Abstract

This document describes an extended format for the NAPTR service fields used in dynamic Diameter agent discovery. The extended format allows NAPTR queries to contain Diameter Application-Id information.

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

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on June 12, 2010.

Copyright Notice

Copyright (c) 2009 IETF Trust and the persons identified as the
Table of Contents

1. Introduction .............................................. 4
2. Terminology ............................................. 4
3. Extended NAPTR Service Field ......................... 4
4. Extended NAPTR-based Diameter Peer Discovery ...... 5
5. IANA Considerations ..................................... 7
6. Security Considerations ................................. 7
7. Normative References ................................. 7
Authors’ Addresses ........................................ 8
1. Introduction

The Diameter base protocol [RFC3588] specifies three mechanisms for the Diameter peer discovery. One of these involves the Diameter implementation performing a NAPTR query [RFC3403] for a server in a particular realm. These NAPTR records provide a mapping from a domain, to the SRV record [RFC2782] for contacting a server with the specific transport protocol in the NAPTR services field.

Section 11.6 of RFC 3588 defines the following NAPTR service fields:

<table>
<thead>
<tr>
<th>Services Field</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA+D2T</td>
<td>TCP</td>
</tr>
<tr>
<td>AAA+D2S</td>
<td>SCTP</td>
</tr>
</tbody>
</table>

However, foreseen network topologies require border AAA nodes that will be specialized by Diameter application and the NAPTR service field does not allow a Diameter implementation to determine the application supported by the AAA node. Without this information, a Diameter implementation must connect and perform a capability negotiation with each candidate AAA node. This document addresses this problem by specifying an extended NAPTR service field format that permits discovery of Diameter peers that support a specific Diameter application.

2. Terminology

The Diameter base protocol specification (Section 1.4 of RFC 3588) defines most of the terminology used in this document.

3. Extended NAPTR Service Field

The Extended NAPTR service field ABNF specification for the discovery of Diameter agents supporting a specific Diameter application is show below.
naptr-svc-field = "AAA+D2" < protocol> [ *appln-list ]
protocol = "T" / "S"
   ; "T" for TCP and "S" for SCTP.
appln-list = "+AP:" appln-id [ *( "," appln-id ) ]
   ; Comma separated list of application
   ; identifiers prefixed by "+AP:".
appln-id = *DIGIT
   ; Application identifier expressed as a
   ; decimal integer.

For example, a NAPTR service field value of:

‘AAA+D2S+AP:6’

Means that the Diameter node in the SRV record supports the
Diameter Session Initiation Protocol (SIP) Application (‘6’) and
SCTP as the transport protocol.

‘AAA+D2S+AP:6,1,5,4294967295’

Means that the Diameter node in the SRV record supports the
Diameter Session Initiation Protocol (SIP) Application (‘6’),
NASREQ Application (‘1’), EAP Application (‘5’) and SCTP as the
transport protocol. The Diameter node also provides Relay
functionality (‘4294967295’).

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]). The DNS administrator of some domain SHOULD also
provision base RFC 3588 style NAPTR records in order to guarantee
backwards compatibility with legacy RFC 3588 compliant Diameter
peers. If the DNS administrator provisions both extended NAPTR
records as defined in this specification and legacy RFC 3588 NAPTR
records, then the extended NAPTR records MUST have higher priority
(e.g. lower order and/or preference values) than legacy NAPTR
records.

4. Extended NAPTR-based Diameter Peer Discovery

The basic Diameter Peer Discover principles are described in Section
5.2 of [RFC3588]. This specification extends 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 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 for that particular transport protocol. If the server supports multiple transport protocols, there will be multiple NAPTR records, each with a different Services Field value and potentially different list of supported Diameter applications.

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. The realm could be deduced, for example, from the ‘realm’ in a NAI that a Diameter implementation needed to perform a Diameter operation on.

b. If the returned NAPTR service fields contain entries formatted as "AAA+D2X+AP:Y" where "X" indicates the transport protocol and "Y" is a comma-separated list of Application Identifiers, the target realm supports the extended format for NAPTR-based Diameter peer discovery defined in this document.

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

   If "X" does not match a transport protocol supported by the client or "Y" does not contain the required Application Identifier, the peer discovery is abandoned.

c. If the returned NAPTR service fields contain entries formatted as "AAA+D2X" where "X" indicates the transport protocol, the target realm supports the NAPTR-based Diameter peer discovery defined in [RFC3588].

   If "X" matches a transport protocol supported by the client, the client resolves the "replacement" field entry to a target host using the lookup method appropriate for the "flags" field.
If "X" does not match a transport protocol supported by the client, the peer discovery is abandoned.

d. 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. IANA Considerations

Section 11.6 of [RFC3588] defines a IANA registry for the NAPTR Services Field entries. Although this document does not define a new transport protocol, it is proposed to add the following entries to the existing registry to reflect the extended format of the NAPTR Services Field:

<table>
<thead>
<tr>
<th>Services Field</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA+D2T+AP:x</td>
<td>TCP</td>
</tr>
<tr>
<td>AAA+D2S+AP:x</td>
<td>SCTP</td>
</tr>
</tbody>
</table>

Editor’s Note: IANA is currently missing the registry for the NAPTR Service Fields defined in [RFC3588]. This oversight will need to be resolved for this document to proceed.

6. Security Considerations

This document specifies an enhancement to the NAPTR service field format defined in the Diameter base protocol and 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 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.

7. Normative References


[RFC2782] Gulbrandsen, A., Vixie, P., and L. Esibov, "A DNS RR for specifying the location of services (DNS SRV)", RFC 2782,
February 2000.


Authors’ Addresses

Mark Jones
Bridgewater Systems

Email: mark.jones@bridgewatersystems.com

Jouni Korhonen
Nokia Siemens Networks

Email: jouni.nospam@gmail.com