

ALTO  
Internet-Draft  
Intended status: Experimental  
Expires: January 16, 2014

S. Kiesel  
K. Krause  
University of Stuttgart  
M. Stiemerling  
NEC Europe Ltd.  
July 15, 2013

**Third-Party ALTO Server Discovery (3pdisc)**  
**draft-kist-alto-3pdisc-04**

Abstract

The goal of Application-Layer Traffic Optimization (ALTO) is to provide guidance to applications that have to select one or several hosts from a set of candidates capable of providing a desired resource. ALTO is realized by a client-server protocol. Before an ALTO client can ask for guidance it needs to discover one or more ALTO servers that can provide suitable guidance.

This document specifies a procedure for third-party ALTO server discovery, which can be used if the ALTO client is not co-located with the actual resource consumer, but instead embedded in a third party such as a peer-to-peer tracker.

Technically, the algorithm specified in this document takes one IP address and a U-NAPTR Service Parameter (i.e., "ALTO:http" or "ALTO:https") as parameters. It performs several DNS lookups (for U-NAPTR and SOA resource records) and returns one or more URI(s) of information resources related to that IP address.

Terminology and Requirements Language

This document makes use of the ALTO terminology defined in [RFC 5693](#) [[RFC5693](#)].

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](#)].

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

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."

This Internet-Draft will expire on January 16, 2014.

## Copyright Notice

Copyright (c) 2013 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

<a href="#">1.</a>	Introduction . . . . .	<a href="#">3</a>
<a href="#">2.</a>	Third-party ALTO Server Discovery Procedure Specification . . . . .	<a href="#">4</a>
<a href="#">2.1.</a>	Interface . . . . .	<a href="#">4</a>
<a href="#">2.2.</a>	Basic Principle . . . . .	<a href="#">4</a>
<a href="#">2.3.</a>	Overall Procedure . . . . .	<a href="#">5</a>
<a href="#">2.4.</a>	Specification of Tasks and Conditional Branches . . . . .	<a href="#">6</a>
<a href="#">2.4.1.</a>	T1: Prepare Domain Name for Reverse DNS Lookup . . . . .	<a href="#">7</a>
<a href="#">2.4.2.</a>	T2/B1: U-NAPTR Lookup in Reverse Zone . . . . .	<a href="#">7</a>
<a href="#">2.4.3.</a>	B2/T3/B3: Acquire SOA Record for Reverse Zone . . . . .	<a href="#">8</a>
<a href="#">2.4.4.</a>	T4/B4: U-NAPTR Lookup on SOA-MNAME . . . . .	<a href="#">9</a>
<a href="#">3.</a>	Implementation, Deployment, and Operational Considerations . . . . .	<a href="#">9</a>
<a href="#">3.1.</a>	Considerations for ALTO Clients . . . . .	<a href="#">9</a>
<a href="#">3.1.1.</a>	Resource Consumer Initiated Discovery . . . . .	<a href="#">9</a>
<a href="#">3.1.2.</a>	IPv4/v6 Dual Stack, Multihoming, NAT, and Host Mobility . . . . .	<a href="#">9</a>
<a href="#">3.2.</a>	Deployment Considerations for Network Operators . . . . .	<a href="#">10</a>
<a href="#">3.2.1.</a>	NAPTR in Reverse Tree vs. SOA-based discovery . . . . .	<a href="#">10</a>
<a href="#">3.2.2.</a>	Separation of Interests . . . . .	<a href="#">11</a>



<a href="#">3.3.</a>	Impact on DNS . . . . .	<a href="#">11</a>
<a href="#">3.3.1.</a>	Non-PTR Resource Records in Reverse Tree . . . . .	<a href="#">11</a>
<a href="#">3.3.2.</a>	Usage with DNS Hidden Master Servers . . . . .	<a href="#">11</a>
<a href="#">3.3.3.</a>	Load on the DNS . . . . .	<a href="#">11</a>
<a href="#">4.</a>	Security Considerations . . . . .	<a href="#">12</a>
<a href="#">5.</a>	IANA Considerations . . . . .	<a href="#">12</a>
<a href="#">6.</a>	References . . . . .	<a href="#">12</a>
<a href="#">6.1.</a>	Normative References . . . . .	<a href="#">13</a>
<a href="#">6.2.</a>	Informative References . . . . .	<a href="#">13</a>
<a href="#">Appendix A.</a>	Contributors List and Acknowledgments . . . . .	<a href="#">14</a>
	Authors' Addresses . . . . .	<a href="#">14</a>

## [1.](#) Introduction

The goal of Application-Layer Traffic Optimization (ALTO) is to provide guidance to applications that have to select one or several hosts from a set of candidates capable of providing a desired resource [[RFC5693](#)]. ALTO is realized by a client-server protocol; see requirement AR-1 in [[RFC6708](#)]. Before an ALTO client can ask for guidance it needs to discover one or more ALTO servers that can provide suitable guidance. For applications that use a centralized resource directory, such as tracker-based P2P applications, the efficiency of ALTO is significantly improved if the ALTO client is embedded in said resource directory instead of the resource consumer (see Section 4.1 of [[I-D.ietf-alto-deployments](#)]). The ALTO client embedded into the resource directory asks for guidance on behalf of the resource consumers. To that end, it needs to discover ALTO servers that can give guidance suitable for these resource consumers, respectively. This is called third-party party ALTO server discovery.

This document specifies a procedure for third-party ALTO server discovery. In other words, this document tries to meet requirement AR-33 in [[RFC6708](#)].

The ALTO protocol specification [[I-D.ietf-alto-protocol](#)] is based on HTTP and expects the discovery procedure to yield the HTTP(S) URI of an ALTO server's information resource directory. Therefore, this document specifies an algorithm that takes a resource consumer's IP address as argument, performs several DNS lookups (for U-NAPTR [[RFC4848](#)] and SOA resource records), and produces URIs of ALTO servers that are able to give reasonable ALTO guidance to a resource consumer willing to communicate using this IP address.

To some extent, AR-32, i.e., resource consumer initiated ALTO server discovery, can be seen as a special case of third-party ALTO server discovery. However, the considerations in [Section 3.1.1](#) apply. Note that a less versatile yet simpler approach for resource consumer



initiated ALTO server discovery is specified in [\[I-D.ietf-alto-server-discovery\]](#).

A more detailed discussion of various options where to place the functional entities comprising the overall ALTO architecture can be found in [\[I-D.ietf-alto-deployments\]](#).

Comments and discussions about this memo should be directed to the ALTO working group: [alto@ietf.org](mailto:alto@ietf.org).

## **[2.](#) Third-party ALTO Server Discovery Procedure Specification**

### **[2.1.](#) Interface**

The algorithm specified in this document takes one IP address and a U-NAPTR Service Parameter (i.e., "ALTO:http" or "ALTO:https") as parameters. It performs several DNS lookups (for U-NAPTR and SOA resource records) and returns one or more URI(s) of information resources related to that IP address.

### **[2.2.](#) Basic Principle**

The algorithm sequentially tries two different lookup strategies. First, an ALTO-specific U-NAPTR lookup is performed in the "reverse tree", i.e., in subdomains of in-addr.arpa. or ip6.arpa., respectively. If this lookup does not yield a usable result, the SOA record for the reverse zone is acquired, its master name server (MNAME) value is extracted and used for a further ALTO-specific U-NAPTR lookup.

The goal is to allow deployment scenarios that require fine-grained discovery on a per-IP basis, as well as large-scale scenarios where discovery is to be enabled for a large number of IP addresses with a small number of additional DNS resource records.



### **2.3. Overall Procedure**

This figure gives an overview on the third-party discovery procedure. All tasks (T) and conditional branches (B) are specified below.



```

(-----)
( START 3pdisc with parameters      )
( IP_address IP, Service_Parameter SP )
(-----+-----)
      V
+- T1 -----+-----+
| R:=<IP>.in-addr.arpa. / <IP>.ip6.arpa. |
+-----+-----+
      V
+- T2 -----+-----+
| X:=DNSlookup(R,U-NAPTR,SP)           |
+-----+-----+
      V
/ B1 -----+-----\
/-----< One or more U-NAPTR results in X >
| yes \-----+-----/
|      V no
|      /- B2 -----+-----\
| /----< Authority sect. with SOA record in X >
| | yes \-----+-----/
| |      V no
| | +- T3 -----+-----+
| | | X:=DNSlookup(R,SOA)           |
| | +-----+-----+
| |      V
| | /- B3 -----+-----\
| | < Lookup OK, SOA record present in X >----\
| | \-----+-----/ no
| |      V yes
| | \----->+
| |      V
| | +- T4 -----+-----+
| | | M:=extract MNAME from SOA record in X |
| | | X:=DNSlookup(M,U-NAPTR,SP)           |
| | +-----+-----+
| |      V
| | /- B4 -----+-----\
\--->+<----< One or more U-NAPTR results in X >---->+
| yes \-----+-----/ no
      V
(-----+-----)
( END, result X )
(-----)
(-----+-----)
( END, failure )
(-----)

```

## 2.4. Specification of Tasks and Conditional Branches



As an example, the following two U-NAPTR resource records can be used for mapping "3.100.51.198.in-addr.arpa." to the HTTPS URI <https://altoserver.isp.example.net/secure/directory> or the HTTP URI <http://altoserver.isp.example.net/secure/directory>.



altoserver.isp.example.net/directory, with the former being preferred.

3.100.51.198.in-addr.arpa.

```
IN NAPTR 100 10 "u" "ALTO:https"
    "!.*!https://altoserver.isp.example.net/secure/directory!" ""

IN NAPTR 200 10 "u" "ALTO:http"
    "!.*!http://altoserver.isp.example.net/directory!" ""
```

Conditional Branch B1 checks whether at least one U-NAPTR record matching the service parameter SP could be retrieved. If so, the procedure ends successfully and the sorted list of U-NAPTR records is the result. Otherwise, if no U-NAPTR records could be retrieved, we continue with B2.

Note: The U-NAPTR lookup in Task T2 is identical to Step 2 specified in [[I-D.ietf-alto-server-discovery](#)], which specifies with "manual input" and "DHCP" two alternatives for acquiring the name to be looked up. Therefore, it is possible to merge both documents into a common ALTO server discovery framework.

#### **2.4.3. B2/T3/B3: Acquire SOA Record for Reverse Zone**

The task of B2/T3/B3 is to acquire the SOA record for the "reverse zone", i.e., the zone in the in-addr.arpa. or ip6.arpa. domain that contains the IP address in question.

A sample SOA record could be:

```
100.51.198.in-addr.arpa
IN SOA dns1.isp.example.net. hostmaster.isp.example.net. (
    1          ; Serial
    604800     ; Refresh
    86400      ; Retry
    2419200    ; Expire
    604800 )   ; Negative Cache TTL
```

Conditional Branch B2 checks whether the SOA record was present in the authority section of X, i.e., the result of Task T2. If not, an explicit lookup is done in Task T3. If Conditional Branch B3 determines that this explicit lookup failed, the discovery procedure is aborted without a result; otherwise we continue with T4.



#### **2.4.4. T4/B4: U-NAPTR Lookup on SOA-MNAME**

Now that the SOA record is available, Task T4 first extracts the MNAME field, i.e., the responsible master name server from the SOA record. An example MNAME could be:

dns1.isp.example.net.

Then, a U-NAPTR lookup as specified in Task T2 is performed on this MNAME and the result is stored in variable "X".

Conditional Branch B4 checks whether at least one U-NAPTR record matching the service parameter SP could be retrieved. If so, the procedure ends successfully and the sorted list of U-NAPTR records is the result. Otherwise, if no U-NAPTR records could be retrieved, the discovery procedure is aborted without a result.

### **3. Implementation, Deployment, and Operational Considerations**

#### **3.1. Considerations for ALTO Clients**

##### **3.1.1. Resource Consumer Initiated Discovery**

To some extent, ALTO requirement AR-32 [[RFC6708](#)], i.e., resource consumer initiated ALTO server discovery, can be seen as a special case of third-party ALTO server discovery. To that end, an ALTO client embedded in a resource consumer would have to figure out its own "public" IP address and perform the procedures described in this document on that address. However, due to the widespread deployment of Network Address Translators (NAT), additional protocols and mechanisms such as STUN [[RFC5389](#)] would be needed and considerations for UNSAF [[RFC3424](#)] apply. Therefore, using the procedures specified in this document for resource consumer based ALTO server discovery is generally NOT RECOMMENDED. Note that a less versatile yet simpler approach for resource consumer initiated ALTO server discovery is specified in [[I-D.ietf-alto-server-discovery](#)].

##### **3.1.2. IPv4/v6 Dual Stack, Multihoming, NAT, and Host Mobility**

The algorithm specified in this document can discover ALTO server URIs for a given IP address. The intention is, that a third party (e.g., a resource directory) that receives query messages from a resource consumer can use the source address in these messages to discover suitable ALTO servers for this specific resource consumer.

However, resource consumers (as defined in [Section 2 of \[RFC5693\]](#)) may reside on hosts with more than one IP address, e.g., due to IPv4/





v6 dual stack operation and/or multihoming. IP packets sent with different source addresses may be subject to different routing policies and path costs. In some deployment scenarios, it may even be required to ask different sets of ALTO servers for guidance. Furthermore, source addresses in IP packets may be modified en-route by Network Address Translators (NAT).

If a resource consumer queries a resource directory for candidate resource providers, the locally selected (and possibly en-route translated) source address of the query message - as observed by the resource directory - will become the basis for the ALTO server discovery and the subsequent optimization of the resource directory's reply. If, however, the resource consumer then selects different source addresses to contact returned resource providers, the desired better-than-random "ALTO effect" may not occur.

Therefore, a dual stack or multihomed resource consumer SHOULD either always use the same address for contacting the resource directory and the resource providers, i.e., overriding the operating system's automatic source IP address selection, or use resource consumer based ALTO server discovery [[I-D.ietf-alto-server-discovery](#)] to discover suitable ALTO servers for every local address and then locally perform ALTO-influenced resource consumer selection and source address selection. Similarly, resource consumers on mobile hosts SHOULD query the resource directory again after a change of IP address, in order to get a list of candidate resource providers that is optimized for the new IP address.

### **[3.2.](#) Deployment Considerations for Network Operators**

#### **[3.2.1.](#) NAPTR in Reverse Tree vs. SOA-based discovery**

As already outlined in [Section 2.2](#), the third-party discovery procedure sequentially tries two different lookup strategies, thus giving network operators the choice of two different deployment options:

- o Individual NAPTR records in the in-addr.arpa or ip6.arpa domains allow very fine-grained discovery of ALTO "entry point" URIs on a per-IP-address basis. This method also gives the fastest response times and causes a comparatively low load on the DNS, as the algorithm terminates successfully after the first DNS query. DNS operators that already maintain reverse zones (e.g., for PTR records) should prefer this option, possibly using DNS server implementation-specific methods for mass deployment (e.g., BIND9's \$GENERATE statement).



- o If a DNS operator considers the first option too cumbersome, or if IPv6 privacy extensions is to be used without dynamic PTR updates, setting up SOA records in the in-addr.arpa. or ip6.arpa. subdomains plus setting up corresponding ALTO-specific U-NAPTR records will also give reasonable, yet less fine-grained results at the cost of slightly higher delay and load on the DNS.

### **3.2.2. Separation of Interests**

We assume that if two organizations share parts of their DNS infrastructure, i.e., have a common SOA record in their in-addr.arpa. or ip6.arpa. subdomain(s), they will also be able to operate a common ALTO server, which still may do redirections if desired or required by policies.

Note that the ALTO server discovery procedure is supposed to produce only a first URI of an ALTO server that can give reasonable guidance to the client. An ALTO server can still return different results based on the client's address (or other identifying properties) or redirect the client to another ALTO server using mechanisms of the ALTO protocol (see Sect. 6.7 of [[I-D.ietf-alto-protocol](#)]).

## **3.3. Impact on DNS**

### **3.3.1. Non-PTR Resource Records in Reverse Tree**

Installing NAPTR records, i.e., a record type other than PTR records, in the in-addr.arpa or ip6.arpa domain may seem uncommon, but it is not a new concept. Earlier documents that specify the usage of Non-PTR resource records in the reverse tree include [RFC 4025](#) [[RFC4025](#)], [RFC 4255](#) [[RFC4255](#)], and [RFC 4322](#) [[RFC4322](#)].

### **3.3.2. Usage with DNS Hidden Master Servers**

In some deployment scenarios, the Master DNS server for a in-addr.arpa. or ip6.arpa. subdomain, as indicated in the respective SOA record, may not be reachable due to traffic restrictions ("hidden master"). This does not cause any problems with the algorithm described here, as the MNAME is only used for further DNS lookups; but it is never attempted to contact this server directly.

### **3.3.3. Load on the DNS**

The procedure described in this document features several nested conditional branches, but no loops. Each time being called it attempts one to three DNS lookups.



#### **4. Security Considerations**

A classification of the main security concerns related to ALTO can be found in the ALTO requirements document [[RFC6708](#)].

Using the procedure described in this document, any third party can discover a set of ALTO servers that can give ALTO guidance to a given IP address. However, this is generally not considered a security or privacy concern.

Forged DNS replies (e.g., due to a compromised name server or due to DNS message interception and modification) may cause the discovery algorithm to fail or produce undesirable results:

First, the third-party discovery procedure might not be able to discover an ALTO server, even if a suitable ALTO server exists. In that case, ALTO guidance will not be used. The resulting application performance and traffic distribution will subsequently correspond to a deployment scenario without ALTO guidance.

Second, the discovery procedure may discover a sub-optimal or wrong ALTO server. Such an ALTO server may either not be able to provide information for a given resource consumer, thus rendering the ALTO service useless. Alternatively, the ALTO server may provide suboptimal or forged information. In the latter case, attackers could try to use ALTO to affect the traffic distribution or the performance of applications. Users may then observe performance problems, and network operators could detect traffic anomalies. A potential counter-measure is to disable the use of the ALTO service if such anomalies are detected.

The application of DNS security (DNSSEC) [[RFC4033](#)] provides a means to limit attacks that rely on forging DNS messages. Security considerations specific to U-NAPTR are described in more detail in [[RFC4848](#)].

#### **5. IANA Considerations**

This document does not require any IANA action.

This document specifies an algorithm that uses U-NAPTR lookups [[RFC4848](#)] with the Application Service Tag "ALTO" and the Application Protocol Tags "http" and "https". These tags have already been registered with IANA. In particular, for the registration of the Application Service Tag "ALTO", see [[I-D.ietf-alto-server-discovery](#)].

#### **6. References**



### **6.1. Normative References**

- [RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, [RFC 1035](#), November 1987.
- [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.
- [RFC3596] Thomson, S., Huitema, C., Ksinant, V., and M. Souissi, "DNS Extensions to Support IP Version 6", [RFC 3596](#), October 2003.
- [RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", [RFC 4033](#), March 2005.
- [RFC4848] Daigle, L., "Domain-Based Application Service Location Using URIs and the Dynamic Delegation Discovery Service (DDDS)", [RFC 4848](#), April 2007.

### **6.2. Informative References**

- [I-D.ietf-alto-deployments] Stiemerling, M., Kiesel, S., and S. Previdi, "ALTO Deployment Considerations", [draft-ietf-alto-deployments-06](#) (work in progress), February 2013.
- [I-D.ietf-alto-protocol] Alimi, R., Penno, R., and Y. Yang, "ALTO Protocol", [draft-ietf-alto-protocol-17](#) (work in progress), July 2013.
- [I-D.ietf-alto-server-discovery] Kiesel, S., Stiemerling, M., Schwan, N., Scharf, M., and S. Yongchao, "ALTO Server Discovery", [draft-ietf-alto-server-discovery-08](#) (work in progress), March 2013.
- [RFC3424] Daigle, L. IAB, "IAB Considerations for UNilateral Self-Address Fixing (UNSAF) Across Network Address Translation", [RFC 3424](#), November 2002.
- [RFC4025] Richardson, M., "A Method for Storing IPsec Keying Material in DNS", [RFC 4025](#), March 2005.





- [RFC4255] Schlyter, J. and W. Griffin, "Using DNS to Securely Publish Secure Shell (SSH) Key Fingerprints", [RFC 4255](#), January 2006.
- [RFC4322] Richardson, M. and D. Redelmeier, "Opportunistic Encryption using the Internet Key Exchange (IKE)", [RFC 4322](#), December 2005.
- [RFC5389] Rosenberg, J., Mahy, R., Matthews, P., and D. Wing, "Session Traversal Utilities for NAT (STUN)", [RFC 5389](#), October 2008.
- [RFC5693] Seedorf, J. and E. Burger, "Application-Layer Traffic Optimization (ALTO) Problem Statement", [RFC 5693](#), October 2009.
- [RFC6708] Kiesel, S., Previdi, S., Stiernerling, M., Woundy, R., and Y. Yang, "Application-Layer Traffic Optimization (ALTO) Requirements", [RFC 6708](#), September 2012.

## [Appendix A](#). Contributors List and Acknowledgments

The initial version of this document was co-authored by Marco Tomsu <marco.tomsu@alcatel-lucent.com>.

Hannes Tschofenig provided the initial input to the U-NAPTR solution part. Hannes and Martin Thomson provided excellent feedback and input to the server discovery.

This memo borrows some text from [[I-D.ietf-alto-server-discovery](#)], as the 3pdisc was historically part of that memo. Special thanks to Michael Scharf and Nico Schwan.

### Authors' Addresses

Sebastian Kiesel  
University of Stuttgart Information Center  
Allmandring 30  
Stuttgart 70550  
Germany

Email: [ietf-alto@skiesel.de](mailto:ietf-alto@skiesel.de)

URI: <http://www.rus.uni-stuttgart.de/nks/>



Kilian Krause  
University of Stuttgart Information Center  
Allmandring 30  
Stuttgart 70550  
Germany

Email: [schreibt@normalerweise.net](mailto:schreibt@normalerweise.net)  
URI: <http://www.rus.uni-stuttgart.de/nks/>

Martin Stiernerling  
NEC Laboratories Europe  
Kurfuerstenanlage 36  
Heidelberg 69115  
Germany

Phone: +49 6221 4342 113  
Email: [martin.stiernerling@neclab.eu](mailto:martin.stiernerling@neclab.eu)  
URI: <http://ietf.stiernerling.org>

