ALTO
Internet-Draft
Intended status: Standards Track
Expires: July 21, 2013

S. Kiesel
University of Stuttgart
M. Stiemerling
NEC Europe Ltd.
N. Schwan
Stuttgart, Germany
M. Scharf
Alcatel-Lucent Bell Labs
H. Song
Huawei

January 17, 2013

# ALTO Server Discovery
# draft-ietf-alto-server-discovery-07

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 resource consumer initiated ALTO server discovery, which can be used if the ALTO client is embedded in the resource consumer.

## Terminology and Requirements Language

This document makes use of the ALTO terminology defined in [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



## Copyright Notice

Table of Contents

## 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.

This document specifies a procedure for resource consumer initiated ALTO server discovery, which can be used if the ALTO client is embedded in the resource consumer. In other words, this document tries to meet requirement AR-32 in [RFC6708] while AR-33 is out of scope. A more complex approach, which tries to meet requirement AR-33, i.e., third-party ALTO server discovery, is addressed in [I-D.kist-alto-3pdisc].

The ALTO protocol specification [I-D.ietf-alto-protocol] is based on HTTP and expects the discovery procedure to yield an HTTP(S) URI. Therefore, this procedure is based on U-NAPTR [RFC4848]. It tries to directly find one or more ALTO server(s) that can give suitable guidance to the ALTO client. Other schemes, such as discovering a random ALTO server (which might not be able to give suitable guidance to the client in question) and asking it to redirect the client to a better server, are not considered in this document.

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

## 2. ALTO Server Discovery Procedure Overview

The ALTO server discovery procedure is performed in two steps:

1. A DNS suffix is yielded, either by manual input or by means of DHCP.

2. This DNS suffix is used for an U-NAPTR lookup yielding the URI. Further DNS lookups may be neccessary to determine the ALTO server's IP address(es).

The primary means for retrieving the DNS suffix is DHCP. However, there may be situations where DHCP is not available or does not return a suitable value. Furthermore, there might be situations in which the user whishes to override the value that could be retrieved from DHCP. In these situations, manual input may be used.

Typically, but not neccessarily, the DNS suffix is the domain name in which the client is located, i.e., a PTR lookup on the client's IP address would yield a similar name. However, due to the widespread use of network address translation (NAT), trying to determine the DNS suffix through a PTR lookup on an interface's IP address is not recommended for resource consumer initiated ALTO server discovery.

## 3. ALTO Server Discovery Procedure Specification

As already outlined in Section 2 the ALTO server discovery procedure is performed in two steps, which will be specified in Section 3.1 and Section 3.2, respectively.

### 3.1. Step 1: Retrieving the Domain Name

#### 3.1.1. Step 1, Option 1: User input

A user may want to use a third party ALTO service instance. Therefore we allow the user to specify a DNS suffix on its own, for example in a configuration file option. The DNS suffix given by the user is combined with the IP address of the resource consumer to allow the third party ALTO service to direct the client to a suitable ALTO server based on the location of the client. A possible DNS suffix entered by the user may be:

myaltoprovider.org

In case no ALTO NAPTR records are found, we consider the discovery process based on user input as failed. A client MAY try to continue with DHCP (see below). If DHCP-based discovery succeeds the client SHOULD inform the user that the user input has been ignored and replaced by information retrieved from the network.

#### 3.1.2. Step 1, Option 2: DHCP

As a second option network operators may configure the domain name to be used for service discovery within an access network using DHCP.

RFC 5986 [RFC5986] defines DHCP IPv4 and IPv6 access network domain name options that identify a domain name that is suitable for service discovery within the access network. RFC 2132 [RFC2132] defines the DHCP IPv4 domain name option. While this option is less suitable, it still may be useful if the RFC 5986 option is not available.

For IPv6, the ALTO server discovery procedure MUST try to retrieve DHCP option 57 (OPTION_V6_ACCESS_DOMAIN). If no such option can be retrieved the procedure fails. For IPv4, the ALTO server discovery procedure MUST try to retrieve DHCP option 213 (OPTION_V4_ACCESS_DOMAIN). If no such option can be retrieved, the procedure SHOULD try to retrieve option 15 (Domain Name). If neither option can be retrieved the procedure fails.

If a result can be retrieved it will be used as an input for the next step (U-NAPTR resolution). One example could be:

```
myisp.com
```

### 3.2. Step 2: U-NAPTR Resolution

The ALTO protocol specification [I-D.ietf-alto-protocol] expects that the ALTO discovery procedure yields the HTTP(S) URI of the ALTO server's Information Resource Directory, which gives further information about the capabilities and services provided by that ALTO server. The first step of the ALTO server discovery procedure (see Section 3.1) yielded an U-NAPTR/DDDS (URI-Enabled NAPTR/Dynamic Delegation Discovery Service) [RFC4848] application unique strings, in the form of a DNS name. An example is "example.com".

In the second step, the ALTO Server discovery procedure needs to use the U-NAPTR [RFC4848] specification described below to obtain a URI (indicating host and protocol) for the ALTO server's Information Resource Directory. In this document, only the HTTP and HTTPS URL schemes are defined, as the ALTO protocol specification defines the access over both protocols, but no other [I-D.ietf-alto-protocol]. Note that the HTTP URL can be any valid HTTP(s) URL, including those containing path elements.

The following two DNS entries show the U-NAPTR resolution for "example.com" to the HTTPS URL https://altoserver.example.com/secure/directory or the HTTP URL http://altoserver.example.com/directory, with the former being preferred.

```
example.com.

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

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

There is a potential that retrieving the domain name or the U-NAPTR lookup itself does not yield to a result, i.e. no ALTO NAPTR record is found. In this case the discovery procedure failed for this interface. It is RECOMMENDED that clients give up the discovery process and wait a period of time before repeating the procedure. Clients MAY repeat the discovery procedure for a different interface instantaneously.

# 4. Deployment Considerations

## 4.1. Issues with Home Gateways

Section 3.1.2 describes the usage of a DHCP option. It enables the network operator of the network, in which the ALTO client is located, to provide a DNS suffix. However, this assumes that this particular DHCP option is correctly passed from the DHCP server to the actual host with the ALTO client, and that the particular host understands this DHCP option. This memo assumes the client to be able to understand the proposed DHCP option, otherwise there is no further use of the DHCP option, but the client has to use the other proposed mechanisms.

There are well-known issues with the handling of DHCP options in home gateways. One issue is that unknown DHCP options are not passed through some home gateways, effectively eliminating the DHCP option.

Another well-known issues is the usage of home gateway specific DNS suffixes which "override" the DNS suffix provided by the network operator. For instance, a host behind a home gateway may receive a DNS suffix ".local" instead of "example.com". In general, this suffix is not usable for the server discovery procedure, unless a DNS server in the home gateway resolves the corresponding NAPTR lookup correctly, e.g., by means of a DNS split horizon approach.

In general, the ALTO server discovery SHOULD be based on the IP address that is used to communicate with other peers, i. e., it should return a server that can provide guidance for that address.

## 4.2. Issues with Multihoming, Mobility and Changing IP Addresses

If the user decides to enter the DNS suffix manually, only one set of ALTO servers will be discovered, irrespectively of multihoming and mobilility. Particularly in mobile scenarios this can lead to undesirable results.

The DHCP-based discovery method can discover different sets of ALTO servers for each interface and address familly (i.e., IPv4/v6). In general, if a client wishes to communicate using one of its interfaces and using a specific IP address familiy, it SHOULD ask the ALTO server(s) for guidance that have been discovered for this specific interface and address family. Selecting an interface and IP address family, as well as comparing results returned from different ALTO servers, is out of the scope of this document.

A change of the IP address at an interface invalidates the result of the ALTO server discovery procedure. For instance, if the IP address

assigned to a mobile host changes due to host mobility, it is required to re-run the ALTO server discovery procedure without relying on earlier gained information.

There are several challenges with DNS on hosts with multiple interfaces [RFC6418], which can affect the ALTO server discovery. If the DNS resolution is performed on the wrong interface, it can return an ALTO server that could provide sub-optimal or wrong guidance. Finding the best ALTO server for multi-interfaced hosts is outside the scope of this document.

When using Virtual Private Network (VPN) connections there is usually no DHCP. The user has to enter the DNS suffix manually. For good optimization results, a DNS suffix corresponding to the VPN concentrator, not corrsponding to the user's current location, has to be entered. Similar considerations apply for Mobile IP.

## 5. IANA Considerations

IANA is requested to register the following U-NAPTR application service tag:

Application Service Tag: ALTO

Intended usage: 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.

Defining Publication: The specification contained within this document.

Contact information: The authors of this document

Author/Change controller: The IESG

# 6. Security Considerations

## 6.1. General

There are two different failures for the ALTO server discovery, which can both be caused by malicious attacks or by configuration problems, e.g., in case of DNS configuration errors or multi-homed hosts.

First, the discovery 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 correspond to a deployment scenario without ALTO guidance. But given that users cannot rely on the availability of an ALTO server, this results in no significant additional security risk.

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 (e.g., behind a NAT), thus rendering the ALTO service useless. Alternatively, it may provide sub-optimal 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 anormalities. A potential counter-measure is to disable the use of the ALTO service.

Security issues of ALTO in general and potential solutions are also discussed in [I-D.ietf-alto-protocol].

## 6.2. For U-NAPTR

The address of an ALTO server is usually well-known within an access network; therefore, interception of messages does not introduce any specific concerns.

The primary attack against the methods described in this document is one that would lead to impersonation of an ALTO server since a device does not necessarily have a prior relationship with an ALTO server.

An attacker could attempt to compromise ALTO discovery at any of three stages:

1. providing a falsified domain name to be used as input to U-NAPTR

2. altering the DNS records used in U-NAPTR resolution

3. impersonation of the ALTO server

This document focuses on the U-NAPTR resolution process and hence

this section discusses the security considerations related to the DNS handling. The security aspects of obtaining the domain name that is used for input to the U-NAPTR process is described in respective documents, such as [RFC5986].

The domain name that is used to authenticated the ALTO server is the domain name in the URI that is the result of the U-NAPTR resolution. Therefore, if an attacker was able to modify or spoof any of the DNS records used in the DDDS resolution, this URI could be replaced by an invalid URI. The application of DNS security (DNSSEC) [RFC4033] provides a means to limit attacks that rely on modification of the DNS records used in U-NAPTR resolution. Security considerations specific to U-NAPTR are described in more detail in [RFC4848].

An "https:" URI is authenticated using the method described in Section 3.1 of [RFC2818]. The domain name used for this authentication is the domain name in the URI resulting from U-NAPTR resolution, not the input domain name as in [RFC3958]. Using the domain name in the URI is more compatible with existing HTTP client software, which authenticate servers based on the domain name in the URI.

# 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.

[RFC2132] Alexander, S. and R. Droms, "DHCP Options and BOOTP Vendor Extensions", RFC 2132, March 1997.

[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.

[RFC4848] Daigle, L., "Domain-Based Application Service Location Using URIs and the Dynamic Delegation Discovery Service (DDDS)", RFC 4848, April 2007.

[RFC5986] Thomson, M. and J. Winterbottom, "Discovering the Local Location Information Server (LIS)", RFC 5986, September 2010.

## 7.2. Informative References

[I-D.ietf-alto-deployments] Stiemerling, M. and S. Kiesel, "ALTO Deployment Considerations", draft-ietf-alto-deployments-05 (work in progress), October 2012.

[I-D.ietf-alto-protocol] Alimi, R., Penno, R., and Y. Yang, "ALTO Protocol", draft-ietf-alto-protocol-13 (work in progress), September 2012.

[I-D.kist-alto-3pdisc] Kiesel, S. and M. Stiemerling, "Third-Party ALTO Server Discovery (3pdisc)", draft-kist-alto-3pdisc-01 (work in progress), October 2012.

[RFC2818] Rescorla, E., "HTTP Over TLS", RFC 2818, May 2000.

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, March 2005.

[RFC5693] Seedorf, J. and E. Burger, "Application-Layer Traffic Optimization (ALTO) Problem Statement", RFC 5693, October 2009.

[RFC6418] Blanchet, M. and P. Seite, "Multiple Interfaces and Provisioning Domains Problem Statement", RFC 6418, November 2011.

[RFC6708] Kiesel, S., Previdi, S., Stiemerling, 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.

Olafur Gudmundsson provided an excellent DNS expert review on an earlier version of this document.

The authors would also like to thank the following persons for their contribution to this document or its predecessors: Richard Alimi, David Bryan, Roni Even, Gustavo Garcia, Jay Gu, Xingfeng Jiang, Enrico Marocco, Victor Pascual, Y. Richard Yang, Yu-Shun Wang, Yunfei Zhang, Ning Zong.

Michael Scharf is supported by the German-Lab project (http://www.german-lab.de) funded by the German Federal Ministry of Education and Research (BMBF).

Martin Stiemerling is partially supported by the CHANGE project (http://www.change-project.eu), a research project supported by the European Commission under its 7th Framework Program (contract no. 257422). The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the CHANGE project or the European Commission.

Authors' Addresses

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

Email: ietf-alto@skiesel.de
URI: http://www.rus.uni-stuttgart.de/nks/

Martin Stiemerling
NEC Laboratories Europe
Kurfuerstenanlage 36
Heidelberg 69115
Germany

Phone: +49 6221 4342 113
Email: martin.stiemerling@neclab.eu
URI: http://ietf.stiemerling.org

Nico Schwan
Stuttgart, Germany

Email: ietf@nico-schwan.de

Michael Scharf
Alcatel-Lucent Bell Labs
Lorenzstrasse 10
Stuttgart 70435
Germany

Email: michael.scharf@alcatel-lucent.com
URI: www.alcatel-lucent.com/bell-labs

Haibin Song
Huawei

Email: melodysong@huawei.com