter protocol possible these services by several functions. Diameter base protocol provides many facilities as Delivery of AVPs, Capabilities negotiation, Error notification, Extensibility, through addition of new commands and AVPs, Basic services necessary for applications, such as handling of user sessions or accounting.

Diameter base protocol was specified as RFC 3588 in September 2003, but there still remains to discuss. The problems make other functions inefficiently and protocol contradictorily. Path authorization is one of such considerations.

In this paper, we suggested more efficient and improved path authorization. Proposed protocol can make more robust system. In real, our protocol can be applied to commercial service for stable and fast service.

References

[1] Diameter Base Protocol, RFC 3588, September 2003

[2] Diameter Credit-Control Application, draft-ietf-aaa-diameter-cc-03.txt, February 2004

[3] Diameter Network Access Server Application, draft-ietf-aaa-diameter-nasreq-14.txt, February 2004

[4] Diameter Mobile IPv6 Application, draft-le-aaa-diameter-mobileipv6-03.txt, April 2003

[5] Diameter Extensible Authentication Protocol Application, draft-ietf-aaa-eap-02.txt, June 2003

[6] Aboba, B., Calhoun, P., Glass, S., Hiller, T., McCann, P., Shiino, H., Zorn, G., Dommety, G., Perkins, C., Patil, B., Mitton, D., Manning, S., Beadles, M., Walsh, P., Chen, X., Sivalingham, S., Hameed, A., Munson, M., Jacobs, S., Lim, B., Hirschman, B., Hsu, R., Xu, Y., Campbell, E., Baba, S. and E. Jaques, "Criteria for Evaluating AAA Protocols for Network Access", RFC 2989, November 2000

[7] Finseth, C., "An Access Control Protocol, Sometimes Called TACACS", RFC 1492, July 1993.

[8] Simpson, W., "The Point-to-Point Protocol (PPP)", STD 51, RFC 1661, July 1994