Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: October 15, 2009

G. Zorn
Network Zen
K. Jiao
Huawei Technologies
April 13, 2009

The Diameter Capabilities Update Application
draft-zorn-dime-capablities-update-01.txt

Status of this Memo

Copyright Notice

Abstract

This document defines a new Diameter application and associated command codes. The Capabilities Update application is intended to allow the dynamic update of 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 [RFC3588], 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 Diameter peer capabilities over an existing connection. Because the Capabilities Update application specified here operates over an existing transport connection, modification of 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.

Discussion of this draft may be directed to the authors.

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 [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 MAY advertise support by including the value of <TBD1> in the Auth-Application-Id of the Capabilities-Exchange-Req and Capabilities-Exchange-Answer commands [RFC3588].

4. Capabilities Update

When the capabilities of a Diameter node conforming to this specification change, it SHOULD notify all of the nodes with which it has an open transport connection using the Capabilities-Update-Req

message (Section 4.1.1). This message allows the update of a peer's identity and its capabilities (protocol version number, supported Diameter applications, etc.).

The receiver only issues commands to its 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 AVPs are not unnecessarily sent to a peer.

The receiver of the Capabilities-Update-Request (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 Capabilities-Update-Req (CUR) message does not have any applications in common with the sender then it MUST return a Capabilities-Update-Answer (CUA) with the Result-Code AVP set to DIAMETER_NO_COMMON_APPLICATION, 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 CUR or CUA from a peer advertising itself as a Relay (see [RFC3588], Section 2.4) MUST be interpreted as having common applications with the peer.

The CUR and CUA messages MUST NOT be proxied, redirected or relayed.

Since the CUR/CUA messages cannot be proxied, it is still possible that an upstream agent receives a message for which it has no available peers to handle the application that corresponds to the Command-Code. In such instances, the 'E' bit is 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 [RFC3588] values that MUST be supported by all Diameter implementations conforming to this specification. The following Command Codes are defined 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 <TBD2> 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 SCTP [RFC2960], 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: TBD2, 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 <TBD3> and the Command Flags' 'R' bit set, is sent in response to a CUR message.

Message Format

```
<CUA> ::= < Diameter Header: TBD3 >
          { Origin-Host }
          { Origin-Realm }
          { Result-Code }
          [ Error-Message ]
         * [ AVP ]
```

5. IANA Considerations

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

5.1. Application Identifier

This specification assigns the value <TBD1> from the Application Identifiers namespace defined in RFC 3588. See section Section 3 for the assignment of the namespace in this specification.

5.2. Command Codes

This specification assigns the values <TBD2> and <TBD3> from the Command Codes namespace defined in RFC 3588. See section Section 4.1 for the assignment of the namespace in this specification.

6. Security Considerations

This document does not introduce any new vulnerabilities into the Diameter protocol.

7. References

7.1. Normative References

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

[RFC3588] Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, "Diameter Base Protocol", RFC 3588, September 2003.

7.2. Informative References

[RFC2960] Stewart, R., Xie, Q., Morneault, K., Sharp, C., Schwarzbauer, H., Taylor, T., Rytina, I., Kalla, M., Zhang, L., and V. Paxson, "Stream Control Transmission Protocol", RFC 2960, October 2000.

Authors' Addresses

Glen Zorn
Network Zen
1310 East Thomas Street
#306
Seattle, Washington 98102
USA

Phone: +1 (206) 377-9035
Email: gwz@net-zen.net

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

Phone: +86 755 28786690
Email: kangjiao@huawei.com