Diameter Maintenance and Extensions (DIME)	M. Jones
Internet-Draft	Bridgewater Systems
Updates: 3588 (if approved)	J. Korhonen
Intended status: Standards Track	Nokia Siemens Networks
Expires: February 04, 2012	L. Morand
	Orange Labs
	August 03, 2011

Diameter S-NAPTR Usage
draft-ietf-dime-extended-naptr-09

Abstract

The Diameter base protocol specifies mechanisms whereby a given realm may advertise Diameter nodes and the supported transport protocol. However, these mechanisms do not reveal the Diameter applications that each node supports. A peer outside the realm would have to perform a Diameter capability exchange with every node until it discovers one that supports the required application. This document updates RFC3588 "Diameter Base Protocol" and describes an improvement using an extended format for the Straightforward-Naming Authority Pointer (S-NAPTR) Application Service Tag that allows for discovery of the supported applications without doing Diameter capability exchange beforehand.

Requirements Language

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].

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction

The Diameter base protocol [RFC3588] specifies three mechanisms for the Diameter peer discovery. One of these involves the Diameter implementation performing a Naming Authority Pointer (NAPTR) query [RFC3403] for a server in a particular realm. These NAPTR records provide a mapping from a domain, to the DNS Service Locator (SRV) record [RFC2782] or A/AAAA record [RFC1035][RFC3596] for contacting a server with the specific transport protocol in the NAPTR services field.
The extended NAPTR usage for Diameter peer discovery defined by this document is based on the Straightforward-NAPTR (S-NAPTR) Dynamic Delegation Discovery System (DDDS) Application defined in [RFC3958]. This document updates the Diameter peer discovery procedure described in Section 11.6 of [RFC3588] and defines S-NAPTR Application Service and Application Protocol Tag values that permit the discovery of Diameter peers that support a specific Diameter application and transport protocol.

2. Terminology

The Diameter base protocol specification (Section 1.4 of [RFC3588]) and the Straightforward-NAPTR (S-NAPTR) DDDS application (section 2.1 in [RFC3958]) define the terminology used in this document.

3. Extended NAPTR Service Field Format

```
service-parms = [ [app-service] *(":" app-protocol)]
app-service   = experimental-service  / iana-registered-service
app-protocol  = experimental-protocol / iana-registered-protocol
experimental-service      = "x-" 1*30ALPHANUMSYM
experimental-protocol     = "x-" 1*30ALPHANUMSYM
iana-registered-service   = ALPHA *31ALPHANUMSYM
iana-registered-protocol  = ALPHA *31ALPHANUMSYM
ALPHA         =  %x41-5A / %x61-7A   ; A-Z / a-z
DIGIT         =  %x30-39 ; 0-9
SYM           =  %x2B / %x2D / %x2E  ; "+" / "-" / "."
ALPHANUMSYM   =  ALPHA / DIGIT / SYM
; The app-service and app-protocol tags are limited to 32
; characters and must start with an alphabetic character.
; The service-parms are considered case-insensitive.
```

The NAPTR Service Field format defined by the S-NAPTR DDDS application in [RFC3958] follows this Augmented Backus-Naur Form (ABNF, [RFC5234]):

```
iana-registered-service =/ aaa-service
aaa-service             = "aaa+ap" appln-id
appln-id                = 1*10DIGIT
                          ; Application identifier expressed as
                          ; a decimal integer without leading
                          ; zeros.
```

This specification refines the "iana-registered-service" tag definition for the discovery of Diameter agents supporting a specific Diameter application as defined below.
The appln-id element is the Application Identifier used to identify a specific Diameter Application. The Diameter Application Identifier is a 32-bit unsigned integer and values are allocated by IANA as defined in [RFC3588].

```
iana-registered-protocol =/ aaa-protocol /
aaa-protocol             = "diameter." aaa-transport
aaa-transport            = "tcp" / "sctp" / "tls.tcp"
```

This specification also refines the "iana-registered-protocol" tag definition for the discovery of Diameter agents supporting a specific Diameter transport protocol as defined below.
The S-NAPTR Application Protocol tags defined by this specification MUST NOT be parsed in any way by the querying application or resolver. The delimiter (".") is present in the tag to improve readability and does not imply a structure or namespace of any kind. The choice of delimiter (".") for the Application Protocol tag follows the format of existing S-NAPTR Application Protocol tag registry entries but this does not imply that that it shares semantics with any other specifications that create registry entries with the same format.
The S-NAPTR Application Service and Protocol tags defined by this specification are unrelated to the IANA Service Name and Transport Protocol Port Number Registry (see [I-D.ietf-tsvwg-iana-ports]).
The maximum length of the NAPTR service field is 256 octets including one octet length field (see Section 4.1 of RFC 3403 and Section 3.3 of [RFC1035]).

3.1. IETF Standard Track Diameter Applications

A Diameter agent MUST be capable of using the extended S-NAPTR Application Service Tag for dynamic discovery of a Diameter agent supporting Standard Track applications. Therefore, every IETF Standard Track Diameter application MUST be associated with a "aaa-service" tag formatted as defined in this specification and allocated in accordance with the IANA policy (see Section 7).
For example, a NAPTR service field value of:

'aaa+ap6:diameter.sctp'

Means that the Diameter node in the SRV or A/AAAA record supports the Diameter Session Initiation Protocol (SIP) Application ('6') and SCTP as the transport protocol.

3.2. Vendor-specific Diameter Applications

S-NAPTR Application Service and Application Protocol Tag values can also be used to discover Diameter peers that support a vendor-specific Diameter application. In this case, the vendor-specific Diameter application MUST be associated with a "aaa-service" tag formatted as defined in this specification and allocated in accordance with the IANA policy (see Section 7).
For example, a NAPTR service field value of:

'aaa+ap16777251:diameter.sctp'

Means that the Diameter node in the SRV or A/AAAA record supports the Diameter 3GPP S6a Application ('16777251') and SCTP as the transport protocol.

4. Backwards Compatibility

Domain Name System (DNS) administrators SHOULD also provision legacy RFC 3588 style NAPTR records [RFC3403] in order to guarantee backwards compatibility with legacy RFC 3588 compliant Diameter peers. If the DNS administrator provisions both extended S-NAPTR records as defined in this specification and legacy RFC 3588 NAPTR records, then the extended S-NAPTR records MUST have higher priority (e.g. lower order and/or preference values) than legacy NAPTR records.

5. Extended NAPTR-based Diameter Peer Discovery

The Diameter Peer Discovery principles are described in Section 5.2 of [RFC3588]. This specification updates the NAPTR query procedure in the Diameter peer discovery mechanism by allowing the querying node to determine which applications are supported by resolved Diameter peers. The extended format NAPTR records provide a mapping from a domain to the SRV record or A/AAAA record for contacting a server supporting a specific transport protocol and Diameter application. The resource record will contain an empty regular expression and a replacement value, which is the SRV record or the A/AAAA record for that particular transport protocol.
The assumption for this mechanism to work is that the DNS administrator of the queried domain has first provisioned the DNS with extended format NAPTR entries. The steps below replace the NAPTR query procedure steps in Section 5.2 of [RFC3588].

a. The Diameter implementation performs a NAPTR query for a server in a particular realm. The Diameter implementation has to know in advance which realm to look for a Diameter agent in and which

Application Identifier it is interested in. For example, the realm could be deduced from the Network Access Identifier (NAI) in the User-Name AVP or extracted from the Destination-Realm AVP.

b. If the returned NAPTR service fields contain entries formatted as "aaa+apX:Y" where "X" indicates the Application Identifier and "Y" indicates the supported transport protocol(s), the target realm supports the extended format for NAPTR-based Diameter peer discovery defined in this document.

If "X" contains the required Application Identifier and "Y" matches a supported transport protocol, the Diameter implementation resolves the "replacement" field entry to a target host using the lookup method appropriate for the "flags" field.

If "X" does not contain the required Application Identifier or "Y" does not match a supported transport protocol, the Diameter implementation abandons the peer discovery.

c. If the returned NAPTR service fields contain entries formatted as "aaa+apX" where "X" indicates the Application Identifier, the target realm supports the extended format for NAPTR-based Diameter peer discovery defined in this document.

If "X" contains the required Application Identifier, the Diameter implementation resolves the "replacement" field entry to a target host using the lookup method appropriate for the "flags" field and attempts to connect using all supported transport protocols following the order specified in section 2.1 of [RFC3588].

If "X" does not contain the required Application Identifier, the Diameter implementation abandons the peer discovery.

d. If the returned NAPTR service fields contain entries formatted as "aaa:X" where "X" indicates the supported transport protocol(s), the target realm supports Diameter but does not support the extended format for NAPTR-based Diameter peer discovery defined in this document.

If "X" matches a supported transport protocol, the Diameter implementation resolves the "replacement" field entry to a target host using the lookup method appropriate for the "flags" field.

e. If the returned NAPTR service fields contain entries formatted as "aaa", the target realm supports Diameter but does not support the extended format for NAPTR-based Diameter peer discovery defined in this document. The Diameter implementation resolves the "replacement" field entry to a target host using the lookup method appropriate for the "flags" field and attempts to connect using all

supported transport protocols following the order specified in section 2.1 of [RFC3588].

f. If the target realm does not support NAPTR-based Diameter peer discovery, the client proceeds with the next peer discovery mechanism described in Section 5.2 of [RFC3588].

5.1. Examples

As an example, consider a client that wishes to discover a Diameter server in the ex1.example.com realm that supports the Credit Control Application. The client performs a NAPTR query for that domain, and the following NAPTR records are returned:

```
;;        order pref flags service   regexp replacement
IN NAPTR  50    50   "s"   "aaa:diameter.sctp" ""
             _diameter._sctp.ex1.example.com
IN NAPTR  50    50   "s"   "aaa+ap1:diameter.sctp" ""
             _diameter._sctp.ex1.example.com
IN NAPTR  50    50   "s"   "aaa+ap4:diameter.sctp" ""
             _diameter._sctp.ex1.example.com
```

This indicates that the server supports NASREQ (ID=1) and Credit Control (ID=4) Applications over SCTP. If the client supports SCTP, it will be used, targeted to a host determined by an SRV lookup of _diameter._sctp.ex1.example.com.
That SRV lookup would return:

```
;;       Priority  Weight  Port    Target
IN SRV   0         1       3868    server1.ex1.example.com
IN SRV   0         2       3868    server2.ex1.example.com
```

As an alternative example, a client that wishes to discover a Diameter server in the ex2.example.com realm that supports the NASREQ application over SCTP. The client performs a NAPTR query for that domain, and the following NAPTR records are returned:

```
;;        order pref flags service   regexp replacement
IN NAPTR  150   50   "a"   "aaa:diameter.stcp"  ""
             server1.ex2.example.com
IN NAPTR  150   50   "a"   "aaa:diameter.tls.tcp"  ""
             server2.ex2.example.com
IN NAPTR  150   50   "a"   "aaa+ap1:diameter.stcp"  ""
             server1.ex2.example.com
IN NAPTR  150   50   "a"   "aaa+ap1:diameter.tls.tcp"  ""
             server2.ex2.example.com
```

This indicates that the server supports NASREQ (ID=1) over SCTP and TLS/TCP via hosts server1.ex2.example.com and server2.ex2.example.com respectively.

6. Usage Guidelines

Diameter is a peer to peer protocol whereas most of the applications that extend the base protocol behave like client/server applications. The role of the peer is not advertised in the NAPTR tags and not even communicated during Diameter capability negotiation (Capabilities-Exchange-Request and Capabilities-Exchange-Answer message exchange). For this reason, NAPTR-based Diameter peer discovery for an application defining client/server roles should only be used by a client to discover servers.

7. IANA Considerations

7.1. IETF Diameter Application Service Tags

IANA is requested to reserve a value of "aaa" for Diameter in the S-NAPTR Application Service Tag registry created by [RFC3958]. IANA is also requested to reserve the following S-NAPTR Application Service Tags for existing IETF Diameter applications in the same registry.

Tag	Diameter Application
aaa+ap1	NASREQ [RFC3588]
aaa+ap2	Mobile IPv4 [RFC4004]
aaa+ap3	Base Accounting [RFC3588]
aaa+ap4	Credit Control [RFC4006]
aaa+ap5	EAP [RFC4072]
aaa+ap6	SIP [RFC4740]
aaa+ap7	Mobile IPv6 IKE [RFC5778]
aaa+ap8	Mobile IPv6 Auth [RFC5778]
aaa+ap9	QoS [RFC5866]
aaa+ap4294967295	Relay [RFC3588]

Future IETF Diameter applications MUST reserve the S-NAPTR Application Service Tag corresponding to the allocated Diameter Application ID as defined in Section 3.

7.2. 3GPP Diameter Application Service Tags

IANA is requested to reserve the following S-NAPTR Application Service Tags for existing 3GPP Diameter applications in the S-NAPTR Application Service Tag registry created by [RFC3958].

Tag	Diameter Application
aaa+ap16777250	3GPP STa [TS29.273]
aaa+ap16777251	3GPP S6a [TS29.272]
aaa+ap16777264	3GPP SWm [TS29.273]
aaa+ap16777267	3GPP S9 [TS29.215]

Future 3GPP Diameter applications can reserve entries in the S-NAPTR Application Service Tag registry created by [RFC3958] which correspond to the allocated Diameter Application IDs as defined in Section 3.

7.3. WiMAX Forum Diameter Application Service Tags

IANA is requested to reserve the following S-NAPTR Application Service Tags for existing WiMAX Forum Diameter applications in the S-NAPTR Application Service Tag registry created by [RFC3958].

Tag	Diameter Application
aaa+ap16777281	WiMAX Network Access Authentication and Authorization Diameter Application (WNAAADA) [WiMAX]
aaa+ap16777282	WiMAX Network Accounting Diameter Application (WNADA) [WiMAX]
aaa+ap16777283	WiMAX MIP4 Diameter Application (WM4DA) [WiMAX]
aaa+ap16777284	WiMAX MIP6 Diameter Application (WM6DA) [WiMAX]
aaa+ap16777285	WiMAX DHCP Diameter Application (WDDA) [WiMAX]
aaa+ap16777286	WiMAX Location Authentication Authorization Diameter Application (WLAADA) [WiMAX]
aaa+ap16777287	WiMAX Policy and Charging Control R3 Policies Diameter Application (WiMAX PCC-R3-P) [WiMAX]
aaa+ap16777288	WiMAX Policy and Charging Control R3 Offline Charging Diameter Application (WiMAX PCC-R3-OFC) [WiMAX]
aaa+ap16777289	WiMAX Policy and Charging Control R3 Offline Charging Prime Diameter Application (WiMAX PCC-R3-OFC-PRIME) [WiMAX]
aaa+ap16777290	WiMAX Policy and Charging Control R3 Online Charging Diameter Application (WiMAX PCC-R3-OC) [WiMAX]

Future WiMAX Forum Diameter applications can reserve entries in the S-NAPTR Application Service Tag registry created by [RFC3958] which correspond to the allocated Diameter Application IDs as defined in Section 3.

7.4. Vendor-Specific Diameter Application Service Tags

Vendor-Specific Diameter Application IDs are allocated by IANA according to the "First Come First Served" policy and do not require an

IETF specification. However, the S-NAPTR Application Service Tag registry created by [RFC3958] defines a registration policy of "Specification Required" with a further stipulation that the "specification" is an RFC (of any category). If a Vendor-Specific Diameter Application requires the functionality defined in this document, an RFC of any category MUST be published which reserves the S-NAPTR Application Service Tag corresponding to the Vendor-Specific Diameter Application ID as defined in Section 3.

7.5. Diameter Application Protocol Tags

IANA is requested to reserve the following S-NAPTR Application Protocol Tags for the Diameter transport protocols in the S-NAPTR Application Protocol Tag registry created by [RFC3958].

Tag	Protocol
diameter.tcp	TCP
diameter.sctp	SCTP
diameter.tls.tcp	TLS/TCP

Future Diameter versions which introduce new transport protocols MUST reserve an appropriate S-NAPTR Application Protocol Tag in the S-NAPTR Application Protocol Tag registry created by [RFC3958].

8. Security Considerations

This document specifies an enhancement to RFC 3588 Diameter base protocol defined NAPTR service field format and also modifications to the NAPTR processing logic defined. The enhancements and modifications are based on the S-NAPTR, which is actually a simplification of the NAPTR, and therefore the same security considerations described in RFC 3588 are applicable to this document. No further extensions are required beyond the security mechanisms offered by RFC 3588. However, a malicious host doing S-NAPTR queries learns applications supported by Diameter agents in a certain realm faster, which might help the malicious host to scan potential targets for an attack more efficiently when some applications have known vulnerabilities.

9. Acknowledgments

We would like to thank Glen Zorn, Avi Lior, Itsuma Tanaka, Sebastien Decugis, Dan Romascanu, Adrian Farrel, David Harrington, Pete Resnick, Robert Sparks, Stephen Farrell, Wesley Eddy, Ralph Droms and Joe Touch and for their comprehensive review comments.

10. Editor's Notes

This section to be removed prior to publication.

This draft updates sections of RFC3588 that are also being updated by RFC3588bis. At the time this draft was started, it was uncertain whether RFC3588bis would be published first. The authors of this draft decided to proceed optimistically assuming this draft would be published first with the understanding that minor updates are required if this is not the case.
The application-neutral aspects of Diameter S-NAPTR usage (e.g "aaa:diameter.sctp") were also contributed to RFC3588bis to ensure that it would be functionally complete if it got published first and this draft would come along later to add the application-specific S-NAPTR entries (e.g."aaa+ap5:diameter.sctp").
Depending on the publication order, the S-NAPTR Application Service Tag registry value of "aaa" and the S-NAPTR Application Protocol Tags values ("diameter.tcp"/"diameter.sctp"/"diameter.tls.tcp") will need to be removed either from this draft or RFC3588bis.

11. References

[RFC2119]	Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
[RFC3403]	Mealling, M., "Dynamic Delegation Discovery System (DDDS) Part Three: The Domain Name System (DNS) Database", RFC 3403, October 2002.
[RFC1035]	Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, November 1987.
[RFC2782]	Gulbrandsen, A., Vixie, P. and L. Esibov, "A DNS RR for specifying the location of services (DNS SRV)", RFC 2782, February 2000.
[RFC3958]	Daigle, L. and A. Newton, "Domain-Based Application Service Location Using SRV RRs and the Dynamic Delegation Discovery Service (DDDS)", RFC 3958, January 2005.
[RFC3588]	Calhoun, P., Loughney, J., Guttman, E., Zorn, G. and J. Arkko, "Diameter Base Protocol", RFC 3588, September 2003.
[RFC4004]	Calhoun, P., Johansson, T., Perkins, C., Hiller, T. and P. McCann, "Diameter Mobile IPv4 Application", RFC 4004, August 2005.
[RFC4006]	Hakala, H., Mattila, L., Koskinen, J-P., Stura, M. and J. Loughney, "Diameter Credit-Control Application", RFC 4006, August 2005.
[RFC4072]	Eronen, P., Hiller, T. and G. Zorn, "Diameter Extensible Authentication Protocol (EAP) Application", RFC 4072, August 2005.
[RFC4740]	Garcia-Martin, M., Belinchon, M., Pallares-Lopez, M., Canales-Valenzuela, C. and K. Tammi, "Diameter Session Initiation Protocol (SIP) Application", RFC 4740, November 2006.

[RFC5778]	Korhonen, J., Tschofenig, H., Bournelle, J., Giaretta, G. and M. Nakhjiri, "Diameter Mobile IPv6: Support for Home Agent to Diameter Server Interaction", RFC 5778, February 2010.
[RFC5866]	Sun, D., McCann, P., Tschofenig, H., Tsou, T., Doria, A. and G. Zorn, "Diameter Quality-of-Service Application", RFC 5866, May 2010.
[RFC3596]	Thomson, S., Huitema, C., Ksinant, V. and M. Souissi, "DNS Extensions to Support IP Version 6", RFC 3596, October 2003.
[RFC5234]	Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, January 2008.
[I-D.ietf-tsvwg-iana-ports]	Cotton, M, Eggert, L, Touch, J, Westerlund, M and S Cheshire, "Internet Assigned Numbers Authority (IANA) Procedures for the Management of the Service Name and Transport Protocol Port Number Registry", Internet-Draft draft-ietf-tsvwg-iana-ports-10, February 2011.
[TS29.272]	3rd Generation Partnership Project, "3GPP TS 29.272; Technical Specification Group Core Network and Terminals; Evolved Packet System; Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) Related Interfaces Based on Diameter Protocol (Release 8) ", .
[TS29.273]	3rd Generation Partnership Project, "3GPP TS 29.273; Technical Specification Group Core Network and Terminals; Evolved Packet System; 3GPP EPS AAA interfaces (Release 8) ", .
[TS29.215]	3rd Generation Partnership Project, "3GPP TS 29.215; Technical Specification Group Core Network and Terminals; Policy and Charging Control (PCC) over S9 reference point; Stage 3 (Release 8) ", .
[WiMAX]	WiMAX Forum, "WiMAX Release 1.5", .

Authors' Addresses

Mark Jones Jones Bridgewater Systems EMail: mark@azu.ca

Jouni Korhonen Korhonen Nokia Siemens Networks EMail: jouni.nospam@gmail.com

Lionel Morand Morand Orange Labs EMail: lionel.morand@orange-ftgroup.com