

ALTO  
Internet-Draft  
Intended status: Standards Track  
Expires: September 3, 2009

H. Song, Ed.  
Huawei  
R. Even  
Gesher Erove  
V. Pascual  
Tekelec  
Y. Zhang  
China Mobile  
March 2, 2009

**Application-Layer Traffic Optimization (ALTO): Discover ALTO Servers**  
**draft-song-alto-server-discovery-00**

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 September 3, 2009.

Copyright Notice

Copyright (c) 2009 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 in effect on the date of publication of this document (<http://trustee.ietf.org/license-info>). Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

## Abstract

A set of mechanisms are required to discover an Application-Layer Traffic Optimization (ALTO) Server. These mechanisms enable applications to find a reliable information source which provides them with information regarding the underlying network. By providing this information it would be possible to greatly increase application performance, reduce congestion and optimize the overall traffic across different networks. This document specifies the use of general means such as DHCP, DNS or static configuration for ALTO server discovery.

## Table of Contents

<a href="#">1.</a>	<a href="#">Introduction . . . . .</a>	<a href="#">3</a>
<a href="#">1.1.</a>	<a href="#">Background . . . . .</a>	<a href="#">3</a>
<a href="#">1.2.</a>	<a href="#">ALTO server distribution . . . . .</a>	<a href="#">3</a>
<a href="#">1.3.</a>	<a href="#">Concerns of ALTO server discovery . . . . .</a>	<a href="#">4</a>
<a href="#">2.</a>	<a href="#">Terminology . . . . .</a>	<a href="#">4</a>
<a href="#">3.</a>	<a href="#">ALTO server discovery using Domain Name System (DNS) . . . . .</a>	<a href="#">5</a>
<a href="#">3.1.</a>	<a href="#">ALTO servers providing service to overall network . . . . .</a>	<a href="#">5</a>
<a href="#">3.2.</a>	<a href="#">ALTO servers providing service to local networks . . . . .</a>	<a href="#">6</a>
<a href="#">3.2.1.</a>	<a href="#">ALTO server discovery by end terminals . . . . .</a>	<a href="#">6</a>
<a href="#">3.2.2.</a>	<a href="#">ALTO server discovery by application trackers . . . . .</a>	<a href="#">9</a>
<a href="#">4.</a>	<a href="#">Other ALTO server discovery mechanisms . . . . .</a>	<a href="#">11</a>
<a href="#">4.1.</a>	<a href="#">Provisioning . . . . .</a>	<a href="#">11</a>
<a href="#">4.2.</a>	<a href="#">Manual Configuration . . . . .</a>	<a href="#">11</a>
<a href="#">4.3.</a>	<a href="#">Caching . . . . .</a>	<a href="#">12</a>
<a href="#">4.4.</a>	<a href="#">ALTO server discovery using DHCP . . . . .</a>	<a href="#">12</a>
<a href="#">5.</a>	<a href="#">Security Considerations . . . . .</a>	<a href="#">12</a>
<a href="#">6.</a>	<a href="#">IANA Considerations . . . . .</a>	<a href="#">12</a>
<a href="#">7.</a>	<a href="#">Acknowledgements . . . . .</a>	<a href="#">12</a>
<a href="#">8.</a>	<a href="#">References . . . . .</a>	<a href="#">12</a>
<a href="#">8.1.</a>	<a href="#">Normative References . . . . .</a>	<a href="#">12</a>
<a href="#">8.2.</a>	<a href="#">Informative References . . . . .</a>	<a href="#">13</a>
	<a href="#">Authors' Addresses . . . . .</a>	<a href="#">13</a>



## **1. Introduction**

### **1.1. Background**

The ALTO problem statement draft [[I-D.marocco-alto-problem-statement](#)] describes that in P2P applications or client/server applications, resources are often available through multiple replicas and each of those are sometimes provided by different service providers. ALTO service gives guidance to a resource consumer or resource directory, like p2p tracker or ALTO service proxy, about which resource provider(s) to select, in order to optimize the client's performance or quality of experience while optimizing resource consumption in the underlying network infrastructure.

### **1.2. ALTO server distribution**

An ALTO server is a logical entity that provides interfaces to query the alto service. ALTO servers can be deployed by :

- (1) A network operator which wants to optimize its traffic, e.g. reduce its transit traffic across the network boundaries;
- (2) A third party on behalf of one or more ISPs;
- (3) user communities which run distributed algorithms, however, in this case, the user community may not know the policy of network operators, so with high probability it will also cause the suboptimal result for the network operator while benefiting the applications;

So there may be different ALTO servers distributed in different operator's networks.

For (1), each network operator may provide the ALTO service using their own ALTO servers. Each network operator may have its own traffic optimization policy based on his network topology, however it may not know other network operator's policies, nor be clear of other network operator's topologies (e.g. topology hiding). The application client must choose the ALTO service from the ALTO server that has information about its local network topology and policy. So in this case, each ALTO server must only provide service to the clients in its own network. A request from a client to an ALTO server not in its own operator's network may cause suboptimal result, because that ALTO server does not observe the network from the client's point of view. So each network operator deploys one or more ALTO servers for clients in its own network. If it is a large ISP, it may also deploy one or more ALTO servers for its sub networks, such as autonomous systems (AS).



For (2), if a third party provides ALTO service on behalf of only one ISP, it is similar to (1).

If a third party provides ALTO service on behalf of many ISPs, or a user community which measures the overall network through some mechanisms and provides ALTO service to numerous application clients located in different network operators, the case is equal to a conventional internet application server providing service to application clients.

This document describes the ALTO server discovery mechanisms for both environments where an ALTO server provides service to the overall network or an ALTO server provides service only to its local network

### **1.3. Concerns of ALTO server discovery**

The following issues should be considered when designing the ALTO server discovery mechanism.

Load Balance: When more than one ALTO server provide identical service for the same area, we must find a mechanism to balance the processing load between the ALTO servers;

Well known port: If ALTO server provides service through a well known port, then the discovery mechanism only needs to discover the IP address of an ALTO server that can provide service for a client, otherwise, the discovery mechanism must discover both IP address and port number through which the ALTO server provides the service.

IP address change: The IP address of the ALTO server may change in some circumstances. The ALTO server discovery mechanism must be well adaptable to this case when necessary.

Mobile Scenarios: When the end terminals are mobile equipments, the data traffic may route via a roaming client's home agent's router to the client, or route to the client directly. Which ALTO server to choose should depend on the routing optimization mode adopted for mobility. If the data traffic routes via the client's home agent, it should choose the ALTO server that serves its home area network, otherwise, it should choose the ALTO server that serves its current network.

## **2. Terminology**

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this



document are to be interpreted in [BCP 14](#), [RFC 2119](#) [[RFC2119](#)] and indicate requirement levels for compliant implementations.

Other terms used in this document are compatible with the definitions in "ALTO problem statement" draft [[I-D.marocco-alto-problem-statement](#)].

### **3. ALTO server discovery using Domain Name System (DNS)**

ALTO service is a conventional client/server mode service. The ALTO server discovery scenarios are classified into two types: one is the ALTO server providing service to overall network, and the other is ALTO server providing service to the local network.

#### **[3.1.](#) ALTO servers providing service to overall network**

The ALTO servers providing service to overall network include the ALTO servers provided by p2p application community and the ALTO servers provided by third party for multiple network operators.

As shown in Figure 1. A simple ALTO server discovery mechanism is used for this type of ALTO server. A DNS SRV query [[RFC2782](#)] mechanism is used. The server must register its SRV resource record with a well known service name (e.g. `_ALTO._TCP.example.com`) in the DNS system. The service name in this document refers to the name used for DNS SRV query, which includes the service label, protocol name (TCP or UDP) and domain name. Any ALTO client that wants to get the IP address and port of the ALTO server sends a DNS SRV query to the DNS server in that domain .



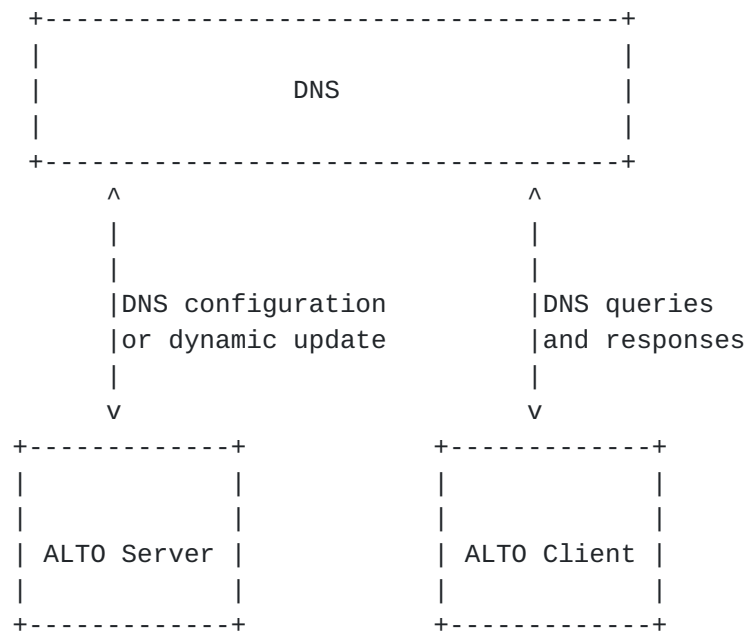


Figure 1: DNS query for well known ALTO servers

### **3.2. ALTO servers providing service to local networks**

In this environment, one or several ALTO servers provide service to their own network or autonomous system. There will be multiple ALTO servers in the overall network. Each of the ALTO server may have a FQDN. However, an end terminal can't easily determine its ALTO server automatically.

#### **3.2.1. ALTO server discovery by end terminals**

In p2p applications without a tracker like DHTs and other conventional client/server applications, an end user needs to discover the ALTO server by itself. It should follow these steps:

- (1) Through DHCP configuration, an end terminal retrieves the DNS SRV service name for local ALTO servers which includes the service provider's domain information, e.g. `_ALTO._TCP.MyISP.com`. A new DHCP Option for the ALTO server discovery is needed.



The DHCPv4 ALTO\_SRV\_Name option has the following format:

```

      0                   1                   2                   3
      0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|      Code      |      len      |                               |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
.      DNS SRV service name for local ALTO servers                .
.                                                                    .
.                                                                    .
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

Code                      ALTO\_SRV\_Name\_V4 (TBDv4)

len                      Length of DNS SRV service name for ALTO server, in  
octets

The DHCPv6 ALTO\_SRV\_Name option has the following format:

```

      0                   1                   2                   3
      0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|      OPTION_ALTO_SRV_Name_V6 |      option-len      |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|      DNS SRV service name for local ALTO servers                |
.                                                                    .
.                                                                    .
.                                                                    .
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

option-code              OPTION\_ALTO\_SRV\_Name\_V6 (TBDv6).

option-len              Length of DNS SRV service name for ALTO server, in  
octets

Once the ALTO server's service name is retrieved, the end terminal should cache this service name for later use.

It should be noticed that there are many residential gateways (RG) which can act as DHCP servers themselves. RG becomes a hindrance between the end terminals and the ALTO service provider's DHCP server if we use DHCP. It should not depend on the update of all these RGs to support this new DHCP Option for ALTO server discovery. A DHCP Container Option [[I-D.ietf-dhc-container-opt](#)] for server configuration must be used here. With the Container Option, the DHCP server for the consumer domain (e.g. RGs) can just pass the server configuration to the end terminals without explicit knowledge of the DHCP options contained in the Container.

The DHCP Option for the ALTO service name should be contained in

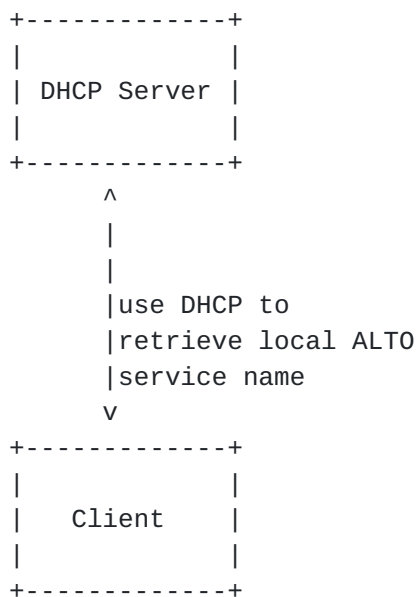
the Container Option.

(2) The end terminal sends an SRV query to the DNS server with the service name. It will retrieve the SRV RR with ALTO server instance name and port information, maybe together with a TXT description RR and an A RR with the IP address of the ALTO server. However, an additional A query is needed if the A RR corresponding to the ALTO server instance is not retrieved at the same time. Eventually the end terminal will get the IP address and port of the ALTO server. If there are more than one ALTO servers in the domain, the DNS server must balance the load between the ALTO servers according to the "priority" and "weight" value in the corresponding SRV RRs. Once the transport address of the ALTO server is retrieved, the end terminal should cache it for later use.

(3) The end terminal then accesses the ALTO server to get service;

Here DHCP protocol is used to retrieve the service name instead of the IP address because the IP address may change and the configuration for the DHCP server is very troublesome. Besides that, with the DNS SRV query, its existing load balance mechanism can be used, instead of introducing a new load balance mechanism in DHCP server.

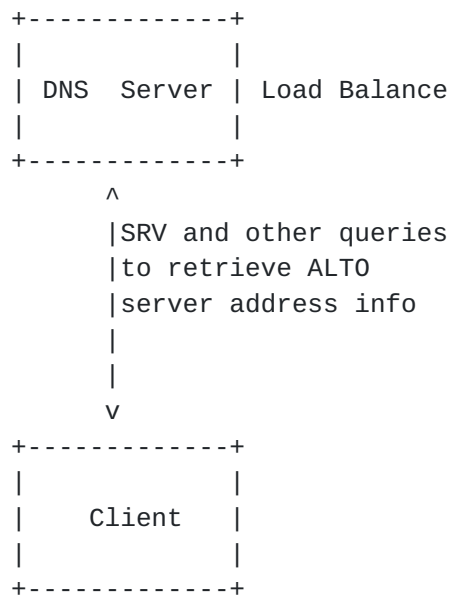
The following Figure 2 and Figure 3 depicts the first and second step of the ALTO server discovery for end terminals.



Step 1: retrieving service name



Figure 2: retrieving service name with DHCP



Step 2: DNS query for ALTO server address info

Figure 3: retrieving ALTO server address with DNS

### 3.2.2. ALTO server discovery by application trackers

Some p2p applications have trackers, and these applications don't need to have their clients looking for the ALTO server guidance. Trackers query the ALTO servers for guidance, and then return the final ranked result to the application clients. However, application clients are distributed among different network operators and autonomous systems. Trackers must find different ALTO servers for the clients located in different network operators or autonomous systems.

Here are the steps for ALTO server discovery in this type of scenarios:

- (1) The tracker should determine to which physical location the corresponding application client belongs to, i.e. which network operator and/or autonomous system the application client belongs to. The subsidiary organizations (e.g. APNIC) of IANA have the information database for the mapping between IP range to ISP/AS or other organizations. The WHOIS service [[www.whois](http://www.whois.com)] on the Internet is also available for this purpose. However, the mapping information may be changed due to the business deals and network adjustment. DHCP can also be used to retrieve the ISP/AS information to the end user, and the tracker can collect the



information from its clients.

(2) The tracker must determine the ALTO server for the corresponding network operator and or/ autonomous system. The tracker should maintain a complete mapping table between (a) the identities of network operators and/or autonomous systems and (b) ALTO server service names. The tracker sends a SRV query to the DNS server (an additional A query is needed when SRV query only responds with ALTO server instance name) to retrieve the ALTO server address information for its application client. From the perspective of efficiency, the tracker should cache the mapping information between network operators and ALTO server addresses for later use.

(3) The tracker contacts with the ALTO server for guidance on behalf of the application client; and sends the final ranked peer list to the application client.

Figure 4 shows an example for tracker's ALTO server discovery. For client 1, the tracker has not cached yet the mapping between client 1's network operator and its ALTO server address, so it queries the DNS server for the ALTO server address in that operator's domain. And then the tracker interacts with the ALTO server on behalf of client 1, finally, the ranked list is sent back to client 1. For client 2, the tracker has cached the mapping between client 2's network operator and its ALTO server address, so it does not need to query the DNS for the address of ALTO server 2.



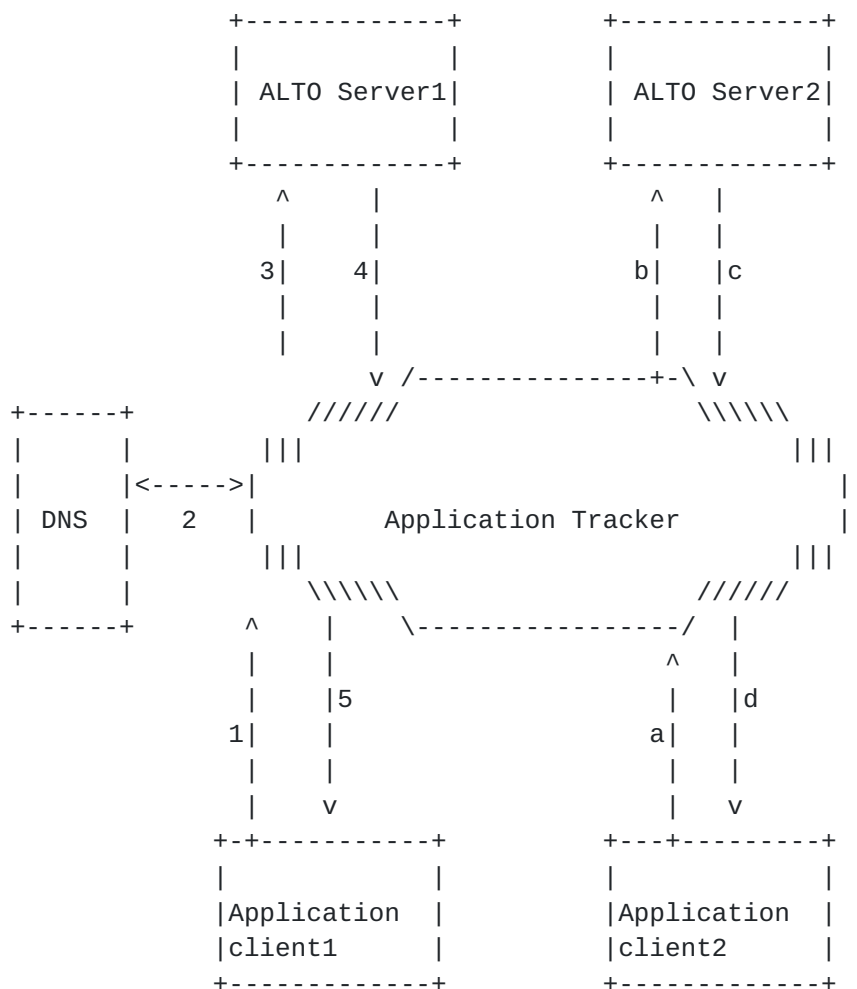


Figure 4: Example for tracker's ALTO discovery

## 4. Other ALTO server discovery mechanisms

### 4.1. Provisioning

A network operator can simply provide a configuration file that contains the ALTO server address for its clients, provided that there are only one or a few ALTO servers which provide identical service for its network. An application can also provide such a configuration file containing the ALTO server address if an existing ALTO server provides identical service to the overall network.

### 4.2. Manual Configuration

ALTO server information could also be configured on the ALTO client by a user or service provider manually.



### **4.3. Caching**

Once a client has located an ALTO server for the first time, it can cache it for use as future ALTO server.

### **4.4. ALTO server discovery using DHCP**

An ALTO client can discover an ALTO server through auto-configuration protocols. A new option could be defined in DHCP protocol to retrieve the IP address of local ALTO servers directly. However, it has drawbacks as described in [Section 3.2.1](#).

## **5. Security Considerations**

As this document mainly proposes to use DNS and DHCP for ALTO service discovery, it will depend on the DHCP security and DNS security for this service discovery.

## **6. IANA Considerations**

The service label for the ALTO service will depend on the final protocol name for application-layer traffic optimization(TBD).

This document requests IANA to assign an option tag from the "BOOTP Vendor Extensions and DHCP Options" registry for ALTO\_SRV\_Name\_V4 (TBDv4).

This document requests IANA to assign an option code from the "DHCPv6 Option Codes" registry for OPTION\_ALTO\_SRV\_Name\_V6 (TBDv6).

## **7. Acknowledgements**

The authors thank the review and valuable comments from Y. Richard Yang, Xingfeng Jiang, Jay Gu and Ning Zong.

## **8. References**

### **8.1. Normative References**

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [RFC2782] Gulbrandsen, A., Vixie, P., and L. Esibov, "A DNS RR for specifying the location of services (DNS SRV)", [RFC 2782](#),



February 2000.

[I-D.marocco-alto-problem-statement]

Seedorf, J. and E. Burger, "Application-Layer Traffic Optimization (ALTO) Problem Statement", [draft-marocco-alto-problem-statement-04](#) (work in progress), February 2009.

[I-D.ietf-dhc-container-opt]

Droms, R., "Container Option for Server Configuration", [draft-ietf-dhc-container-opt-04](#) (work in progress), November 2008.

## **8.2. Informative References**

[RFC2629] Rose, M., "Writing I-Ds and RFCs using XML", [RFC 2629](#), June 1999.

[RFC3552] Rescorla, E. and B. Korver, "Guidelines for Writing RFC Text on Security Considerations", [BCP 72](#), [RFC 3552](#), July 2003.

[I-D.narten-iana-considerations-rfc2434bis]

Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", [draft-narten-iana-considerations-rfc2434bis-09](#) (work in progress), March 2008.

[WWW.WHOIS]

"http://www.whois.net".

## **Authors' Addresses**

Song Haibin (editor)  
Huawei  
Baixia Road No. 91  
Nanjing, Jiangsu Province 210001  
P.R.China

Phone: +86-25-84565867  
Fax: +86-25-84565888  
Email: melodysong@huawei.com



Roni Even  
Gesher Erove  
14 David Hamelech  
Tel Aviv 64953  
Israel

Email: [ron.even.tlv@gmail.com](mailto:ron.even.tlv@gmail.com)

Victor Pascual  
Tekelec  
Am Borsigturm 11  
Berlin D-13507  
Germany

Phone: +49 30 32 51 32 12  
Email: [victor@iptel.org](mailto:victor@iptel.org)

Yunfei Zhang  
China Mobile

Phone: +86 10 66006688  
Email: [zhangyunfei@chinamobile.com](mailto:zhangyunfei@chinamobile.com)

