



XMPP

XEP-0156: Discovering Alternative XMPP Connection Methods

Joe Hildebrand
<mailto:jhildebr@cisco.com>
<xmpp:hildjj@jabber.org>

Peter Saint-Andre
<mailto:xsf@stpeter.im>
<xmpp:peter@jabber.org>
<http://stpeter.im/>

Lance Stout
<mailto:lance@andyet.com>
<xmpp:lance@lance.im>

2019-02-20
Version 1.2.0

Status	Type	Short Name
Draft	Standards Track	alt-connections

This document defines a DNS TXT Resource Record format for use in discovering alternative methods of connecting to an XMPP server.

Legal

Copyright

This XMPP Extension Protocol is copyright © 1999 – 2018 by the [XMPP Standards Foundation](#) (XSF).

Permissions

Permission is hereby granted, free of charge, to any person obtaining a copy of this specification (the "Specification"), to make use of the Specification without restriction, including without limitation the rights to implement the Specification in a software program, deploy the Specification in a network service, and copy, modify, merge, publish, translate, distribute, sublicense, or sell copies of the Specification, and to permit persons to whom the Specification is furnished to do so, subject to the condition that the foregoing copyright notice and this permission notice shall be included in all copies or substantial portions of the Specification. Unless separate permission is granted, modified works that are redistributed shall not contain misleading information regarding the authors, title, number, or publisher of the Specification, and shall not claim endorsement of the modified works by the authors, any organization or project to which the authors belong, or the XMPP Standards Foundation.

Warranty

NOTE WELL: This Specification is provided on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE.

Liability

In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall the XMPP Standards Foundation or any author of this Specification be liable for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising from, out of, or in connection with the Specification or the implementation, deployment, or other use of the Specification (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if the XMPP Standards Foundation or such author has been advised of the possibility of such damages.

Conformance

This XMPP Extension Protocol has been contributed in full conformance with the XSF's Intellectual Property Rights Policy (a copy of which can be found at <https://xmpp.org/about/xsf/ipr-policy>) or obtained by writing to XMPP Standards Foundation, P.O. Box 787, Parker, CO 80134 USA).

Contents

1	Introduction	1
2	DNS Lookup Method	1
2.1	Record Format	1
2.2	Business Rules	2
2.3	Examples	2
3	HTTP Lookup Method	2
3.1	Link Format	2
3.2	Business Rules	3
3.3	Examples	3
4	Implementation Notes	4
5	Security Considerations	4
6	IANA Considerations	5
7	XMPP Registrar Considerations	5
7.1	Namespaces	5
7.2	Alternative Connection Methods Registry	5
7.2.1	Process	5
7.2.2	Registered Values	6

1 Introduction

Although [XMPP Core](#)¹ specifies the use of TCP as the method of connecting to an XMPP server, alternative connection methods exist, including the [BOSH \(XEP-0124\)](#)² method (for which [XMPP Over BOSH \(XEP-0206\)](#)³ is the XMPP profile) and the websocket subprotocol specified in [RFC 7395](#)⁴. For some of these methods, it is necessary to discover further parameters before connecting, such as the HTTP URL of an alternative connection manager. Without ways to auto-discover alternative connection methods, the relevant information would need to be provided manually by a human user (which is cumbersome and error-prone) or hard-coded into XMPP software applications (which is brittle and not interoperable).

This document defines two ways to encapsulate information about alternative connection methods for auto-discovery:

1. DNS TXT resource records
2. Link entries in a server's "host-meta" file

2 DNS Lookup Method

2.1 Record Format

The following format for DNS TXT resource records is specified in RFC 1464:

```
<owner> <class> <ttl> <TXT> <"attribute_name=attribute_value">
```

This document specifies that the following additional rules apply for DNS TXT resource records used to specify alternative connection methods:

1. It is RECOMMENDED for the owner to be "_xmppconnect".
2. The class field SHOULD be IN.
3. The ttl field is OPTIONAL.
4. The attribute name SHOULD begin with the string "_xmpp-client-" or "_xmpp-server-" and SHOULD be registered as described in the [XMPP Registrar Considerations](#) section of this document.
5. If the txt-data field contains only an attribute name (i.e., no unquoted "=" character followed by additional characters), the receiving application SHOULD interpret it as indicating the presence of the attribute or feature with no defined value.

¹RFC 6120: Extensible Messaging and Presence Protocol (XMPP): Core <<http://tools.ietf.org/html/rfc6120>>.

²XEP-0124: Bidirectional-streams Over Synchronous HTTP <<https://xmpp.org/extensions/xep-0124.html>>.

³XEP-0206: XMPP Over BOSH <<https://xmpp.org/extensions/xep-0206.html>>.

⁴RFC 7395: An Extensible Messaging and Presence Protocol (XMPP) Subprotocol for WebSocket <<http://tools.ietf.org/html/rfc7395>>.

6. If the txt-data field contains an unquoted "=" character, it MUST also contain an attribute value.

2.2 Business Rules

The following business rules apply:

1. TXT lookups MUST be used only as a fallback after the methods specified in RFC 6120 have been exhausted. ⁵
2. A domain SHOULD NOT present information in DNS TXT records that is available via the DNS SRV records defined in RFC 6120.
3. The order of DNS TXT records SHOULD NOT be interpreted as significant by the presenting domain or the receiving entity.

2.3 Examples

The following examples show two DNS TXT resource records: the first indicates support for the XMPP Over BOSH connection method defined in XEP-0124 and XEP-0206 and the second indicates support for XMPP over WebSocket connections defined in RFC 7395;

Listing 1: TXT Resource Records

```
_xmppconnect IN TXT "_xmpp-client-xbosh=https://web.example.org:5280/
bosh"
_xmppconnect IN TXT "_xmpp-client-websocket=wss://web.example.com:443/
ws"
```

3 HTTP Lookup Method

3.1 Link Format

The HTTP lookup method uses Web Host Metadata RFC 6415 ⁶ to categorize and list the URIs of alternative connection methods. It is primarily intended for use by clients in environments where the ability to perform DNS queries is restricted, such as in web browsers.

Each alternative connection method is specified in the host-meta (XRD) file using a distinctive link relation RFC 5988 ⁷. This specification defines several extension relation types:

- urn:xmpp:alt-connections:httplib

⁵The point of this rule is to prevent someone from defining a new XEP-0156 connection method like "_xmpp-client-tcp" to override the SRV records defined in the core XMPP specification.

⁶RFC 6415: Web Host Metadata <<http://tools.ietf.org/html/rfc6415>>.

⁷RFC 5988: Web Linking <<http://tools.ietf.org/html/rfc5988>>.

- urn:xmpp:alt-connections:websocket
- urn:xmpp:alt-connections:xbosh

3.2 Business Rules

The following business rules apply:

1. HTTP queries for host-meta information MUST be used only as a fallback after the methods specified in RFC 6120 have been exhausted.
2. A domain SHOULD NOT present information in host-meta link records that is available via the DNS SRV records defined in RFC 6120.
3. The order of XMPP related link entries in the host-meta file SHOULD NOT be interpreted as significant by the presenting domain or the receiving entity.

3.3 Examples

The following examples show two host-meta link records: the first indicates support for the XMPP Over BOSH connection method defined in XEP-0124 and XEP-0206 and the second indicates support for the XMPP Over WebSocket connection method defined in RFC 7395⁸. As specified in RFC 6120 §3, support for the XML encoding of the host-meta resource is REQUIRED while alternative representations such as JSON are OPTIONAL.

Listing 2: Result for /.well-known/host-meta

```
<?xml version='1.0' encoding='utf-8'?>
<XRD xmlns='http://docs.oasis-open.org/ns/xri/xrd-1.0'>
  ...
  <Link rel="urn:xmpp:alt-connections:xbosh"
        href="https://web.example.com:5280/bosh" />
  <Link rel="urn:xmpp:alt-connections:websocket"
        href="wss://web.example.com:443/ws" />
  ...
</XRD>
```

It is possible to use an alternative JSON format for host-meta information, in which case the above example would be presented as:

Listing 3: Result for /.well-known/host-meta.json

```
{
  ...
}
```

⁸RFC 7395: An Extensible Messaging and Presence Protocol (XMPP) Subprotocol for WebSocket <<http://tools.ietf.org/html/rfc7395>>.

```
"links": [  
  ...  
  {  
    "rel": "urn:xmpp:alt-connections:xbosh",  
    "href": "https://web.example.com:5280/bosh"  
  },  
  {  
    "rel": "urn:xmpp:alt-connections:websocket",  
    "href": "wss://web.example.com:443/ws"  
  }  
]  
}
```

4 Implementation Notes

To make connection discovery work in web clients (including those hosted on a different domain) the host service SHOULD set appropriate [CORS](#) headers for Web Host Metadata files. The exact headers and values are out of scope of this document but may include: *Access-Control-Allow-Origin*, *Access-Control-Allow-Methods* and *Access-Control-Allow-Headers*. Due care has to be exercised in limiting the scope of *Access-Control-Allow-Origin* response header to Web Host Metadata files only.

```
Access-Control-Allow-Origin: *
```

Access-Control-Allow-Origin header with a value of * allows JavaScript code running on a different domain to read the content of Web Host Metadata files. Special value * ensures that the request will only succeed if it is [invoked without user credentials](#) (e.g. cookies, HTTP authentication).

5 Security Considerations

It is possible that advertisement of alternative connection methods can introduce security vulnerabilities, since a connecting entity (usually a client) might deliberately seek to connect using the method with the weakest security mechanisms (e.g., no channel encryption or relatively weak authentication). Care needs to be taken in determining which alternative connection methods are appropriate to advertise.

Entities that use these connection methods MUST conform to the security considerations of each method, for example by preferring to use 'https' or 'wss' URLs that are protected using Transport Layer Security (TLS).

6 IANA Considerations

Because the link relations specified here are extension relation types rather than registered relation types (see Section 4 of RFC 5988), this document requires no interaction with the [Internet Assigned Numbers Authority \(IANA\)](#)⁹.

7 XMPP Registrar Considerations

7.1 Namespaces

The [XMPP Registrar](#)¹⁰ shall include 'urn:xmpp:alt-connections' in its registry of protocol namespaces (see <https://xmpp.org/registrar/namespaces.html>).

- urn:xmpp:alt-connections

7.2 Alternative Connection Methods Registry

The [XMPP Registrar](#)¹¹ maintains a registry of attributes for use in DNS TXT resource records that advertise alternative XMPP connection methods (see <https://xmpp.org/registrar/alt-connections.html>).

7.2.1 Process

In order to submit new values to this registry, the registrant shall define an XML fragment of the following form and either include it in the relevant XMPP Extension Protocol or send it to the email address registrar@xmpp.org:

```
<method>
  <name>the name of the attribute to be used in DNS TXT records</name>
  <desc>a natural-language description of the alternative connection
    method</desc>
  <syntax>the syntax of the DNS TXT record attribute value</syntax>
  <doc>the document in which the alternative connection method is
    specified</doc>
```

⁹The Internet Assigned Numbers Authority (IANA) is the central coordinator for the assignment of unique parameter values for Internet protocols, such as port numbers and URI schemes. For further information, see <http://www.iana.org/>.

¹⁰The XMPP Registrar maintains a list of reserved protocol namespaces as well as registries of parameters used in the context of XMPP extension protocols approved by the XMPP Standards Foundation. For further information, see <https://xmpp.org/registrar/>.

¹¹The XMPP Registrar maintains a list of reserved protocol namespaces as well as registries of parameters used in the context of XMPP extension protocols approved by the XMPP Standards Foundation. For further information, see <https://xmpp.org/registrar/>.


```
</method>
```

The registrant can register more than one attribute at a time, each contained in a separate `<method/>` element.

7.2.2 Registered Values

This document registers the following values.

```
<method>
  <name>_xmpp-client-httppoll</name>
  <desc>HTTP Polling connection method</desc>
  <syntax>
    The http: or https: URL at which to contact the HTTP Polling
    connection manager or proxy
  </syntax>
  <doc>XEP-0025</doc>
</method>

<method>
  <name>_xmpp-client-websocket</name>
  <desc>XMPP Over WebSocket connection method</desc>
  <syntax>
    The ws: or wss: URL at which to contact the WebSocket connection
    manager or proxy
  </syntax>
  <doc>RFC 7395</doc>
</method>

<method>
  <name>_xmpp-client-xbosh</name>
  <desc>XMPP Over Bosh connection method</desc>
  <syntax>
    The http: or https: URL at which to contact the HTTP Binding (BOSH
    ) connection manager or proxy
  </syntax>
  <doc>XEP-0206</doc>
</method>
```