ALTO WG
Internet Draft
Intended status: Informational
Expires: September 2009

G. Garcia
Telefonica I+D
M. Tomsu
Alcatel-Lucent Bell Labs
Y. Wang
Microsoft

March 3, 2009

ALTO Discovery Protocols
draft-wang-alto-discovery-00.txt

Status of this Memo

Copyright Notice

Abstract

The Application-Layer Traffic Optimization service aims to provide applications with information to perform better-than-random initial peer selection when multiple peers in the network are available to provide a resource or service. This document discusses the discovery protocols for the service.

Table of Contents

1. Introduction

Application-Layer Traffic Optimization (ALTO) service aims to provide distributed network applications with information to perform better-than-random initial peer selection when multiple peers in the network are available to provide a resource or service. A discovery mechanism is needed for the applications to find a suitable entity that provides the ALTO service. This document discusses various scenarios of ALTO discovery, provides a survey of available options, and addresses potential issues and consideration for each.

1.1. Status of this Memo

The ALTO service architecture and protocol are currently under discussion and development within the IETF ALTO working group.

Although it is identified in the charter that a discovery mechanism is needed, the preference is to adopt one or more existing mechanisms for ALTO discovery rather than designing a new one. Note though certain design decisions of the final ALTO framework will affect the selection of discovery mechanisms. As a result, this document makes minimum assumptions of the ALTO framework, and presents different scenarios and available options based on prior and related discovery mechanisms. This document will be updated to track the progress of the ALTO requirements and solution.

2. Conventions used in this document

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].

3. Scenarios for ALTO Service Discovery

This section explores the various dimensions of the ALTO service deployment and access scenarios, and briefly discusses their implications to the discovery mechanisms. Figure 1 below shows a generic ALTO framework diagram with discovery. The terminology is defined in [ALTO-PS].

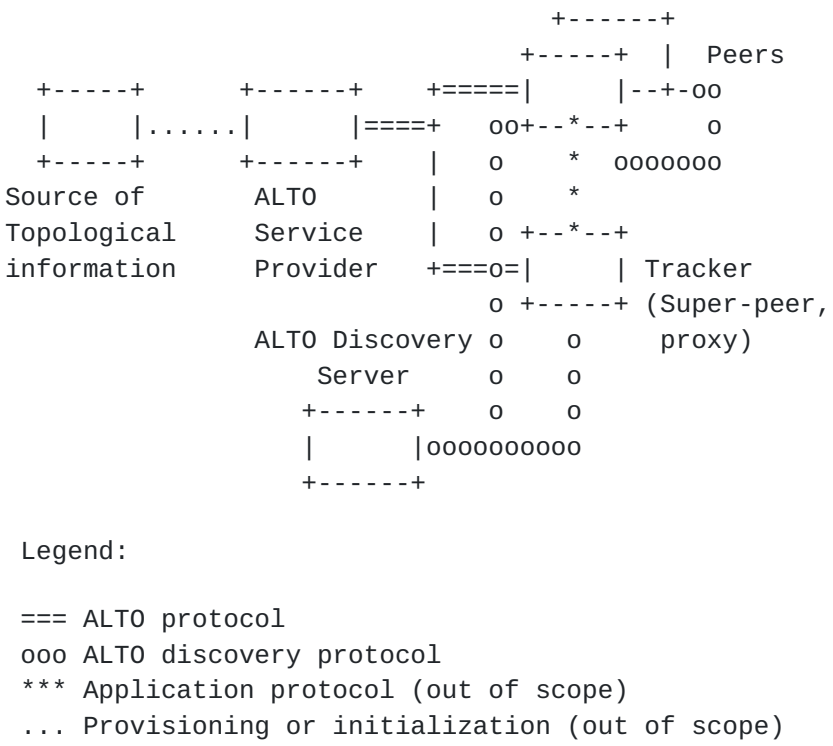

Figure 1 ALTO Discovery Diagram

In addition to the generic ALTO descriptions, the following terms are used to describe the discovery mechanisms in this document:

- ALTO Discovery Client: The logical entity discovering the ALTO Service. Depending on the scenario, this could be a Peer or a Super-peer.

- ALTO Discovery Server: The logical entity providing information to locate the ALTO Service. Depending on the discovery mechanism, this could be another Peer or a dedicated entity in the network.

- ALTO Discovery Domain: The scope of the network handled by a particular ALTO Discovery Server.

3.1. ALTO Service Provider

The ALTO service could be provided in a distributed and cooperative fashion by the Peers in an overlay, or it can be provided by a centralized entity (the ALTO Server) for a given scope. In the former case, a DHT-style key-based routing algorithm is commonly used to locate the peers with the target network information in this type of distributed environment. For the latter case, where a centralized ALTO Server is implicitly or explicitly assigned to a specific network scope, an out-of-band discovery mechanism is often required. All current ALTO solution proposals, ([Infoexp], [P4P]), fall into the second category.

3.2. ALTO Service Location

The ALTO Server for a Peer could be in the same Local Area Network (LAN), within the same ISP Network but not on the same LAN, or in the Global Internet outside the ISP Network. Different network scopes place different constraints on the discovery mechanisms. Multicast discovery generally works within a single LAN only, whereas DNS-based or DHCP-based discovery can span multiple subnets within a single ISP or a single network administrative domain. Internet scope discovery usually requires cross-domain indexing or directory services. Note that peers participating in a single P2P application may reside on the same or different ISP networks. Scenarios like this may require hybrid discovery solutions that can adapt to multiple network scopes at the same time. The discovery mechanisms listed in this document should take into account possible limitations of the ALTO service deployment in those network scopes.

[Open -NAT traversal discussion]

3.3. ALTO Service Clients

The ALTO Client can be the Peer in the end-user host or an external entity like a Super-peer or Resource Directory on behalf of the Peer. [ALTO-PS] If a Super-Peers acts as an ALTO Client, it needs to know and select the suitable ALTO Service for the Peer being served. The location of the ALTO Server could be communicated from the Peer to the Super-Peer using the application protocol. It could also be discovered by the Super-Peer from other Peer information received implicitly (like the Peer public IP address) or received explicitly. There could be scenarios where only the Peer is able to access to the ALTO Service, for example if the ALTO Server is located in a private network or in case the ALTO Server requires to receive the ALTO Queries from the Peer which network information is being queried.

3.4. When is ALTO Service Discovered and Accessed

The discovery process takes place before the first access to the ALTO server. This discovery process could be done at host network initialization time, at application initialization time or just before the first ALTO query is sent.

4. Options for ALTO Service Discovery

4.1. Manual

Manual configuration of the ALTO service location(s) could work in a single ISP network scope, but is not scalable when multiple ISPs or cross-domain ALTO services are required. P2P applications often connect peers from ISPs that they may not have contacted before, and manual configuration will not work without any prior knowledge of the ALTO servers.

4.2. DHCP

In environments where the access network itself either deploys an ALTO server or knows a third party that operates an ALTO server, DHCP [RFC2131] can provide the end host with a domain name. This domain name can then used as input to a DNS-based resolution mechanism described in Section 4.3.

The DHCP mechanism seems adequate for an ALTO Service Discovery as it defines the delivery of host-specific configuration from a DHCP server to a host. Also the placement close to the end host is advantageous as local knowledge is important for the ALTO Service. Commonly a DHCP procedure is executed by hosts (Peers) each time they connect to an access network and thus to a new ALTO discovery domain.

Network providers who are interested in providing an ALTO Service can introduce and enable this mechanism in their DHCP servers.

The DHCP based ALTO Discovery mechanism needs to define the IANA registration of IPv4 and IPv6 options [RFC2939] for the delivery of the host-specific of the ALTO service configuration.

As DHCP is limited to a broadcast domain, DHCP relaying must be considered.

Examples of DHCP based mechanisms are the discovery of a Location-to-Service Translation LoST Service [RFC5223] or the configuration of a Session Initiation Protocol (SIP) Server [RFC3361]

4.3. DNS

DNS infrastructure can be used to discover the location of entities providing the ALTO service. The DNS discovery methods described in this section require a domain name as input that can be determined making use of the mechanisms discussed in Section 4.6.

NAPTR [RFC3402] and SRV [RFC2782] DNS resource records are appropriate to provide service discovery mechanisms. The concrete application of these resource records depends on the final ALTO requests/response protocol, but S-NAPTR [RFC3958] and U-NAPTR [RFC4848] provides a generic standardized solution that could be used for the ALTO discovery use case. S-NAPTR and U-NAPTR mechanisms provide a Dynamic Delegation Discovery System (DDDS) Application to map domain name, service name and protocol name to a target host and port or to a target URI.

An ALTO service discovery mechanism could be defined just using NAPTR records or just using SRV records, but the combination of both provides and additional indirection level and more flexibility as described in [RFC3958] Section 5.

The use of NAPTR records for ALTO discovery requires the definition of an Application Service tag and an Application Protocol tag that must be IANA-registered.

The next example shows a NAPTR record for the ALTO service in the example.com domain. This record references the HTTP URI where the ALTO service using the PROTOCOL_A is located:

```
example.com.
 ;; order pref flags
 IN NAPTR 100 10 "u" "ALTO:PROTOCOL_A" ( ; service
 "!*.!http://alto.example.com/service.cgi!" ; regex
 . ; replacement
 )
```

The next example shows a NAPTR record for the ALTO service in the example.com domain. This NAPTR record references a SRV domain name for the ALTO service using the PROTOCOL_B. This SRV record could be dereferenced to obtain the target host and port where the service can be located:

```
example.com.
 ;; order pref flags
 IN NAPTR 100 10 "s" "ALTO:PROTOCOL_B" ( ; service
 "" ; regex
 _protocol_b._tcp.example.com. ; replacement
 )
 ;; prior weight port target
IN SRV 10 0 8888 alto.example.com
```

There are some advantages of using DNS-based discovery:

- DNS infrastructure is widely deployed, probed and available.
- Most of the end user equipment already include DNS protocol implementations.

DNS service discovery is used in IETF protocols for example to locate SIP servers [RFC3263] or to locate LIS servers [GeoprivDisc] and also in other protocols like bittorrent to discover local trackers [BEP-22].

4.4. Multicast (IP)

IP-multicast-based discovery generally works in two ways:

1. Clients send out multicast discovery requests and listen for responses (usually unicast) from available servers or service providers.
2. Servers or service providers send out multicast announcements when they become available or periodically, and clients waits for the next available multicast announcement to identify the servers or service providers.

The on-demand requests and periodic announcements are not mutually exclusive. An implementation can choose to utilize both simultaneously. The configuration effort of multicast discovery is fairly straightforward, only the multicast address and port are needed. Service types and additional information are often encoded in the requests or announcements messages, enabling the same multicast channel to support discovery of different resources or services. There are two main constraints of multicast-based discovery - scopes and flooding messages. Routers disable multicast forwarding by default, making it practically a single-subnet solution. Some forms of discovery proxies are needed to extend the scope of multicast discovery to multiple subnets. The second issue is the flooding of multicast messages to all hosts on the same subnet. The total bandwidth consumed by multicast depends on the arrival rate the client application requests, and/or the frequency of the service announcements. Older generations of 802.11-based wireless access points often slow down the transmission of multicast messages or generally have a higher packet loss rate for those, causing some multicast discovery implementation to automatically re-send multicast requests or announcements by default. This mitigation further increases the amount of flooding messages on the LAN. Examples of multicast-based discovery include [mDNS], [SSDP], [WSD], SLP [RFC2165], and LLMNR [RFC4795].

4.5. XRDS

[XRDS] (eXtensible Resource Descriptor Sequence), and its simplified profile [XRDS-Simple], specifies an XML format to describe resources associated with a URI, and the protocol to retrieve that XML document. One of the purposes of this XRDS document is to enumerate and describe the service endpoints associated with the resource, including the URI to access the service and a a type of service and/or media-type identifying the service being discovered.

The use of XRDS for ALTO Service Discovery requires using a URI to retrieve the XRDS document and the specification of a type of service and/or media-type identifying the ALTO Service. This is an example of a XRDS document including a possible the description of the ALTO service:

```
<XRDS xmlns="xri://$xrds">
  <XRD xmlns="xri://$XRD*($v*2.0)" version="2.0">
    <Type>xri://$xrds*simple</Type>
    <Service>
      <Type>http://ietf.org/rfcxxx</Type>
      <MediaType>application/xml+alto</MediaType>
      <URI>http://alto.example.com/</URI>
    </Service>
  </XRD>
</XRDS>
```

The necessity of an initial URI to retrieve the XRDS document requires an additional pre-discovery mechanism similar to the discovery of the ALTO service itself. This extra complexity and roundtrip seems to make XRDS not especially appropriate for the ALTO discovery use case.

4.6. IP and Domain discovery

Some of the mechanisms described in the previous sections require the knowledge of the domain name representing the entity providing the ALTO service for this endpoint or the knowledge of the endpoint IP Address.

The domain name associated with the entity providing the ALTO service could be manually configured in the end user application or extracted automatically from the endpoint domain name obtained through a reverse DNS lookup process (using DNS PTR records) or from a DHCP server ([RFC4702] for DHCPv4, [RFC4704] for DHCPv6). In case the endpoint domain name is used, the application tries to get the ALTO service for that domain name; if this request fails it removes iteratively the labels from the left of the domain name until an answer to the service location request is successful. The process ends notifying an error when the only label in the domain name is the top level domain.

For example in case of an endpoint with a public address 80.80.80.80, it requests the DNS PTR record at 80.80.80.in-addr.arpa. obtaining a domain name like pc1.network1.example.com. The application requests the ALTO service for that domain making a DNS SRV request for alto.tcp.pc1.network1.example.com. In case that request fails, the application makes a new request for alto.tcp.network1.example.com. and then for alto.tcp.example.com. stopping when a successful answer is returned.

To discover the domain name using reverse DNS lookups, the application requires first the knowledge of the endpoint IP address.

In presence of Network Address Translation (NAT) this could be done using mechanisms specific of the application (for example asking an application server using the application specific protocol like [BEP-24] in case of a Bittorrent protocol) or using additional standard protocols like STUN, UPnP or NAT-PMP that require additional servers in the network or impose additional requirements in the routers implementing the NATs.

Similar Domain Name and IP resolution mechanisms have been described in other discovery mechanisms like the BitTorrent Local Tracker Discovery Protocol [BEP-22].

5. Security Considerations

The security considerations for the ALTO discovery protocol will be detailed in further versions of this document after the final discovery mechanism will be selected.

In case of DHCP security consideration needs to be taken into account as a client accepts configuration responses from any server.

The security considerations for the DNS discovery mechanisms depend on the Resource Records in use. U-NAPTR security considerations are detailed in [RFC4848] and those for SRV in [RFC2782]. The security of the IP and Domain discovery described in 4.6. must also be considered.

Each multicast discovery mechanism has specific security considerations that will be addressed if any of them is used in the final ALTO discovery protocol.

6. IANA Considerations

This version of the draft presents a survey of possible discovery mechanisms for ALTO service discovery. There is no formal recommendation on the discovery mechanisms at this point. As such, there is no IANA consideration on any forms of assignment.

7. Conclusions

The document intends to start the discussion about ALTO discovery in the ALTO WG. It discusses various scenarios of ALTO discovery, provides a survey of available options, and addresses potential issues and consideration for each.

8. References

8.1. Normative References

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

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

8.2. Informative References

[BEP-22] Harrison, D., Shalunov, S., and G. Hazel "BitTorrent Local Tracker Discovery Protocol," http://bittorrent.org/beps/bep_0022.html, October 2008.

[Infoexp] Shalunov, S., Penno, and R., Woundy, "ALTO Information Export Service," draft-shalunov-alto-infoexport-00, (work in progress), October 2008.

[GeoprivDisc] Thomson, M., Winterbottom, J., "Discovering the Local Location Information Server (LIS)," draft-ietf-geopriv-lis-discovery-07, (work in progress), February, 2009.

[mDNS] Cheshire, S., Krochmal, M, "Multicast DNS," draft-cheshire-dnsext-multicastdns-07, (work in progress), September 2008.

[P4P] Alimi, R., Pasko, D., Popkin, L., Wang, Y., and Y. Yang, "P4P: Provider Portal for P2P Applications", draft-p4p-framework-00 (work in progress), November 2008.

[RFC2131] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997

[RFC2165] Veizades, J., Guttman, E., Perkins, C. and S. Kaplan, "Service Location Protocol", RFC 2165, July 1997.

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

[RFC2939] Droms, R., "Procedures and IANA Guidelines for Definition of New DHCP Options and Message Types", September 2000

[RFC3263] Rosenberg, J., Schulzrinne, H., "Session Initiation Protocol (SIP): Locating SIP Servers," RFC 3263, June 2002.

[RFC3361] Schulzrinne, H., "Dynamic Host Configuration Protocol (DHCP-for-IPv4) Option for Session Initiation Protocol (SIP) Servers", RFC 3361, August 2002

[RFC3402] Mealling, M., "Dynamic Delegation Discovery System (DDDS): Part Two: The Algorithm," RFC 3402, October 2002.

[RFC3958] Daigle, L., Newton, A., "Domain-Based Application Service Location Using SRV RRs and the Dynamic Delegation Discovery Service (DDDS)," RFC 3958, Janurary 2005.

[RFC4702] Stapp, M., Volz, B., and Y. Rekhter, "The Dynamic Host Configuration Protocol (DHCP) Client Fully Qualified Domain Name (FQDN) Option," RFC 4702, October 2006.

[RFC4704] Volz, B., "The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Client Fully Qualified Domain Name (FQDN) Option," RFC 4704, October 2006.

[RFC4795] Aboba, B., Thaler, D., and L. Esibov, "Link-Local Multicast Name Resolution (LLMNR)," RFC 4795, January 2007.

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

[RFC5223] Schulzrinne, H., Polk, J., Tschofenig, H., "Discovering Location-to-Service Translation (LoST) Servers Using the Dynamic Host Configuration Protocol (DHCP)", RFC 5223, August 2008

[SSDP] Goland, Y., Cai, T., Leach, P., Gu, Y., and S. Albright, "Simple Service Discovery Protocol/1.0: Operating without an Arbiter," draft-cai-ssdp-v1-03, (work in progress), October 1999.

[WSD] Beatty, J., et al., "Web Services Dynamic Discovery (WS-Discovery)", April 2005, http://specs.xmlsoap.org/ws/2005/04/discovery/ws-discovery.pdf

[XRDS] http://docs.oasis-open.org/xri/2.0/specs/xri-resolution-V2.0.html

[XRDS-Simple] http://xrds-simple.net/core/1.0

9. Acknowledgments

This document was prepared using 2-Word-v2.0.template.dot.

Authors' Addresses

Gustavo Garcia
Telefonica I+D
Emilio Vargas
Madrid, Madrid
Spain

Phone: +34 913129826
Email: ggb@tid.es

Marco Tomsu
Alcatel-lucent Bell Labs
Lorenzstrasse 10
70435 Stuttgart
Germany

Email: marco.tomsu@alcatel-lucent.com
URI: www.alcatel-lucent.com/bell-labs

Yu-Shun Wang
Microsoft Corp.
One Microsoft Way
Redmond, WA 98052
USA

Email: yu-shun.wang@microsoft.com