                The Diameter Capabilities Update Application
                   draft-ietf-dime-capablities-update-07

Abstract

   This document defines a new Diameter application and associated
   command codes. The Capabilities Update application is intended to
   allow the dynamic update of certain Diameter peer capabilities while
   the peer-to-peer connection is in the open state.

Table of Contents

1. Introduction

   Capabilities exchange is an important component of the Diameter Base
   Protocol [I-D.ietf-dime-rfc3588bis], allowing peers to exchange
   identities and Diameter capabilities (protocol version number,
   supported Diameter applications, security mechanisms, etc.). As
   defined in RFC 3588, however, the capabilities exchange process takes
   place only once, at the inception of a transport connection between a
   given pair of peers. Therefore, if a peer's capabilities change (due
   to software update, for example), the existing connection(s) must be
   torn down (along with all of the associated user sessions) and
   restarted before the modified capabilities can be advertised.

   This document defines a new Diameter application intended to allow
   the dynamic update of a subset of Diameter peer capabilities over an
   existing connection. Because the Capabilities Update application
   specified herein operates over an existing transport connection,
   modification of certain capabilities is prohibited. Specifically,
   modifying the security mechanism in use is not allowed; if the
   security method used between a pair of peers is changed the affected
   connection MUST be restarted.

2. Specification of Requirements

   The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",
   "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this
   document are to be interpreted as described in RFC 2119 [RFC2119].

3. Diameter Protocol Considerations

   This section details the relationship of the Diameter Capabilities
   Update application to the Diameter Base Protocol.

   This document specifies Diameter Application-ID <TBD1>. Diameter
   nodes conforming to this specification MUST advertise support by
   including the value <TBD1> in the Auth-Application-Id of the
   Capabilities-Exchange-Request (CER) and Capabilities-Exchange-Answer
   (CEA) commands [I-D.ietf-dime-rfc3588bis].

4. Capabilities Update

   When the capabilities of a Diameter node conforming to this
   specification change, it MUST notify all of the nodes with which it
   has an open transport connection and which have also advertised
   support for the Capabilities Update application using the

Capabilities-Update-Request (CUR) message (Section 4.1.1). This
message allows the update of a peer's capabilities (supported
Diameter applications, etc.).

A Diameter node only issues a given command to those peers that have
advertised support for the Diameter application that defines the
command; a Diameter node must cache the supported applications in
order to ensure that unrecognized commands and/or Attribute-Value
Pairs (AVPs) are not unnecessarily sent to a peer.

The receiver of the CUR MUST determine common applications by
computing the intersection of its own set of supported Application Id
against all of the application identifier AVPs (Auth-Application-Id,
Acct-Application-Id and Vendor-Specific- Application-Id) present in
the CUR. The value of the Vendor-Id AVP in the Vendor-Specific-
Application-Id MUST NOT be used during computation.

If the receiver of a CUR does not have any applications in common
with the sender then it MUST return a Capabilities-Update-Answer
(CUA) (Section 4.1.2) with the Result-Code AVP set to
DIAMETER_NO_COMMON_APPLICATION [I-D.ietf-dime-rfc3588bis], and SHOULD
disconnect the transport layer connection; however, if active
sessions are using the connection, peers MAY delay disconnection
until the sessions can be redirected or gracefully terminated. Note
that receiving a CUA from a peer advertising itself as a Relay (see
[I-D.ietf-dime-rfc3588bis], Section 2.4) MUST be interpreted as
having common applications with the peer.

As for CER/CEA messages, the CUR and CUA messages MUST NOT be
proxied, redirected or relayed.

Even though the CUR/CUA messages cannot be proxied, it is still
possible for an upstream agent to receive a message for which there
are no peers available to handle the application that corresponds to
the Command-Code. This could happen if, for example, the peers are
too busy or down. In such instances, the 'E' bit MUST be set in the
answer message with the Result-Code AVP set to
DIAMETER_UNABLE_TO_DELIVER to inform the downstream peer to take
action (e.g., re-routing requests to an alternate peer).

4.1. Command-Code Values

This section defines Command-Code [I-D.ietf-dime-rfc3588bis] values
that MUST be supported by all Diameter implementations conforming to
this specification. The following Command Codes are defined (using
modified ABNF [I-D.ietf-dime-rfc3588bis]) in this document:
Capabilities-Update-Request (CUR, Section 4.1.1) and Capabilities-
Update-Answer (CUA, Section 4.1.2).

4.1.1. Capabilities-Update-Request

   The Capabilities-Update-Request (CUR), indicated by the Command-Code
   set to <CUCC> and the Command Flags' 'R' bit set, is sent to update
   local capabilities. Upon detection of a transport failure, this
   message MUST NOT be sent to an alternate peer.

   When Diameter is run over the Stream Control Transmission Protocol
   [RFC4960], which allows connections to span multiple interfaces and
   multiple IP addresses, the Capabilities-Update-Request message MUST
   contain one Host-IP-Address AVP for each potential IP address that
   may be locally used when transmitting Diameter messages.

   Message Format

      <CUR> ::= < Diameter Header: <CUCC>, REQ >
                   { Origin-Host }
                   { Origin-Realm }
               1* { Host-IP-Address }
                   { Vendor-Id }
                   { Product-Name }
                   [Origin-State-Id]
                 * [Supported-Vendor-Id]
                 * [Auth-Application-Id]
                 * [Acct-Application-Id]
                 * [Vendor-Specific-Application-Id]
                   [Firmware-Revision]
                 * [AVP]

4.1.2. Capabilities-Update-Answer

   The Capabilities-Update-Answer, indicated by the Command-Code set to
   <CUCC> and the Command Flags' 'R' bit cleared, is sent in response to
   a CUR message.

                   Message Format

                   <CUA> ::= < Diameter Header: <CUCC> >
                           { Origin-Host }
                           { Origin-Realm }
                           { Result-Code }
                           [Error-Message]
                         * [AVP]

5. Security Considerations

   The security considerations applicable to the Diameter Base Protocol
   [I-D.ietf-dime-rfc3588bis] are also applicable to this document.

6. IANA Considerations

   This section explains the criteria to be used by the IANA for
   assignment of numbers within namespaces used within this document.

6.1. Application Identifier

   This specification assigns the value <TBD1> from the Application
   Identifiers namespace [I-D.ietf-dime-rfc3588bis]. See Section 3 for
   the assignment of the namespace in this specification.

6.2. Command Codes

   This specification assigns the value <CUCC> from the Command Codes
   namespace [I-D.ietf-dime-rfc3588bis]. See Section 4.1 for the
   assignment of the namespace in this specification.

7. Contributors

   This document is based upon work done by Tina Tsou.

8. Acknowledgements

   Thanks to Sebastien Decugis, Niklas Neumann, Subash Comerica, Lionel
   Morand, Dan Romascanu, Dan Harkins and Ravi for helpful review and
   discussion.

9. References

9.1. Normative References

   [I-D.ietf-dime-rfc3588bis]
              Fajardo, V., Arkko, J., Loughney, J., and G. Zorn,
              "Diameter Base Protocol", draft-ietf-dime-rfc3588bis-25
              (work in progress), September 2010.

   [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
              Requirement Levels", BCP 14, RFC 2119, March 1997.

9.2. Informative References

   [RFC4960] Stewart, R., "Stream Control Transmission Protocol",
              RFC 4960, September 2007.

Authors' Addresses

   Jiao Kang
   Huawei Technologies
   Section B1, Huawei Industrial Base
   Bantian, Longgang District
   Shenzhen 518129
   P.R. China

   Phone: +86 755 2878-6690
   Email: kangjiao@huawei.com

   Glen Zorn
   Network Zen
   227/358 Thanon Sanphawut
   Bang Na, Bangkok 10260
   Thailand

   Phone: +66 (0) 87-040-4617
   Email: gwz@net-zen.net