Network Working Group
Internet-Draft
Expires: December 22, 2003

P. Saint-Andre
J. Miller
Jabber Software Foundation

June 23, 2003

# XMPP Core
# draft-ietf-xmpp-core-14

## Status of this Memo



## Copyright Notice



## Abstract

This document describes the core features of the Extensible Messaging and Presence Protocol (XMPP), a protocol for streaming XML elements in order to exchange messages and presence information in close to real time. While XMPP provides a generalized, extensible framework for transporting structured information, it is used mainly for the purpose of building instant messaging and presence applications that meet the requirements of RFC 2779.

Table of Contents

# 1. Introduction

## 1.1 Overview

The Extensible Messaging and Presence Protocol (XMPP) is an open XML [1] protocol for near-real-time messaging, presence, and request-response services. The basic syntax and semantics were developed originally within the Jabber open-source community, mainly in 1999. In 2002, the XMPP WG was chartered with developing an adaptation of the Jabber protocol that would be suitable as an IETF instant messaging (IM) and presence technology. As a result of work by the XMPP WG, the current document defines the core features of XMPP; XMPP IM [23] defines the extensions required to provide the instant messaging and presence functionality defined in RFC 2779 [2].

## 1.2 Terminology

The capitalized 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 [3].

## 1.3 Discussion Venue

The authors welcome discussion and comments related to the topics presented in this document. The preferred forum is the <xmppwg@jabber.org> mailing list, for which archives and subscription information are available at <http://www.jabber.org/cgi-bin/mailman/listinfo/xmppwg/>.

## 1.4 Intellectual Property Notice

This document is in full compliance with all provisions of Section 10 of RFC 2026. Parts of this specification use the term "jabber" for identifying namespaces and other protocol syntax. Jabber[tm] is a registered trademark of Jabber, Inc. Jabber, Inc. grants permission to the IETF for use of the Jabber trademark in association with this specification and its successors, if any.

## 2. Generalized Architecture

### 2.1 Overview

Although XMPP is not wedded to any specific network architecture, to this point it usually has been implemented via a typical client-server architecture, wherein a client utilizing XMPP accesses a server over a TCP [4] socket.

The following diagram provides a high-level overview of this architecture (where "-" represents communications that use XMPP and "=" represents communications that use any other protocol).

```
C1 -  S1 - S2 - C3
     /  \
C2 -     G1 = FN1 = FC1
```

The symbols are as follows:

- C1, C2, C3 -- XMPP clients
- S1, S2 -- XMPP servers
- G1 -- A gateway that translates between XMPP and the protocol(s) used on a foreign (non-XMPP) messaging network
- FN1 -- A foreign messaging network
- FC1 -- A client on a foreign messaging network

### 2.2 Server

A server acts as an intelligent abstraction layer for XMPP communications. Its primary responsibilities are to manage connections from or sessions for other entities (in the form of XML streams to and from authorized clients, servers, and other entities) and to route appropriately-addressed XML data "stanzas" among such entities over XML streams. Most XMPP-compliant servers also assume responsibility for the storage of data that is used by clients (e.g., contact lists for users of XMPP-based instant messaging applications); in this case, the XML data is processed directly by the server itself on behalf of the client and is not routed to another entity. Compliant server implementations MUST ensure in-order processing of XML stanzas between any two entities.

### 2.3 Client

Most clients connect directly to a server over a TCP socket and use XMPP to take full advantage of the functionality provided by a server and any associated services. Although there is no necessary coupling of an XML stream to a TCP socket (e.g., a client COULD connect via HTTP polling or some other mechanism), this specification defines a binding for XMPP to TCP only. Multiple resources (e.g., devices or locations) MAY connect simultaneously to a server on behalf of each authorized client, with each resource connecting over a discrete TCP socket and differentiated by the resource identifier of a JID (e.g., <user@domain/home> vs. <user@domain/work>) as defined under Addressing Scheme (Section 3). The port registered with the IANA for connections between a client and a server is 5222 (see IANA Considerations (Section 10)).

### 2.4 Gateway

A gateway is a special-purpose server-side service whose primary function is to translate XMPP into the protocol used by a foreign (non-XMPP) messaging system, as well as to translate the return data back into XMPP. Examples are gateways to Internet Relay Chat (IRC), Short Message Service (SMS), SMTP, and legacy instant messaging networks such as AIM, ICQ, MSN Messenger, and Yahoo! Instant Messenger. Communications between gateways and servers, and between gateways and the foreign messaging system, are not defined in this document.

### 2.5 Network

Because each server is identified by a network address and because server-to-server communications are a straightforward extension of the client-to-server protocol, in practice the system consists of a network of servers that inter-communicate. Thus user-a@domain1 is able to exchange messages, presence, and other information with user-b@domain2. This pattern is familiar from messaging protocols (such as SMTP) that make use of network addressing standards. Communications between any two servers are OPTIONAL; if enabled, such communications occur over XML streams that are normally bound to TCP sockets, using port 5269 as registered with the IANA (see IANA Considerations (Section 10)).

# 3. Addressing Scheme

## 3.1 Overview

An entity is anything that can be considered a network endpoint (i.e., an ID on the network) and that can communicate using XMPP. All such entities are uniquely addressable in a form that is consistent with RFC 2396 [24]. For historical reasons, the address of such an entity is called a Jabber Identifier or JID. A valid JID contains a set of ordered elements formed of a domain identifier, node identifier, and resource identifier in the following format: [node@]domain[/resource]. Each allowable portion of a JID (node identifier, domain identifier, and resource identifier) may be up to 1023 bytes in length, resulting in a maximum total size (including the '@' and '/' separators) of 3071 bytes.

All JIDs are based on the foregoing structure. The most common use of this structure is to identify an instant messaging user, the server to which the user connects, and the user's active session or connection (e.g., a specific client) in the form of <user@domain/resource>. However, node types other than clients are possible; for example, a specific chat room offered by a multi-user chat service could be addressed as <room@service> (where "room" is the name of the chat room and "service" is the hostname of the multi-user chat service) and a specific occupant of such a room could be addressed as <room@service/nick> (where "nick" is the occupant's room nickname). Many other JID types are possible (e.g., <domain/resource> could be a server-side script or service).

## 3.2 Domain Identifier

The domain identifier is the primary identifier and is the only REQUIRED element of a JID (a mere domain identifier is a valid JID). It usually represents the network gateway or "primary" server to which other entities connect for XML routing and data management capabilities. However, the entity referenced by a domain identifier is not always a server, and may be a service that is addressed as a subdomain of a server and that provides functionality above and beyond the capabilities of a server (e.g., a multi-user chat service, a user directory, or a gateway to a foreign messaging system).

The domain identifier for every server or service that will communicate over a network SHOULD resolve to a Fully Qualified Domain Name. A domain identifier MUST conform to RFC 952 [6] and RFC 1123 [7]. In addition, a domain identifier MUST be no more than 1023 bytes in length and MUST conform to the nameprep [8] profile of stringprep [9].

### 3.3 Node Identifier

The node identifier is an optional secondary identifier placed before the domain identifier and separated from the latter by the '@' character. It usually represents the entity requesting and using network access provided by the server or gateway (i.e., a client), although it can also represent other kinds of entities (e.g., a chat room associated with a multi-user chat service). The entity represented by a node identifier is addressed within the context of a specific domain; within instant messaging applications of XMPP this address is called a "bare JID" and is of the form <node@domain>.

A node identifier MUST be no more than 1023 bytes in length and MUST conform to the nodeprep [10] profile of stringprep [9].

### 3.4 Resource Identifier

The resource identifier is an optional tertiary identifier placed after the domain identifier and separated from the latter by the '/' character. A resource identifier may modify either a <user@domain> or mere <domain> address. It usually represents a specific session, connection (e.g., a device or location), or object (e.g., a participant in a multi-user chat room) belonging to the entity associated with a node identifier. A resource identifier is opaque to both servers and other clients, and is typically defined by a client implementation as the authzid value provided during stream authentication. An entity may maintain multiple resources simultaneously.

A resource identifier MUST be no more than 1023 bytes in length and MUST conform to the resourceprep [11] profile of stringprep [9].

# 4. XML Streams

## 4.1 Overview

Two fundamental concepts make possible the rapid, asynchronous exchange of relatively small payloads of structured information between presence-aware entities: XML streams and XML stanzas. These terms may be defined as follows:

Definition of XML Stream: An XML stream is a container for the exchange of XML elements between any two entities over a network. An XML stream is negotiated from an initiating entity (usually a client or server) to a receiving entity (usually a server), normally over a TCP socket, and corresponds to the initiating entity's "session" with the receiving entity. The start of the XML stream is denoted unambiguously by an opening XML <stream> tag with appropriate attributes and namespace declarations, and the end of the XML stream is denoted unambiguously by a closing XML </stream> tag. An XML stream is unidirectional; in order to enable bidirectional information exchange, the initiating entity and receiving entity MUST negotiate one stream in each direction, normally over the same TCP connection.

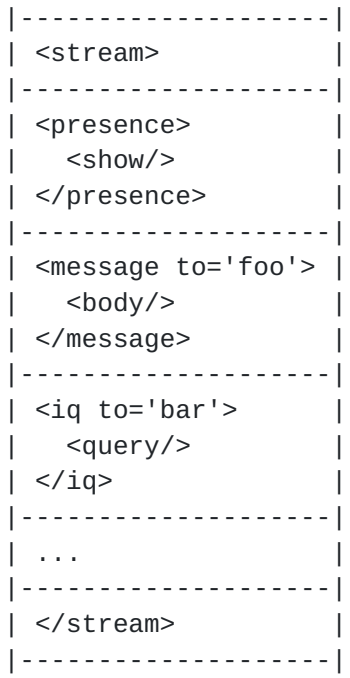
Definition of XML Stanza: An XML stanza is a discrete semantic unit of structured information that is sent from one entity to another over an XML stream. An XML stanza exists at the direct child level of the root <stream/> element and is said to be well-balanced if it matches production [43] content of the XML specification [1]). The start of any XML stanza is denoted unambiguously by the element start tag at depth=1 of the XML stream (e.g., <presence>), and the end of any XML stanza is denoted unambiguously by the corresponding close tag at depth=1 (e.g., </presence>). An XML stanza MAY contain child elements (with accompanying attributes, elements, and CDATA) as necessary in order to convey the desired information. An XML element sent for the purpose of stream encryption, stream authentication, or server dialback is not considered to be an XML stanza.

Consider the example of a client's session with a server. In order to connect to a server, a client MUST initiate an XML stream by sending an opening <stream> tag to the server, optionally preceded by a text declaration specifying the XML version supported and the character encoding (see also Character Encodings (Section 9.4)). The server SHOULD then reply with a second XML stream back to the client, again optionally preceded by a text declaration. Once the client has authenticated with the server (see Section 6), the client MAY send an unlimited number of XML stanzas over the stream to any recipient on the network. When the client desires to close the stream, it simply

sends a closing </stream> tag to the server (alternatively, the stream may be closed by the server), after which both the client and server SHOULD close the underlying TCP connection as well.

Those who are accustomed to thinking of XML in a document-centric manner may wish to view a client's session with a server as consisting of two open-ended XML documents: one from the client to the server and one from the server to the client. From this perspective, the root <stream/> element can be considered the document entity for each "document", and the two "documents" are built up through the accumulation of XML stanzas sent over the two XML streams. However, this perspective is a convenience only, and XMPP does not deal in documents but in XML streams and XML stanzas.

In essence, then, an XML stream acts as an envelope for all the XML stanzas sent during a session. We can represent this graphically as follows:




## 4.2 Stream Attributes

The attributes of the stream element are as follows:

o to -- The 'to' attribute SHOULD be used only in the XML stream header from the initiating entity to the receiving entity, and MUST be set to the JID of the receiving entity. There SHOULD be no 'to' attribute set in the XML stream header by which the receiving entity replies to the initiating entity; however, if a 'to'

attribute is included, it SHOULD be silently ignored by the initiating entity.

- from -- The 'from' attribute SHOULD be used only in the XML stream header from the receiving entity to the initiating entity, and MUST be set to the JID of the receiving entity granting access to the initiating entity. There SHOULD be no 'from' attribute on the XML stream header sent from the initiating entity to the receiving entity; however, if a 'from' attribute is included, it SHOULD be silently ignored by the receiving entity.

- id -- The 'id' attribute SHOULD be used only in the XML stream header from the receiving entity to the initiating entity. This attribute is a unique identifier created by the receiving entity to function as a session key for the initiating entity's streams with the receiving entity, and MUST be unique within the receiving application (normally a server). There SHOULD be no 'id' attribute on the XML stream header sent from the initiating entity to the receiving entity; however, if an 'id' attribute is included, it SHOULD be silently ignored by the receiving entity.

- version -- The presence of the version attribute set to a value of "1.0" indicates compliance with this specification. Detailed rules regarding generation and handling of this attribute are defined below.

We can summarize as follows:

| | initiating to receiving | receiving to initiating |
|---|---|---|
| to | hostname of receiver | silently ignored |
| from | silently ignored | hostname of receiver |
| id | silently ignored | session key |
| version | signals XMPP 1.0 support | signals XMPP 1.0 support |

### 4.2.1 Version Support

The following rules apply to the generation and handling of the 'version' attribute:

1. If the initiating entity complies with the protocol defined herein, it MUST include the 'version' attribute in the XML stream header it sends to the receiving entity, and it MUST set the value of the 'version' attribute to "1.0".

2. If the initiating entity includes the 'version' attribute set to a value of "1.0" in its stream header and the receiving entity

supports XMPP 1.0, the receiving entity MUST reciprocate by including the 'version' attribute set to a value of "1.0" in its stream header response.

3. If the initiating entity does not include the 'version' attribute in its stream header, the receiving entity still SHOULD include the 'version' attribute set to a value of "1.0" in its stream header response.

4. If the initiating entity includes the 'version' attribute set to a value other than "1.0", the receiving entity SHOULD include the 'version' attribute set to a value of "1.0" in its stream header response, but MAY at its discretion generate an <unsupported-version/> stream error and terminate the XML stream and underlying TCP connection.

5. If the receiving entity includes the 'version' attribute set to a value other than "1.0" in its stream header response, the initiating entity SHOULD generate an <unsupported-version/> stream error and terminate the XML stream and underlying TCP connection.

### 4.3 Namespace Declarations

The stream element MUST possess both a stream namespace declaration and a default namespace declaration (as "namespace declaration" is defined in the XML namespaces specification [12]). For detailed information regarding the stream namespace and default namespace, see Namespace Names and Prefixes (Section 9.2).

### 4.4 Stream Features

If the initiating entity includes the 'version' attribute set to a value of "1.0" in its initiating stream element, the receiving entity MUST send a <features/> child element (prefixed by the stream namespace prefix) to the initiating entity in order to announce any stream-level features that can be negotiated (or capabilities that otherwise need to be advertised). Currently this is used for TLS and SASL negotiation only, but it could be used for other negotiable features in the future (usage is defined under Stream Encryption (Section 5) and Stream Authentication (Section 6) below). If an entity does not understand or support some features, it SHOULD silently ignore them.

### 4.5 Stream Encryption and Authentication

XML streams in XMPP 1.0 SHOULD be encrypted as defined under Stream

Encryption (Section 5) and MUST be authenticated as defined under Stream Authentication (Section 6). If the initiating entity attempts to send an XML stanza before the stream is authenticated, the receiving entity SHOULD return a <not-authorized/> stream error to the initiating entity and then terminate both the XML stream and the underlying TCP connection.

### 4.6 Stream Errors

The root stream element MAY contain an <error/> child element that is prefixed by the stream namespace prefix. The error child MUST be sent by a compliant entity (usually a server rather than a client) if it perceives that a stream-level error has occurred.

#### 4.6.1 Rules

The following rules apply to stream-level errors:

- It is assumed that all stream-level errors are unrecoverable; therefore, if an error occurs at the level of the stream, the entity that detects the error MUST send a stream error to the other entity, send a closing </stream> tag, and terminate the underlying TCP connection.

- If the error occurs while the stream is being set up, the receiving entity MUST still send the opening <stream> tag, include the <error/> element as a child of the stream element, send the closing </stream> tag, and terminate the underlying TCP connection. In this case, if the initiating entity provides an unknown host in the 'to' attribute (or provides no 'to' attribute at all), the server SHOULD provide the server's authoritative hostname in the 'from' attribute of the stream header sent before termination.

#### 4.6.2 Syntax

The syntax for stream errors is as follows:

```
<stream:error>
  <defined-condition xmlns='urn:ietf:params:xml:ns:xmpp-streams'/>
  <text xmlns='urn:ietf:params:xml:ns:xmpp-streams'>
    OPTIONAL descriptive text
  </text>
  [OPTIONAL application-specific condition element]
</stream:error>
```

The <error/> element:

- MUST contain a child element corresponding to one of the defined stanza error conditions defined below; this element MUST be qualified by the 'urn:ietf:params:xml:ns:xmpp-streamstreams' namespace

- MAY contain a <text/> child containing CDATA that describes the error in more detail; this element MUST be qualified by the 'urn:ietf:params:xml:ns:xmpp-streams' namespace and SHOULD possess an 'xml:lang' attribute

- MAY contain a child element for an application-specific error condition; this element MUST be qualified by an application-defined namespace, and its structure is defined by that namespace

The <text/> element is OPTIONAL. If included, it SHOULD be used only to provide descriptive or diagnostic information that supplements the meaning of a defined condition or application-specific condition. It SHOULD NOT be interpreted programmatically by an application. It SHOULD NOT be used as the error message presented to user, but MAY be shown in addition to the error message associated with the included condition element (or elements).

Note: the XML namespace name 'urn:ietf:params:xml:ns:xmpp-streams' that qualifies the descriptive element adheres to the format defined in The IETF XML Registry [25].

### 4.6.3 Defined Conditions

The following stream-level error conditions are defined:

- <host-gone/> -- the value of the 'to' attribute provided by the initiating entity in the stream header corresponds to a hostname that is no longer hosted by the server.

- <host-unknown/> -- the value of the 'to' attribute provided by the initiating entity in the stream header does not correspond to a hostname that is hosted by the server.

- <improper-addressing/> -- a stanza sent between two servers lacks a 'to' or 'from' attribute (or the attribute has no value).

- <internal-server-error/> -- the server has experienced a misconfiguration or an otherwise-undefined internal error that prevents it from servicing the stream.

- <invalid-id/> -- the stream ID or dialback ID is invalid or does not match an ID previously provided.

- <invalid-namespace/> -- the stream namespace name is something other than "http://etherx.jabber.org/streams" or the dialback namespace name is something other than "jabber:server:dialback".

- <nonmatching-hosts/> -- the hostname provided in a 'from' address does not match the hostname (or other validated domain) negotiated via SASL or dialback.

- <not-authorized/> -- the entity has attempted to send data before authenticating, or otherwise is not authorized to perform an action related to stream negotiation; the receiving entity SHOULD silently drop the offending stanza and MUST NOT process it before sending the stream error.

- <remote-connection-failed/> -- the server is unable to properly connect to a remote resource that is required for authentication or authorization.

- <resource-constraint/> -- the server is resource-contrained and is unable to service the stream.

- <see-other-host/> -- the server will not provide service to the initiating entity but is redirecting traffic to another host; this element SHOULD contain CDATA specifying the alternate hostname or IP address to which the initiating entity MAY attempt to connect.

- <system-shutdown/> -- the server is being shut down and all active streams are being closed.

- <unsupported-stanza-type/> -- the initiating entity has sent a first-level child of the stream that is not supported by the server.

- <unsupported-version/> -- the value of the 'version' attribute provided by the initiating entity in the stream header specifies a version of XMPP that is not supported by the server; this element MAY contain CDATA specifying the XMPP version(s) supported by the server.

- <xml-not-well-formed/> -- the initiating entity has sent XML that is not well-formed as defined by the XML specification [1].

#### 4.6.4 Application-Specific Conditions

As noted, an application MAY provide application-specific stream error information by including a properly-namespaced child in the error element. The application-specific element SHOULD supplement or

further qualify a defined element. Thus the <error/> element will contain two or three child elements:

```
<stream:error>
  <xml-not-well-formed
      xmlns='urn:ietf:params:xml:ns:xmpp-streams'/>
    <text xml:lang='en' xmlns='urn:ietf:params:xml:ns:xmpp-streams'>
      Some special application diagnostic information!
    </text>
  <escape-your-data xmlns='application-ns'/>
</stream:error>
</stream:stream>
```

### 4.7 Simple Streams Example

The following is a stream-based session of a client on a server (where the "C" lines are sent from the client to the server, and the "S" lines are sent from the server to the client):

A basic session:

```
C: <?xml version='1.0'?>
   <stream:stream
       to='shakespeare.lit'
       xmlns='jabber:client'
       xmlns:stream='http://etherx.jabber.org/streams'
       version='1.0'>
S: <?xml version='1.0'?>
   <stream:stream
       from='shakespeare.lit'
       id='id_123456789'
       xmlns='jabber:client'
       xmlns:stream='http://etherx.jabber.org/streams'
       version='1.0'>
... authentication ...
C:   <message from='juliet@shakespeare.lit'
              to='romeo@shakespeare.lit'
              xml:lang='en'>
C:     <body>Art thou not Romeo, and a Montague?</body>
C:   </message>
S:   <message from='romeo@shakespeare.lit'
              to='juliet@shakespeare.lit'
              xml:lang='en'>
S:     <body>Neither, fair saint, if either thee dislike.</body>
S:   </message>
C: </stream:stream>
S: </stream:stream>
```

A stream gone bad:

```
C: <?xml version='1.0'?>
   <stream:stream
       to='shakespeare.lit'
       xmlns='jabber:client'
       xmlns:stream='http://etherx.jabber.org/streams'
       version='1.0'>
S: <?xml version='1.0'?>
   <stream:stream
       from='shakespeare.lit'
       id='id_123456789'
       xmlns='jabber:client'
       xmlns:stream='http://etherx.jabber.org/streams'
       version='1.0'>
... authentication ...
C: <message xml:lang='en'>
     <body>Bad XML, no closing body tag!
   </message>
S: <stream:error>
    <xml-not-well-formed
        xmlns='urn:ietf:params:xml:ns:xmpp-streams'/>
   </stream:error>
S: </stream:stream>
```

# 5. Stream Encryption

## 5.1 Overview

XMPP includes a method for securing the stream from tampering and eavesdropping. This channel encryption method makes use of the Transport Layer Security (TLS) [13] protocol, along with a "STARTTLS" extension that is modelled after similar extensions for the IMAP [26], POP3 [27], and ACAP [28] protocols as described in RFC 2595 [29]. The namespace name for the STARTTLS extension is 'urn:ietf:params:xml:ns:xmpp-tls', which adheres to the format defined in The IETF XML Registry [25].

An administrator of a given domain MAY require the use of TLS for client-to-server communications, server-to-server communications, or both. Servers SHOULD use TLS betweeen two domains for the purpose of securing server-to-server communications. See Mandatory to Implement Technologies (Section 12.6) regarding mechanisms that MUST be supported.

The following rules apply:

1. An initiating entity that complies with this specification MUST include the 'version' attribute set to a value of "1.0" in the initiating stream header.

2. If the TLS negotiation occurs between two servers, communications MUST NOT proceed until the DNS hostnames asserted by the servers have been resolved (see Server-to-Server Communications (Section 12.3)).

3. When a receiving entity that complies with this specification receives an initiating stream header that includes the 'version' attribute set to a value of "1.0", after sending a stream header in reply (including the version flag) it MUST include a <starttls/> element (qualified by the 'urn:ietf:params:xml:ns:xmpp-tls' namespace) along with the list of other stream features it supports.

4. If the initiating entity chooses to use TLS for stream encryption, TLS negotiation MUST be completed before proceeding to SASL negotiation.

5. The receiving entity MUST consider the TLS negotiation to have begun immediately after sending the closing ">" of the <proceed/> element. The initiating entity MUST consider the TLS negotiation to have begun immediately after receiving the closing ">" of the <proceed/> element from the receiving entity.

6. The initiating entity MUST validate the certificate presented by the receiving entity; there are two cases:

   Case 1 -- The initiating entity has been configured with a set of trusted root certificates: Normal certificate validation processing is appropriate, and SHOULD follow the rules defined for HTTP over TLS [14]. The trusted roots may be either a well-known public set or a manually configured Root CA (e.g., an organization's own Certificate Authority or a self-signed Root CA for the service as described under High Security (Section 12.1)). This case is RECOMMENDED.

   Case 2 -- The initiating entity has been configured with the receiving entity's self-signed service certificate: Simple comparison of public keys is appropriate. This case is NOT RECOMMENDED (see High Security (Section 12.1) for details).

   If the above methods fail, the certificate SHOULD be presented to a human (e.g., an end user or server administrator) for approval; if presented, the receiver MUST deliver the entire certificate chain to the human, who SHOULD be given the option to store the Root CA certificate (not the service or End Entity certificate) and to not be queried again regarding acceptance of the certificate for some reasonable period of time.

7. If the TLS negotiation is successful, the receiving entity MUST discard any knowledge obtained from the initiating entity before TLS takes effect.

8. If the TLS negotiation is successful, the initiating entity MUST discard any knowledge obtained from the receiving entity before TLS takes effect.

9. If the TLS negotiation is successful, the receiving entity MUST NOT offer the STARTTLS extension to the initiating entity along with the other stream features that are offered when the stream is restarted.

10. If the TLS negotiation is successful, the initiating entity SHOULD continue with SASL negotiation.

11. If the TLS negotiation results in failure, the receiving entity MUST terminate both the XML stream and the underlying TCP connection.

### 5.2 Narrative

When an initiating entity secures a stream with a receiving entity, the steps involved are as follows:

1. The initiating entity opens a TCP connection and initiates the stream by sending the opening XML stream header to the receiving entity, including the 'version' attribute set to a value of "1.0".

2. The receiving entity responds by opening a TCP connection and sending an XML stream header to the initiating entity, including the 'version' attribute set to a value of "1.0".

3. The receiving entity offers the STARTTLS extension to the initiating entity by including it with the list of other supported stream features (if TLS is required for interaction with the receiving entity, it SHOULD signal that fact by including a <required/> element as a child of the <starttls/> element).

4. The initiating entity issues the STARTTLS command (i.e., a <starttls/> element qualified by the 'urn:ietf:params:xml:ns:xmpp-tls' namespace) to instruct the receiving entity that it wishes to begin a TLS negotiation to secure the stream.

5. The receiving entity MUST reply with either a <proceed/> element or a <failure/> element qualified by the 'urn:ietf:params:xml:ns:xmpp-tls' namespace. If the failure case occurs, the receiving entity MUST terminate both the XML stream and the underlying TCP connection. If the proceed case occurs, the receiving entity MUST ignore any further XML data sent over the XML stream but keep the underlying TCP connection open for the purpose of completing the TLS negotiation.

6. The initiating entity and receiving entity attempt to complete a TLS negotiation in accordance with RFC 2246 [13].

7. If the TLS negotiation is unsuccessful, the receiving entity MUST terminate the TCP connection. If the TLS negotiation is successful, the initiating entity MUST initiate a new stream by sending an opening XML stream header to the receiving entity.

8. Upon receiving the new stream header from the initiating entity, the receiving entity MUST respond by sending a new XML stream header to the initiating entity along with the remaining available features (but NOT including the STARTTLS feature).

### 5.3 Client-to-Server Example

The following example shows the data flow for a client securing a stream using STARTTLS (the IANA-registered port 5222 SHOULD be used; see IANA Considerations (Section 10)).

Step 1: Client initiates stream to server:

```
<stream:stream
    xmlns='jabber:client'
    xmlns:stream='http://etherx.jabber.org/streams'
    to='capulet.com'
    version='1.0'>
```

Step 2: Server responds by sending a stream tag to client:

```
<stream:stream
    xmlns='jabber:client'
    xmlns:stream='http://etherx.jabber.org/streams'
    id='12345678'
    from='capulet.com'
    version='1.0'>
```

Step 3: Server sends the STARTTLS extension to client along with authentication mechanisms and any other stream features:

```
<stream:features>
  <starttls xmlns='urn:ietf:params:xml:ns:xmpp-tls'>
    <required/>
  </starttls>
  <mechanisms xmlns='urn:ietf:params:xml:ns:xmpp-sasl'>
    <mechanism>DIGEST-MD5</mechanism>
    <mechanism>PLAIN</mechanism>
  </mechanisms>
</stream:features>
```

Step 4: Client sends the STARTTLS command to server:

```
<starttls xmlns='urn:ietf:params:xml:ns:xmpp-tls'/>
```

Step 5: Server informs client to proceed:

```
<proceed xmlns='urn:ietf:params:xml:ns:xmpp-tls'/>
```

Step 5 (alt): Server informs client that TLS negotiation has failed and closes both stream and TCP connection:

```
<failure xmlns='urn:ietf:params:xml:ns:xmpp-tls'/>
</stream:stream>
```

Step 6: Client and server attempt to complete TLS negotiation over the existing TCP connection.

Step 7: If TLS negotiation is successful, client initiates a new stream to server:

```
<stream:stream
    xmlns='jabber:client'
    xmlns:stream='http://etherx.jabber.org/streams'
    to='capulet.com'
    version='1.0'>
```

Step 7 (alt): If TLS negotiation is unsuccessful, server MUST close TCP connection.

Step 8: Server responds by sending a stream header to client along with any remaining negotiable stream features:

```
<stream:stream
    xmlns='jabber:client'
    xmlns:stream='http://etherx.jabber.org/streams'
    from='capulet.com'
    id='12345678'
    version='1.0'>
<stream:features>
  <mechanisms xmlns='urn:ietf:params:xml:ns:xmpp-sasl'>
    <mechanism>DIGEST-MD5</mechanism>
    <mechanism>PLAIN</mechanism>
    <mechanism>EXTERNAL</mechanism>
  </mechanisms>
</stream:features>
```

Step 9: Client SHOULD continue with Stream Authentication (Section 6).

### 5.4 Server-to-Server Example

The following example shows the data flow for two servers securing a stream using STARTTLS (the IANA-registered port 5269 SHOULD be used; see IANA Considerations (Section 10)).

Step 1: Server1 initiates stream to Server2:

```
<stream:stream
    xmlns='jabber:server'
    xmlns:stream='http://etherx.jabber.org/streams'
    to='montague.net'
    version='1.0'>
```

Step 2: Server2 responds by sending a stream tag to Server1:

```
<stream:stream
    xmlns='jabber:server'
    xmlns:stream='http://etherx.jabber.org/streams'
    from='montague.net'
    id='12345678'
    version='1.0'>
```

Step 3: Server2 sends the STARTTLS extension to Server1 along with authentication mechanisms and any other stream features:

```
<stream:features>
  <starttls xmlns='urn:ietf:params:xml:ns:xmpp-tls'/>
    <required/>
  </starttls>
  <mechanisms xmlns='urn:ietf:params:xml:ns:xmpp-sasl'>
    <mechanism>DIGEST-MD5</mechanism>
    <mechanism>KERBEROS_V4</mechanism>
  </mechanisms>
</stream:features>
```

Step 4: Server1 sends the STARTTLS command to Server2:

```
<starttls xmlns='urn:ietf:params:xml:ns:xmpp-tls'/>
```

Step 5: Server2 informs Server1 to proceed:

```
<proceed xmlns='urn:ietf:params:xml:ns:xmpp-tls'/>
```

Step 5 (alt): Server2 informs Server1 that TLS negotiation has failed and closes stream:

```
<failure xmlns='urn:ietf:params:xml:ns:xmpp-tls'/>
</stream:stream>
```

Step 6: Server1 and Server2 attempt to complete TLS negotiation via TCP.

Step 7: If TLS negotiation is successful, Server1 initiates a new stream to Server2:

```
<stream:stream
    xmlns='jabber:server'
    xmlns:stream='http://etherx.jabber.org/streams'
    to='montague.net'
    version='1.0'>
```

Step 7 (alt): If TLS negotiation is unsuccessful, server MUST close TCP connection.

Step 8: Server2 responds by sending a stream header to Server1 along with any remaining negotiable stream features:

```
<stream:stream
    xmlns='jabber:server'
    xmlns:stream='http://etherx.jabber.org/streams'
    from='montague.net'
    id='12345678'
    version='1.0'>
<stream:features>
  <mechanisms xmlns='urn:ietf:params:xml:ns:xmpp-sasl'>
    <mechanism>DIGEST-MD5</mechanism>
    <mechanism>KERBEROS_V4</mechanism>
    <mechanism>EXTERNAL</mechanism>
  </mechanisms>
</stream:features>
```

Step 9: Server1 SHOULD continue with Stream Authentication (Section 6).

# 6. Stream Authentication

## 6.1 Overview

XMPP includes a method for authenticating a stream using an XMPP adaptation of the Simple Authentication and Security Layer (SASL) [15]. SASL provides a generalized method for adding authentication support to connection-based protocols, and XMPP uses a generic XML namespace profile for SASL that conforms to section 4 ("Profiling Requirements") of RFC 2222 [15] (the XMPP-specific namespace name is 'urn:ietf:params:xml:ns:xmpp-sasl', which adheres to the format defined in The IETF XML Registry [25]). Finally, see Mandatory to Implement Technologies (Section 12.6) regarding mechanisms that MUST be supported.

The following rules apply:

1. If the SASL negotiation occurs between two servers, communications MUST NOT proceed until the DNS hostnames asserted by the servers have been resolved (see Server-to-Server Communications (Section 12.3)).

2. If TLS is used for stream encryption, SASL SHOULD NOT be used for anything except stream authentication (i.e., a security layer SHOULD NOT be negotiated using SASL). Conversely, if a security layer is to be negotiated via SASL, TLS SHOULD NOT be used.

3. If the initiating entity is capable of authenticating via SASL, it MUST include the 'version' attribute set to a value of "1.0" in the initiating stream header.

4. If the receiving entity is capable of negotiating authentication via SASL, it MUST send one or more authentication mechanisms within a <mechanisms/> element qualified by the 'urn:ietf:params:xml:ns:xmpp-sasl' namespace in response to the opening stream tag received from the initiating entity (if the opening stream tag included the 'version' attribute set to a value of "1.0").

5. Upon successful SASL negotiation that involves negotiation of a security layer, the receiving entity MUST discard any knowledge obtained from the initiating entity which was not obtained from the SASL negotiation itself.

6. Upon successful SASL negotiation that involves negotiation of a security layer, the initiating entity MUST discard any knowledge obtained from the receiving entity which was not obtained from the SASL negotiation itself.

7. The initiating entity MUST provide an authzid during SASL negotiation. The authzid-value MUST be a valid JID of the form <domain> (i.e., a domain identifier only) for servers and of the form <user@domain/resource> (i.e., node identifier, domain identifier, and resource identifier) for clients. The initiating entity MAY process the authzid-value in accordance with the rules defined in Addressing Scheme (Section 3) before providing it to the receiving entity, but is NOT REQUIRED to do so.

8. Any character data contained within the XML elements used during SASL negotiation MUST be encoded using base64.

### 6.2 Narrative

When an initiating entity authenticates with a receiving entity, the steps involved are as follows:

1. The initiating entity requests SASL authentication by including the 'version' attribute in the opening XML stream header sent to the receiving entity, with the value set to "1.0".

2. After sending an XML stream header in response, the receiving entity sends a list of available SASL authentication mechanisms; each of these is a <mechanism/> element included as a child within a <mechanisms/> container element qualified by the 'urn:ietf:params:xml:ns:xmpp-sasl' namespace, which in turn is a child of a <features/> element in the streams namespace. If channel encryption needs to be established before a particular authentication mechanism may be used, the receiving entity MUST NOT provide that mechanism in the list of available SASL authentication methods prior to channel encryption. If the initiating entity presents a valid certificate during prior TLS negotiation, the receiving entity MAY offer the SASL EXTERNAL mechanism to the initiating entity during stream authentication (refer to RFC 2222 [15]).

3. The initiating entity selects a mechanism by sending an <auth/> element qualified by the 'urn:ietf:params:xml:ns:xmpp-sasl' namespace to the receiving entity and including an appropriate value for the 'mechanism' attribute; this element MAY optionally contain character data (in SASL terminology the "initial response") if the mechanism supports or requires it. If the initiating entity selects the EXTERNAL mechanism for authentication, the authentication credentials shall be taken from the certificate presented during prior TLS negotiation.

4. If necessary, the receiving entity challenges the initiating

entity by sending a <challenge/> element qualified by the 'urn:ietf:params:xml:ns:xmpp-sasl' namespace to the initiating entity; this element MAY optionally contain character data (which MUST be computed in accordance with the SASL mechanism chosen by the initiating entity).

5. The initiating entity responds to the challenge by sending a <response/> element qualified by the 'urn:ietf:params:xml:ns:xmpp-sasl' namespace to the receiving entity; this element MAY optionally contain character data (which MUST be computed in accordance with the SASL mechanism chosen by the initiating entity).

6. If necessary, the receiving entity sends more challenges and the initiating entity sends more responses.

This series of challenge/response pairs continues until one of three things happens:

1. The initiating entity aborts the handshake by sending an <abort/> element qualified by the 'urn:ietf:params:xml:ns:xmpp-sasl' namespace to the receiving entity. Upon receiving the <abort/> element, the receiving entity MUST terminate the TCP connection.

2. The receiving entity reports failure of the handshake by sending a <failure/> element qualified by the 'urn:ietf:params:xml:ns:xmpp-sasl' namespace to the initiating entity (the particular cause of failure SHOULD be communicated in an appropriate child element of the <failure/> element as defined under SASL Errors (Section 6.3)). Immediately after sending the <failure/> element, the receiving entity MUST terminate the TCP connection.

3. The receiving entity reports success of the handshake by sending a <success/> element qualified by the 'urn:ietf:params:xml:ns:xmpp-sasl' namespace to the initiating entity; this element MAY optionally contain character data (in SASL terminology "additional data with success"). Upon receiving the <success/> element, the initiating entity MUST initiate a new stream by sending an opening XML stream header to the receiving entity (it is not necessary to send a closing </stream:stream> element first, since the receiving entity and initiating entity MUST consider the original stream to be closed upon sending or receiving the <success/> element). Upon receiving the new stream header from the initiating entity, the receiving entity MUST respond by sending a new XML stream header to the initiating entity, along with any remaining available features (but NOT including the STARTTLS feature or any authentication mechanisms)

or an empty features element (to signify that no additional features are available); note that any such additional features are not defined herein, and MUST be defined by the relevant extension to XMPP.

### 6.3 SASL Errors

The following SASL-related error conditions are defined:

- <bad-protocol/> -- The data provided by the initiating entity does not adhere to the protocol for the requested mechanism; sent in response to the <response/> element.

- <encryption-required/> -- The mechanism chosen by the initiating entity may be used only if the stream is already encrypted; sent in response to the <auth/> element.

- <invalid-authzid/> -- The authzid provided by the initiating entity is invalid, either because it is incorrectly formatted or because the initiating entity does not have permissions to authorize that ID; sent in response to a <response/> element.

- <invalid-mechanism/> -- The initiating entity did not provide a mechanism or requested a mechanism that is not supported by the receiving entity; sent in response to the <auth/> element.

- <invalid-realm/> -- The realm provided by the initiating entity (in mechanisms that support the concept of a realm) does not match one of the hostnames served by the receiving entity; sent in response to a <response/> element.

- <mechanism-too-weak/> -- The mechanism requested by the initiating entity is weaker than server policy permits for that initiating entity; sent in response to the <response/> element.

- <not-authorized/> -- The authentication failed because the initiating entity did not provide valid credentials (this includes the case of an unknown username); sent in response to a <response/> element.

- <temporary-auth-failure/> -- The authentication failed because of a temporary error condition within the receiving entity; sent in response to an <auth/> element or <response/> element.

### 6.4 SASL Definition

Section 4 of the SASL specification [15] requires that the following information be supplied by a protocol definition:

service name: "xmpp"

initiation sequence: After the initiating entity provides an opening XML stream header and the receiving entity replies in kind, the receiving entity provides a list of acceptable authentication methods. The initiating entity chooses one method from the list and sends it to the receiving entity as the value of the 'mechanism' attribute possessed by an <auth/> element, optionally including an initial response to avoid a round trip.

exchange sequence: Challenges and responses are carried through the exchange of <challenge/> elements from receiving entity to initiating entity and <response/> elements from initiating entity to receiving entity. The receiving entity reports failure by sending a <failure/> element and success by sending a <success/> element; the initiating entity aborts the exchange by sending an <abort/> element. (All of these elements are qualified by the 'urn:ietf:params:xml:ns:xmpp-sasl' namespace.) Upon successful negotiation, both sides consider the original XML stream closed and new <stream> headers are sent by both entities.

security layer negotiation: The security layer takes effect immediately after sending the closing ">" character of the <success/> element for the server, and immediately after receiving the closing ">" character of the <success/> element for the client (this element is qualified by the 'urn:ietf:params:xml:ns:xmpp-sasl' namespace).

use of the authorization identity: The authorization identity is used by xmpp to denote the "full JID" (<user@domain/resource>) of a client or the sending domain of a server.

### 6.5 Client-to-Server Example

The following example shows the data flow for a client authenticating with a server using SASL (the IANA-registered port 5222 SHOULD be used; see IANA Considerations (Section 10)).

Step 1: Client initiates stream to server:

```
<stream:stream
    xmlns='jabber:client'
    xmlns:stream='http://etherx.jabber.org/streams'
    to='capulet.com'
    version='1.0'>
```

Step 2: Server responds with a stream tag sent to client:

```
<stream:stream
    xmlns='jabber:client'
    xmlns:stream='http://etherx.jabber.org/streams'
    id='12345678'
    from='capulet.com'
    version='1.0'>
```

Step 3: Server informs client of available authentication mechanisms:

```
<stream:features>
  <mechanisms xmlns='urn:ietf:params:xml:ns:xmpp-sasl'>
    <mechanism>DIGEST-MD5</mechanism>
    <mechanism>PLAIN</mechanism>
  </mechanisms>
</stream:features>
```

Step 4: Client selects an authentication mechanism:

```
<auth
    xmlns='urn:ietf:params:xml:ns:xmpp-sasl'
    mechanism='DIGEST-MD5'/>
```

Step 5: Server sends a base64-encoded challenge to client:

```
<challenge xmlns='urn:ietf:params:xml:ns:xmpp-sasl'>
    cmVhbG09ImNhdGFjbHlzbS5jeCIsbm9uY2U9Ik9BNk1HOXRFUUdtMmhoIi
    xxb3A9ImF1dGgiLGNoYXJzZXQ9dXRmLTgsYWxnb3JpdGhtPW1kNS1zZXNz
</challenge>
```

The decoded challenge is:

```
realm="cataclysm.cx",nonce="OA6MG9tEQGm2hh",\
qop="auth",charset=utf-8,algorithm=md5-sess
```

Step 5 (alt): Server returns error to client:

```
<failure xmlns='urn:ietf:params:xml:ns:xmpp-sasl'>
  <mechanism-too-weak/>
</failure>
```

Step 6: Client responds to the challenge:

```
<response xmlns='urn:ietf:params:xml:ns:xmpp-sasl'>
    dXNlcm5hbWU9InJvYiIscmVhbG09ImNhdGFjbHlzbS5jeCIsbm9uY2U9Ik
    9BNk1HOXRFUUdtMmhoIixjbm9uY2U9Ik9BNk1IWGg2VnFUclJrIixuYz0w
    MDAwMDAwMSxxb3A9YXV0aCxkaWdlc3QtdXJpPSJ4bXBwL2NhdGFjbHlzbS
    5jeCIscmVzcG9uc2U9ZDM4OGRhZDkwZDRiYmQ3NjBhMTUyMzIxZjIxNDNh
    ZjcsY2hhcnNldD11dGYtOCxhdXRoemlkPSJyb2JAY2F0YWNseXNtLmN4L2
    15UmVzb3VyY2Ui
</response>
```

The decoded response is:

```
username="rob",realm="cataclysm.cx",\
nonce="OA6MG9tEQGm2hh",cnonce="OA6MHXh6VqTrRk",\
nc=00000001,qop=auth,digest-uri="xmpp/cataclysm.cx",\
response=d388dad90d4bbd760a152321f2143af7,charset=utf-8,\
authzid="rob@cataclysm.cx/myResource"
```

Step 7: Server sends another challenge to client:

```
<challenge xmlns='urn:ietf:params:xml:ns:xmpp-sasl'>
    cnNwYXV0aD1lYTQwZjYwMzM1YzQyN2I1NTI3Yjg0ZGJhYmNkZmZmZA==
</challenge>
```

The decoded challenge is:

```
rspauth=ea40f60335c427b5527b84dbabcdfffd
```

Step 7 (alt): Server returns error to client:

```
<failure xmlns='urn:ietf:params:xml:ns:xmpp-sasl'>
  <invalid-realm/>
</failure>
```

Step 8: Client responds to the challenge:

```
<response xmlns='urn:ietf:params:xml:ns:xmpp-sasl'/>
```

Step 9: Server informs client of successful authentication:

```
<success xmlns='urn:ietf:params:xml:ns:xmpp-sasl'/>
```

Step 9 (alt): Server informs client of failed authentication:

```
<failure xmlns='urn:ietf:params:xml:ns:xmpp-sasl'>
  <temporary-auth-failure/>
</failure>
```

Step 10: Client initiates a new stream to server:

```
<stream:stream
    xmlns='jabber:client'
    xmlns:stream='http://etherx.jabber.org/streams'
    to='capulet.com'
    version='1.0'>
```

Step 11: Server responds by sending a stream header to client along with any additional features (or an empty features element):

```
<stream:stream
    xmlns='jabber:client'
    xmlns:stream='http://etherx.jabber.org/streams'
    id='12345678'
    from='capulet.com'
    version='1.0'>
<stream:features/>
```

### 6.6 Server-to-Server Example

The following example shows the data flow for a server authenticating with another server using SASL (the IANA-registered port 5269 SHOULD be used; see IANA Considerations (Section 10)).

Step 1: Server1 initiates stream to Server2:

```
<stream:stream
    xmlns='jabber:server'
    xmlns:stream='http://etherx.jabber.org/streams'
    to='montague.net'
    version='1.0'>
```

Step 2: Server2 responds with a stream tag sent to Server1:

```
<stream:stream
    xmlns='jabber:server'
    xmlns:stream='http://etherx.jabber.org/streams'
    from='montague.net'
    id='12345678'
    version='1.0'>
```

Step 3: Server2 informs Server1 of available authentication mechanisms:

```
<stream:features>
  <mechanisms xmlns='urn:ietf:params:xml:ns:xmpp-sasl'>
    <mechanism>DIGEST-MD5</mechanism>
    <mechanism>KERBEROS_V4</mechanism>
  </mechanisms>
</stream:features>
```

Step 4: Server1 selects an authentication mechanism:

```
<auth
    xmlns='urn:ietf:params:xml:ns:xmpp-sasl'
    mechanism='DIGEST-MD5'/>
```

Step 5: Server2 sends a base64-encoded challenge to Server1:

```
<challenge xmlns='urn:ietf:params:xml:ns:xmpp-sasl'>
    cmVhbG09ImNhdGFjbHlzbS5jeCIsbm9uY2U9Ik9BNk1HOXRFUUdtMmhoIi
    xxb3A9ImF1dGgiLGNoYXJzZXQ9dXRmLTgsYWxnb3JpdGhtPW1kNS1zZXNz
</challenge>
```

The decoded challenge is:

```
realm="cataclysm.cx",nonce="OA6MG9tEQGm2hh",\
qop="auth",charset=utf-8,algorithm=md5-sess
```

Step 5 (alt): Server2 returns error to Server1:

```
<failure xmlns='urn:ietf:params:xml:ns:xmpp-sasl'>
  <encryption-required/>
</failure>
```

Step 6: Server1 responds to the challenge:

```
<response xmlns='urn:ietf:params:xml:ns:xmpp-sasl'>
    cmVhbG09ImNhdGFjbHlzbS5jeCIsbm9uY2U9Ik9BNk1HOXRFUUdtMmhoIi
    xjbm9uY2U9Ik9BNk1IWGg2VnFUclJrIixuYz0wMDAwMDAwMSxxb3A9YXV0
    aCxkaWdlc3QtdXJpPSJ4bXBwL2NhdGFjbHlzbS5jeCIscmVzcG9uc2U9ZD
    M4OGRhZDkwZDRiYmQ3NjBhMTUyMzIxZjIxNDNhZjcsY2hhcnNldD11dGYt
    OAo=
</response>
```

The decoded response is:

```
realm="cataclysm.cx",nonce="OA6MG9tEQGm2hh",cnonce="OA6MHXh6VqTrRk",\
nc=00000001,qop=auth,digest-uri="xmpp/cataclysm.cx",\
response=d388dad90d4bbd760a152321f2143af7,charset=utf-8
```

Step 7: Server2 sends another challenge to Server1:

```
<challenge xmlns='urn:ietf:params:xml:ns:xmpp-sasl'>
    cnNwYXV0aD1lYTQwZjYwMzM1YzQyN2I1NTI3Yjg0ZGJhYmNkZmZmZA==
</challenge>
```

The decoded challenge is:

```
rspauth=ea40f60335c427b5527b84dbabcdfffd
```

Step 5 (alt): Server2 returns error to Server1:

```
<failure xmlns='urn:ietf:params:xml:ns:xmpp-sasl'>
  <invalid-authzid/>
</failure>
```

Step 8: Server1 responds to the challenge:

```
<response xmlns='urn:ietf:params:xml:ns:xmpp-sasl'/>
```

Step 9: Server2 informs Server1 of successful authentication:

```
<success xmlns='urn:ietf:params:xml:ns:xmpp-sasl'/>
```

Step 9 (alt): Server2 informs Server1 of failed authentication:

```
<failure xmlns='urn:ietf:params:xml:ns:xmpp-sasl'>
  <temporary-auth-failure/>
</failure>
```

Step 10: Server1 initiates a new stream to Server2:

```
<stream:stream
    xmlns='jabber:server'
    xmlns:stream='http://etherx.jabber.org/streams'
    to='montague.net'
    version='1.0'>
```

Step 11: Server2 responds by sending a stream header to Server1 along with any additional features (or an empty features element):

```
<stream:stream
    xmlns='jabber:client'
    xmlns:stream='http://etherx.jabber.org/streams'
    from='montague.net'
    id='12345678'
    version='1.0'>
<stream:features/>
```

# 7. Server Dialback

## 7.1 Overview

The Jabber protocol from which XMPP was adapted includes a "server dialback" method for protecting against domain spoofing, thus making it more difficult to spoof XML stanzas (see Server-to-Server Communications (Section 12.3) regarding this method's security characteristics). Server dialback also makes it easier to deploy systems in which outbound messages and inbound messages are handled by different machines for the same domain. The server dialback method is made possible by the existence of DNS, since one server can (normally) discover the authoritative server for a given domain.

Because dialback depends on the Domain Name System, inter-domain communications MUST NOT proceed until the DNS hostnames asserted by the servers have been resolved (see Server-to-Server Communications (Section 12.3)).

The method for generating and verifying the keys used in server dialback MUST take into account the hostnames being used, the random ID generated for the stream, and a secret known by the authoritative server's network.

Any error that occurs during dialback negotiation MUST be considered a stream error, resulting in termination of the stream and of the underlying TCP connection. The possible error conditions are specified in the protocol description below.

The following terminology applies:

- Originating Server -- the server that is attempting to establish a connection between two domains.

- Receiving Server -- the server that is trying to authenticate that Originating Server represents the domain which it claims to be.

- Authoritative Server -- the server that answers to the DNS hostname asserted by Originating Server; for basic environments this will be Originating Server, but it could be a separate machine in Originating Server's network.

The following is a brief summary of the order of events in dialback:

1. Originating Server establishes a connection to Receiving Server.

2. Originating Server sends a 'key' value over the connection to Receiving Server.

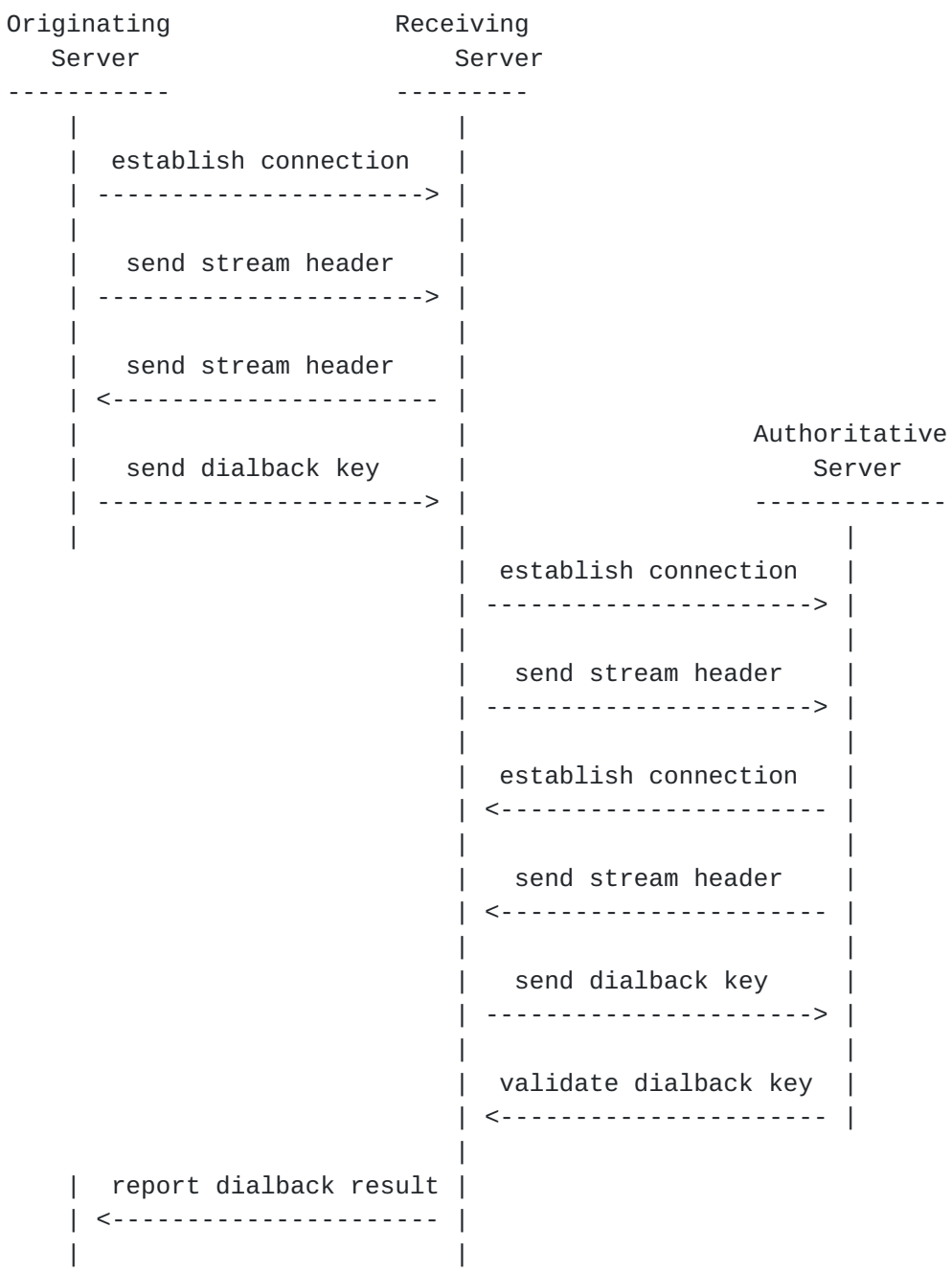
3. Receiving Server establishes a connection to Authoritative Server.

4. Receiving Server sends the same 'key' value to Authoritative Server.

5. Authoritative Server replies that key is valid or invalid.

6. Receiving Server informs Originating Server whether it is authenticated or not.

We can represent this flow of events graphically as follows:




## 7.2 Protocol

The interaction between the servers is as follows:

1. Originating Server establishes TCP connection to Receiving Server.

2. Originating Server sends a stream header to Receiving Server:

```
<stream:stream
    xmlns:stream='http://etherx.jabber.org/streams'
    xmlns='jabber:server'
    xmlns:db='jabber:server:dialback'>
```

Note: the 'to' and 'from' attributes are NOT REQUIRED on the root stream element. The inclusion of the xmlns:db namespace declaration with the name shown indicates to Receiving Server that Originating Server supports dialback. If the namespace name is incorrect, then Receiving Server MUST generate an <invalid-namespace/> stream error condition and terminate both the XML stream and the underlying TCP connection.

3. Receiving Server SHOULD send a stream header back to Originating Server, including a unique ID for this interaction:

```
<stream:stream
    xmlns:stream='http://etherx.jabber.org/streams'
    xmlns='jabber:server'
    xmlns:db='jabber:server:dialback'
    id='457F9224A0...'>
```

Note: The 'to' and 'from' attributes are NOT REQUIRED on the root stream element. If the namespace name is incorrect, then Originating Server MUST generate an <invalid-namespace/> stream error condition and terminate both the XML stream and the underlying TCP connection. Note well that Receiving Server is NOT REQUIRED to reply and MAY silently terminate the XML stream and underlying TCP connection depending on security policies in place.

4. Originating Server sends a dialback key to Receiving Server:

```
<db:result
    to='Receiving Server'
    from='Originating Server'>
  98AF014EDC0...
</db:result>
```

Note: this key is not examined by Receiving Server, since Receiving Server does not keep information about Originating Server between sessions. The key generated by Originating Server MUST be based in part on the value of the ID provided by Receiving Server in the previous step, and in part on a secret shared by Originating Server and Authoritative Server. If the value of the 'to' address does not match a hostname recognized by Receiving Server, then Receiving Server MUST generate a <host-unknown/> stream error condition and terminate both the

XML stream and the underlying TCP connection. If the value of the 'from' address matches a domain with which Receiving Server already has an established connection, then Receiving Server MUST maintain the existing connection until it validates whether the new connection is legitimate; additionally, Receiving Server MAY choose to generate a <not-authorized/> stream error condition for the new connection and then terminate both the XML stream and the underlying TCP connection related to the new request.

5. Receiving Server establishes a TCP connection back to the domain name asserted by Originating Server, as a result of which it connects to Authoritative Server. (Note: as an optimization, an implementation MAY reuse an existing trusted connection here rather than opening a new TCP connection.)

6. Receiving Server sends Authoritative Server a stream header:

```
<stream:stream
    xmlns:stream='http://etherx.jabber.org/streams'
    xmlns='jabber:server'
    xmlns:db='jabber:server:dialback'>
```

Note: the 'to' and 'from' attributes are NOT REQUIRED on the root stream element. If the namespace name is incorrect, then Authoritative Server MUST generate an <invalid-namespace/> stream error condition and terminate both the XML stream and the underlying TCP connection.

7. Authoritative Server sends Receiving Server a stream header:

```
<stream:stream
    xmlns:stream='http://etherx.jabber.org/streams'
    xmlns='jabber:server'
    xmlns:db='jabber:server:dialback'
    id='1251A342B...'>
```

Note: if the namespace name is incorrect, then Receiving Server MUST generate an <invalid-namespace/> stream error condition and terminate both the XML stream and the underlying TCP connection between it and Authoritative Server. If the ID does not match that provided by Receiving Server in Step 3, then Receiving Server MUST generate an <invalid-id/> stream error condition and terminate both the XML stream and the underlying TCP connection between it and Authoritative Server. If either of the foregoing stream errors occurs between Receiving Server and Authoritative Server, then Receiving Server MUST generate a <remote-connection-failed/> stream error condition and terminate

both the XML stream and the underlying TCP connection between it and Originating Server.

8. Receiving Server sends Authoritative Server a stanza requesting that Authoritative Server verify a key:

```
<db:verify
    from='Receiving Server'
    to='Originating Server'
    id='457F9224A0...'>
  98AF014EDC0...
</db:verify>
```

Note: passed here are the hostnames, the original identifier from Receiving Server's stream header to Originating Server in Step 3, and the key that Originating Server sent to Receiving Server in Step 4. Based on this information as well as shared secret information within the Authoritative Server's network, the key is verified. Any verifiable method MAY be used to generate the key. If the value of the 'to' address does not match a hostname recognized by Authoritative Server, then Authoritative Server MUST generate a <host-unknown/> stream error condition and terminate both the XML stream and the underlying TCP connection. If the value of the 'from' address does not match the hostname represented by Receiving Server when opening the TCP connection (or any validated domain), then Authoritative Server MUST generate a <nonmatching-hosts/> stream error condition and terminate both the XML stream and the underlying TCP connection.

9. Authoritative Server sends a stanza back to Receiving Server verifying whether the key was valid or invalid:

```
<db:verify
    from='Originating Server'
    to='Receiving Server'
    type='valid'
    id='457F9224A0...'/>
```

or

```
<db:verify
    from='Originating Server'
    to='Receiving Server'
    type='invalid'
    id='457F9224A0...'/>
```

Note: if the ID does not match that provided by Receiving Server

in Step 3, then Receiving Server MUST generate an <invalid-id/> stream error condition and terminate both the XML stream and the underlying TCP connection. If the value of the 'to' address does not match a hostname recognized by Receiving Server, then Receiving Server MUST generate a <host-unknown/> stream error condition and terminate both the XML stream and the underlying TCP connection. If the value of the 'from' address does not match the hostname represented by Originating Server when opening the TCP connection (or any validated domain), then Receiving Server MUST generate a <nonmatching-hosts/> stream error condition and terminate both the XML stream and the underlying TCP connection.

10. Receiving Server informs Originating Server of the result:

```
<db:result
    from='Receiving Server'
    to='Originating Server'
    type='valid'/>
```

Note: At this point the connection has either been validated via a type='valid', or reported as invalid. If the connection is invalid, then Receiving Server MUST terminate both the XML stream and the underlying TCP connection. If the connection is validated, data can be sent by Originating Server and read by Receiving Server; before that, all data stanzas sent to Receiving Server SHOULD be silently dropped.

Even if dialback negotiation is successful, a server MUST verify that all XML stanzas received from the other server include a 'from' attribute and a 'to' attribute; if a stanza does not meet this restriction, the server that receives the stanza MUST generate an <improper-addressing/> stream error condition and terminate both the XML stream and the underlying TCP connection. Furthermore, a server MUST verify that the 'from' attribute of stanzas received from the other server includes a validated domain for the stream; if a stanza does not meet this restriction, the server that receives the stanza MUST generate a <nonmatching-hosts/> stream error condition and terminate both the XML stream and the underlying TCP connection. Both of these checks help to prevent spoofing related to particular stanzas.

# 8. XML Stanzas

## 8.1 Overview

Once XML streams in both directions have been authenticated and (if desired) encrypted, XML stanzas can be sent over the streams. Three XML stanza types are defined for the 'jabber:client' and 'jabber:server' namespaces: <message/>, <presence/>, and <iq/>.

In essence, the <message/> stanza type can be seen as a "push" mechanism whereby one entity pushes information to another entity, similar to the communications that occur in a system such as email. The <presence/> element can be seen as a basic broadcast or "publish-subscribe" mechanism, whereby multiple entities receive information (in this case, presence information) about an entity to which they have subscribed. The <iq/> element can be seen as a "request-response" mechanism similar to HTTP, whereby two entities can engage in a structured conversation using 'get' or 'set' requests and 'result' or 'error' responses.

## 8.2 Common Attributes

The following five attributes are common to message, presence, and IQ stanzas:

### 8.2.1 to

The 'to' attribute specifies the JID of the intended recipient for the stanza.

In the 'jabber:client' namespace, a stanza SHOULD possess a 'to' attribute, although a stanza sent from a client to a server for handling by that server (e.g., presence sent to the server for broadcasting to other entities) SHOULD NOT possess a 'to' attribute.

In the 'jabber:server' namespace, a stanza MUST possess a 'to' attribute; if a server receives a stanza that does not meet this restriction, it MUST generate an <improper-addressing/> stream error condition and terminate both the XML stream and the underlying TCP connection with the offending server.

If the value of the 'to' attribute is invalid or cannot be contacted, the entity discovering that fact (usually the sender's or recipient's server) MUST return an appropriate error to the sender.

### 8.2.2 from

The 'from' attribute specifies the JID of the sender.

In the 'jabber:client' namespace, a client MUST NOT include a 'from' attribute on the stanzas it sends to a server; if a server receives an XML stanza from a client and the stanza possesses a 'from' attribute, it MUST ignore the value of the 'from' attribute and MAY return an error to the sender. When a client sends an XML stanza within the context of an authenticated stream, the server MUST stamp the stanza with the full JID (<user@domain/resource>) of the connected resource that generated the stanza as defined by the authzid provided in the SASL negotiation. If a client attempts to send an XML stanza before the stream is authenticated, the server SHOULD return a <not-authorized/> stream error to the client and then terminate both the XML stream and the underlying TCP connection.

In the 'jabber:server' namespace, a stanza MUST possess a 'from' attribute; if a server receives a stanza that does not meet this restriction, it MUST generate an <improper-addressing/> stream error condition. Furthermore, the domain identifier portion of the JID contained in the 'from' attribute MUST match the hostname of the sending server (or any validated domain) as communicated in the SASL negotiation or dialback negotiation; if a server receives a stanza that does not meet this restriction, it MUST generate a <nonmatching-hosts/> stream error condition. Both of these conditions MUST result in closing of the stream and termination of the underlying TCP connection.

### 8.2.3 id

The optional 'id' attribute MAY be used by a sending entity for internal tracking of stanzas that it sends and receives (especially for tracking the request-response interaction inherent in the use of IQ stanzas). If the stanza sent by the sending entity is an IQ stanza of type "get" or "set", the receiving entity MUST include an 'id' attribute with the same value in any replies of type "result" or "error". The value of the 'id' attribute is NOT REQUIRED to be unique either globally, within a domain, or within a stream.

### 8.2.4 type

The 'type' attribute specifies detailed information about the purpose or context of the message, presence, or IQ stanza. The particular allowable values for the 'type' attribute vary depending on whether the stanza is a message, presence, or IQ, and thus are defined in the following sections.

### 8.2.5 xml:lang

A stanza SHOULD possess an 'xml:lang' attribute (as defined in Section 2.12 of the XML specification [1]) if the stanza contains XML

character data that is intended to be presented to a human user (as explained in RFC 2277 [31], "internationalization is for humans"). The value of the 'xml:lang' attribute specifies the default language of any such XML character data, which MAY be overridden by the 'xml:lang' attribute of a specific child element. The value of the attribute MUST be an NMTOKEN and MUST conform to the format defined in RFC 3066 [17].

### 8.3 Message Stanzas

Message stanzas in the 'jabber:client' or 'jabber:server' namespace are used to "push" information to another entity. Common uses in the context of instant messaging include single messages, messages sent in the context of a chat conversation, messages sent in the context of a multi-user chat room, headlines, and errors.

#### 8.3.1 Types of Message

The 'type' attribute of a message stanza is RECOMMENDED; if included, it specifies the conversational context of the message. The 'type' attribute SHOULD have one of the following values:

- chat
- error
- groupchat
- headline
- normal

A message stanza with a different value, or without a 'type' attribute, SHOULD be handled as if the 'type' were "normal".

For information regarding the meaning of these message types in the context of XMPP-based instant messaging and presence applications, refer to XMPP IM [23].

#### 8.3.2 Children

As described under extended namespaces (Section 8.6), a message stanza MAY contain any properly-namespaced child element.

In accordance with the default namespace declaration, by default a message stanza is in the 'jabber:client' or 'jabber:server' namespace, which defines certain allowable children of message stanzas. If the message stanza is of type "error", it MUST include an

<error/> child; for details, see Stanza Errors (Section 8.7). Otherwise, the message stanza MAY contain any of the following child elements without an explicit namespace declaration:

1. <subject/>

2. <body/>

3. <thread/>

#### 8.3.2.1 Subject

The <subject/> element specifies the topic of the message. The <subject/> element SHOULD NOT possess any attributes, with the exception of the 'xml:lang' attribute. Multiple instances of the <subject/> element MAY be included for the purpose of providing alternate versions of the same subject, but only if each instance possesses an 'xml:lang' attribute with a distinct language value. The <subject/> element MUST NOT contain mixed content.

#### 8.3.2.2 Body

The <body/> element contains the textual contents of the message; this child element is normally included but NOT REQUIRED. The <body/> element SHOULD NOT possess any attributes, with the exception of the 'xml:lang' attribute. Multiple instances of the <body/> element MAY be included but only if each instance possesses an 'xml:lang' attribute with a distinct language value. The <body/> element MUST NOT contain mixed content.

#### 8.3.2.3 Thread

The <thread/> element contains a string that is generated by the sender and that SHOULD be copied back in replies; it is used for tracking a conversation thread (sometimes referred to as an "instant messaging session") between two entities. If used, it MUST be unique to that conversation thread within the stream and MUST be consistent throughout that conversation (a client that receives a message from the same full JID but with a different thread ID MUST assume that the message in question exists outside the context of the existing conversation thread). The use of the <thread/> element is OPTIONAL and is not used to identify individual messages, only conversations. Only one <thread/> element MAY be included in a message stanza, and it MUST NOT possess any attributes. The <thread/> element MUST be treated as an opaque string by entities; no semantic meaning may be derived from it, and only exact comparisons may be made against it. The <thread/> element MUST NOT contain mixed content.

### 8.4 Presence Stanzas

Presence stanzas are used in the 'jabber:client' or 'jabber:server' namespace to express an entity's current availability status (offline or online, along with various sub-states of the latter and optional user-defined descriptive text) and to communicate that status to other entities. Presence stanzas are also used to negotiate and manage subscriptions to the presence of other entities.

#### 8.4.1 Types of Presence

The 'type' attribute of a presence stanza is OPTIONAL. A presence stanza that does not possess a 'type' attribute is used to signal to the server that the sender is online and available for communication. If included, the 'type' attribute specifies a lack of availability, a request to manage a subscription to another entity's presence, a request for another entity's current presence, or an error related to a previously-sent presence stanza. The 'type' attribute MAY have one of the following values:

- unavailable -- Signals that the entity is no longer available for communication.
- subscribe -- The sender wishes to subscribe to the recipient's presence.
- subscribed -- The sender has allowed the recipient to receive their presence.
- unsubscribe -- A notification that an entity is unsubscribing from another entity's presence.
- unsubscribed -- The subscription request has been denied or a previously-granted subscription has been cancelled.
- probe -- A request for an entity's current presence; in general, SHOULD NOT be sent by a client.
- error -- An error has occurred regarding processing or delivery of a previously-sent presence stanza.

For information regarding presence semantics and the subscription model used in the context of XMPP-based instant messaging and presence applications, refer to XMPP IM [23].

#### 8.4.2 Children

As described under extended namespaces (Section 8.6), a presence

stanza MAY contain any properly-namespaced child element.

In accordance with the default namespace declaration, by default a presence stanza is in the 'jabber:client' or 'jabber:server' namespace, which defines certain allowable children of presence stanzas. If the presence stanza is of type "error", it MUST include an <error/> child; for details, see Stanza Errors (Section 8.7). If the presence stanza possesses no 'type' attribute, it MAY contain any of the following child elements (note that the <status/> child MAY be sent in a presence stanza of type "unavailable" or, for historical reasons, "subscribe"):

1. <show/>

2. <status/>

3. <priority/>

#### 8.4.2.1 Show

The OPTIONAL <show/> element specifies the particular availability status of an entity or specific resource (if a <show/> element is not provided, default availability is assumed). Only one <show/> element MAY be included in a presence stanza, and it SHOULD NOT possess any attributes. The CDATA value SHOULD be one of the following (values other than these four SHOULD be ignored; additional availability types could be defined through a properly-namespaced child element of the presence stanza):

- away
- chat
- dnd
- xa

For information regarding the meaning of these values in the context of XMPP-based instant messaging and presence applications, refer to XMPP IM [23].

#### 8.4.2.2 Status

The OPTIONAL <status/> element contains a natural-language description of availability status. It is normally used in conjunction with the show element to provide a detailed description of an availability state (e.g., "In a meeting"). The <status/>

element SHOULD NOT possess any attributes, with the exception of the 'xml:lang' attribute. Multiple instances of the <status/> element MAY be included but only if each instance possesses an 'xml:lang' attribute with a distinct language value.

#### 8.4.2.3 Priority

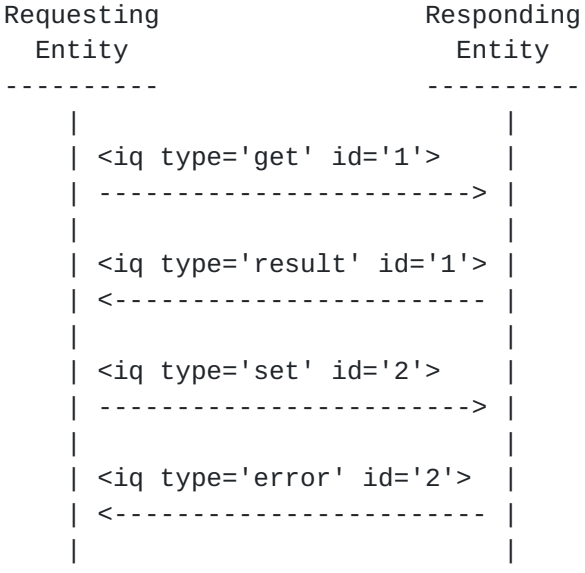
The OPTIONAL <priority/> element specifies the priority level of the connected resource. The value may be any integer between -128 and +127. Only one <priority/> element MAY be included in a presence stanza, and it MUST NOT possess any attributes. If no priority is provided, a server SHOULD consider the priority to be zero. For information regarding the semantics of priority values in stanza routing within instant messaging applications, refer to XMPP IM [23].

## 8.5 IQ Stanzas

### 8.5.1 Overview

Info/Query, or IQ, is a request-response mechanism, similar in some ways to HTTP [32]. IQ stanzas in the 'jabber:client' or 'jabber:server' namespace enable an entity to make a request of, and receive a response from, another entity. The data content of the request and response is defined by the namespace declaration of a direct child element of the IQ element, and the interaction is tracked by the requesting entity through use of the 'id' attribute.

Most IQ interactions follow a common pattern of structured data exchange such as get/result or set/result (although an error may be returned in response to a request if appropriate):



An entity that receives an IQ request of type "get" or "set" MUST reply with an IQ response of type "result" or "error" (which response MUST preserve the 'id' attribute of the request, if provided). An entity that receives a stanza of type "result" or "error" MUST NOT respond to the stanza by sending a further IQ response of type "result" or "error"; however, as shown above, the requesting entity MAY send another request (e.g., an IQ of type "set" in order to provide required information discovered through a get/result pair).

### 8.5.2 Types of IQ

The 'type' attribute of an IQ stanza is REQUIRED. The 'type' attribute specifies a distinct step within a request-response interaction. The value SHOULD be one of the following (all other values SHOULD be ignored):

- get -- The stanza is a request for information or requirements.
- set -- The stanza provides required data, sets new values, or replaces existing values.
- result -- The stanza is a response to a successful get or set request.
- error -- An error has occurred regarding processing or delivery of a previously-sent get or set.

### 8.5.3 Children

As described under extended namespaces (Section 8.6), an IQ stanza MAY contain any properly-namespaced child element. Note that an IQ stanza of type "get", "set", or "result" contains no children in the 'jabber:client' or 'jabber:server' namespace since it is a vessel for XML in another namespace.

An IQ stanza of type "get" or "set" MUST include one and only one child element. An IQ stanza of type "result" MUST include zero or one child elements. An IQ stanza of type "error" SHOULD include the child element contained in the associated "get" or "set" and MUST include an <error/> child; for details, see Stanza Errors (Section 8.7).

## 8.6 Extended Namespaces

While the three XML stanza types defined in the "jabber:client" or "jabber:server" namespace (along with their attributes and child elements) provide a basic level of functionality for messaging and presence, XMPP uses XML namespaces to extend the stanzas for the

purpose of providing additional functionality. Thus a message, presence, or IQ stanza MAY house one or more optional child elements containing content that extends the meaning of the message (e.g., an XHTML-formatted version of the message body). This child element MAY have any name and MUST possess an 'xmlns' namespace declaration (other than "jabber:client", "jabber:server", or "http://etherx.jabber.org/streams") that defines all data contained within the child element.

Support for any given extended namespace is OPTIONAL on the part of any implementation. If an entity does not understand such a namespace, the entity's expected behavior depends on whether the entity is (1) the recipient or (2) an entity that is routing the stanza to the recipient:

Recipient: If a recipient receives a stanza that contains a child element it does not understand, it SHOULD ignore that specific XML data, i.e., it SHOULD not process it or present it to a user or associated application (if any). In particular:

* If an entity receives a message or presence stanza that contains XML data qualified by a namespace it does not understand, the portion of the stanza that is in the unknown namespace SHOULD be ignored.

* If an entity receives a message stanza containing only a child element qualified by a namespace it does not understand, it MUST ignore the entire stanza.

* If an entity receives an IQ stanza of type "get" or "set" containing a child element qualified by a namespace it does not understand, the entity SHOULD return an IQ stanza of type "error" with an error condition of <feature-not-implemented/>.

Router: If a routing entity (usually a server) handles a stanza that contains a child element it does not understand, it SHOULD ignore the associated XML data by passing it on untouched to the recipient.

### 8.7 Stanza Errors

Stanza-related errors are handled in a manner similar to stream errors (Section 4.6), except that hints are also provided to the receiving application regarding actions to take in reponse to the error.

### 8.7.1 Rules

The following rules apply to stanza-related errors:

- A stanza whose 'type' attribute has a value of "error" MUST contain an <error/> child element.

- The receiving or processing entity that returns an error to the sending entity SHOULD include the original XML sent so that the sender can inspect and if necessary correct the XML before re-sending.

- An entity that receives a stanza whose 'type' attribute has a value of "error" MUST NOT respond to the stanza with a further stanza of type "error"; this helps to prevent looping.

- An <error/> child MUST NOT be included if the 'type' attribute has a value other than "error" (or if there is no 'type' attribute).

### 8.7.2 Syntax

The syntax for stanza-related errors is as follows:

```
<stanza-name to='sender' type='error'>
  [RECOMMENDED to include sender XML here]
  <error type='error-type'>
    <defined-condition xmlns='urn:ietf:params:xml:ns:xmpp-stanzas'/>
    <text xmlns='urn:ietf:params:xml:ns:xmpp-stanzas'>
      OPTIONAL descriptive text
    </text>
    [OPTIONAL application-specific condition element]
  </error>
</stanza-name>
```

The stanza-name is one of message, presence, or iq.

The value of the <error/> element's 'type' attribute MUST be one of the following:

- cancel -- do not retry (the error is unrecoverable)

- continue -- proceed (the condition was only a warning)

- modify -- retry after changing the data sent

- auth -- retry after providing credentials

- wait -- retry after waiting (the error is temporary)

The <error/> element:

- MUST contain a child element corresponding to one of the defined stanza error conditions defined below; this element MUST be qualified by the 'urn:ietf:params:xml:ns:xmpp-stanzas' namespace

- MAY contain a <text/> child containing CDATA that describes the error in more detail; this element MUST be qualified by the 'urn:ietf:params:xml:ns:xmpp-stanzas' namespace and SHOULD possess an 'xml:lang' attribute

- MAY contain a child element for an application-specific error condition; this element MUST be qualified by an application-defined namespace, and its structure is defined by that namespace

The <text/> element is OPTIONAL. If included, it SHOULD be used only to provide descriptive or diagnostic information that supplements the meaning of a defined condition or application-specific condition. It SHOULD NOT be interpreted programmatically by an application. It SHOULD NOT be used as the error message presented to user, but MAY be shown in addition to the error message associated with the included condition element (or elements).

Note: the XML namespace name 'urn:ietf:params:xml:ns:xmpp-stanzas' that qualifies the descriptive element adheres to the format defined in The IETF XML Registry [25].

### 8.7.3 Defined Conditions

The following stanza-related error conditions are defined for use in stanza errors.

- <bad-request/> -- the sender has sent XML that is malformed or that cannot be processed (e.g., a client-generated stanza includes a 'from' address, or an IQ stanza includes an unrecognized value of the 'type' attribute); the associated error type SHOULD be "modify".

- <conflict/> -- access cannot be granted because an existing resource or session exists with the same name or address; the associated error type SHOULD be "cancel".

- <feature-not-implemented/> -- the feature requested is not implemented by the recipient or server and therefore cannot be processed; the associated error type SHOULD be "cancel".

- <forbidden/> -- the requesting entity does not possess the required permissions to perform the action; the associated error type SHOULD be "auth".

- <internal-server-error/> -- the server could not process the stanza because of a misconfiguration or an otherwise-undefined internal server error; the associated error type SHOULD be "wait".

- <item-not-found/> -- the addressed JID or item requested cannot be found; the associated error type SHOULD be "cancel".

- <jid-malformed/> -- the value of the 'to' attribute in the sender's stanza does not adhere to the syntax defined in Addressing Scheme (Section 3); the associated error type SHOULD be "modify".

- <not-allowed/> -- the recipient does not allow any entity to perform the action; the associated error type SHOULD be "cancel".

- <recipient-unavailable/> -- the specific recipient requested is currently unavailable; the associated error type SHOULD be "wait".

- <registration-required/> -- the user is not authorized to access the requested service because registration is required; the associated error type SHOULD be "auth".

- <remote-server-not-found/> -- a remote server or service specified as part or all of the JID of the intended recipient does not exist; the associated error type SHOULD be "cancel".

- <remote-server-timeout/> -- a remote server or service specified as part or all of the JID of the intended recipient could not be contacted within a reasonable amount of time; the associated error type SHOULD be "wait".

- <resource-constraint/> -- the server is resource-contrained and is unable to service the request; the associated error type SHOULD be "wait".

- <service-unavailable/> -- the service requested is currently unavailable on the server; the associated error type SHOULD be "cancel".

- <subscription-required/> -- the user is not authorized to access the requested service because a subscription is required; the associated error type SHOULD be "auth".

- <undefined-condition/> -- the error condition is not one of those

defined by the other conditions in this list; any error type may be associated with this condition, and it SHOULD be used only in conjuction with an application-specific condition.

- <unexpected-request/> -- the recipient understood the request but was not expecting it at this time (e.g., the request was out of order); the associated error type SHOULD be "wait".

### 8.7.4 Application-Specific Conditions

As noted, an application MAY provide application-specific stanza error information by including a properly-namespaced child in the error element. The application-specific element SHOULD supplement or further qualify a defined element. Thus the <error/> element will contain two or three child elements:

```
<iq type='error' id='some-id'>
  <error type='modify'>
    <bad-request xmlns='urn:ietf:params:xml:ns:xmpp-stanzas'/>
    <too-many-parameters xmlns='application-ns'/>
  </error>
</iq>


<message type='error' id='another-id'>
  <error type='modify'>
    <undefined-condition xmlns='urn:ietf:params:xml:ns:xmpp-stanzas'/>
    <text xml:lang='en' xmlns='urn:ietf:params:xml:ns:xmpp-stanzas'>
      Some special application diagnostic information!
    </text>
    <special-application-condition xmlns='application-ns'/>
  </error>
</message>
```

# 9. XML Usage within XMPP

## 9.1 Restrictions

XMPP is a simplified and specialized protocol for streaming XML elements in order to exchange messages and presence information in close to real time. Because XMPP does not require the parsing of arbitrary and complete XML documents, there is no requirement that XMPP needs to support the full XML specification [1]. In particular, the following restrictions apply.

With regard to XML generation, an XMPP implementation MUST NOT inject into an XML stream any of the following:

- comments (as defined in Section 2.5 of the XML specification [1])
- processing instructions (Section 2.6)
- internal or external DTD subsets (Section 2.8)
- internal or external entity references (Section 4.2) with the exception of predefined entities (Section 4.6)
- character data or attribute values containing unescaped characters that map to the predefined entities (Section 4.6); such characters MUST be escaped

With regard to XML processing, if an XMPP implementation receives such restricted XML data, it MUST ignore the data.

## 9.2 XML Namespace Names and Prefixes

XML Namespaces [12] are used within all XMPP-compliant XML to create strict boundaries of data ownership. The basic function of namespaces is to separate different vocabularies of XML elements that are structurally mixed together. Ensuring that XMPP-compliant XML is namespace-aware enables any XML to be structurally mixed with any data element within XMPP. Rules for XML namespace names and prefixes are defined below.

### 9.2.1 Stream Namespace

A stream namespace declaration is REQUIRED in both XML stream headers. The name of the stream namespace MUST be 'http://etherx.jabber.org/streams'. The element names of the <stream/> element and its <features/> and <error/> children MUST be qualified by the stream namespace prefix in all instances. An implementation SHOULD generate only the 'stream:' prefix for these elements, and for

historical reasons MAY accept only the 'stream:' prefix.

### 9.2.2 Default Namespace

A default namespace declaration is REQUIRED and is used in both XML streams in order to define the allowable first-level children of the root stream element. This namespace declaration MUST be the same for the initiating stream and the responding stream so that both streams are qualified consistently. The default namespace declaration applies to the stream and all stanzas sent within a stream (unless explicitly qualified by another namespace, or by the prefix of the stream namespace or the dialback namespace).

A server implementation MUST support the following two default namespaces (for historical reasons, some implementations MAY support only these two default namespaces):

- jabber:client -- this default namespace is declared when the stream is used for communications between a client and a server

- jabber:server -- this default namespace is declared when the stream is used for communications between two servers

A client implementation MUST support the 'jabber:client' default namespace, and for historical reasons MAY support only that default namespace.

An implementation MUST NOT generate namespace prefixes for elements in the default namespace if the default namespace is 'jabber:client' or 'jabber:server'. An implementation SHOULD NOT generate namespace prefixes for elements qualified by "extended" namespaces as described under Extended Namespaces (Section 8.6).

Note: the 'jabber:client' and 'jabber:server' namespaces are nearly identical but are used in different contexts (client-to-server communications for 'jabber:client' and server-to-server communications for 'jabber:server'). The only difference between the two is that the 'to' and 'from' attributes are OPTIONAL on stanzas sent within 'jabber:client', whereas they are REQUIRED on stanzas sent within 'jabber:server'. If a compliant implementation accepts a stream that is qualified by the 'jabber:client' or 'jabber:server' namespace, it MUST support all three core stanza types (message, presence, and IQ) as described herein and defined in the schema.

### 9.2.3 Dialback Namespace

A dialback namespace declaration is REQUIRED for all elements used in server dialback. The name of the dialback namespace MUST be

'jabber:server:dialback'. All elements qualified by this namespace MUST be prefixed. An implementation SHOULD generate only the 'db:' prefix for such elements and MAY accept only the 'db:' prefix.

### 9.3 Validation

Except as noted with regard to 'to' and 'from' addresses for stanzas within the 'jabber:server' namespace, a server is not responsible for validating the XML elements forwarded to a client or another server; an implementation MAY choose to provide only validated data elements but is NOT REQUIRED to do so (although an implementation MUST NOT accept XML that is not well-formed). Clients SHOULD NOT rely on the ability to send data which does not conform to the schemas, and SHOULD ignore any non-conformant elements or attributes on the incoming XML stream. Validation of XML streams and stanzas is NOT REQUIRED or recommended, and schemas are included herein for descriptive purposes only.

### 9.4 Character Encodings

Software implementing XML streams MUST support the UTF-8 (RFC 2279 [19]) and UTF-16 (RFC 2781 [20]) transformations of Universal Character Set (ISO/IEC 10646-1 [21]) characters. Implementations MUST NOT attempt to use any other encoding for transmitted data. The encodings of the transmitted and received streams are independent. Implementations MAY select either UTF-8 or UTF-16 for the transmitted stream, and SHOULD deduce the encoding of the received stream as described in the XML specification [1]. For historical reasons, existing implementations MAY support UTF-8 only.

### 9.5 Inclusion of Text Declaration

An application MAY send a text declaration. Applications MUST follow the rules in the XML specification [1] regarding the circumstances under which a text declaration is included.

## 10. IANA Considerations

### 10.1 XML Namespace Name for TLS Data

A URN sub-namespace for TLS-related data in the Extensible Messaging and Presence Protocol (XMPP) is defined as follows.

URI: urn:ietf:params:xml:ns:xmpp-tls

Specification: [RFCXXXX]

Description: This is the XML namespace name for TLS-related data in the Extensible Messaging and Presence Protocol (XMPP) as defined by [RFCXXXX].

Registrant Contact: IETF, XMPP Working Group, <xmppwg@jabber.org>

### 10.2 XML Namespace Name for SASL Data

A URN sub-namespace for SASL-related data in the Extensible Messaging and Presence Protocol (XMPP) is defined as follows.

URI: urn:ietf:params:xml:ns:xmpp-sasl

Specification: [RFCXXXX]

Description: This is the XML namespace name for SASL-related data in the Extensible Messaging and Presence Protocol (XMPP) as defined by [RFCXXXX].

Registrant Contact: IETF, XMPP Working Group, <xmppwg@jabber.org>

### 10.3 XML Namespace Name for Stream Errors

A URN sub-namespace for stream-related error data in the Extensible Messaging and Presence Protocol (XMPP) is defined as follows.

URI: urn:ietf:params:xml:ns:xmpp-streams

Specification: [RFCXXXX]

Description: This is the XML namespace name for stream-related error data in the Extensible Messaging and Presence Protocol (XMPP) as defined by [RFCXXXX].

Registrant Contact: IETF, XMPP Working Group, <xmppwg@jabber.org>

### 10.4 XML Namespace Name for Stanza Errors

A URN sub-namespace for stanza-related error data in the Extensible Messaging and Presence Protocol (XMPP) is defined as follows.

URI: urn:ietf:params:xml:ns:xmpp-stanzas

Specification: [RFCXXXX]

Description: This is the XML namespace name for stanza-related error data in the Extensible Messaging and Presence Protocol (XMPP) as defined by [RFCXXXX].

Registrant Contact: IETF, XMPP Working Group, <xmppwg@jabber.org>

### 10.5 Existing Registrations

The IANA registers "xmpp" as a GSSAPI [22] service name, as specified in SASL Definition (Section 6.4).

Additionally, the IANA registers "jabber-client" and "jabber-server" as keywords for TCP ports 5222 and 5269 respectively. These ports SHOULD be used for client-to-server and server-to-server communications respectively, but their use is NOT REQUIRED. The use of the string "jabber" in these keywords is historical.

## 11. Internationalization Considerations

Each XML stanza SHOULD include an 'xml:lang' attribute. Servers MUST NOT modify or delete 'xml:lang' attributes from stanzas they receive from other entities.

## 12. Security Considerations

### 12.1 High Security

For the purposes of XMPP communications (client-to-server and server-to-server), the term "high security" refers to the use of security technologies that provide both mutual authentication and integrity-checking; in particular, when using certificate-based authentication to provide high security, a chain-of-trust SHOULD be established out-of-band, although a shared certificate authority signing certificates could allow a previously unknown certificate to establish trust in-band.

Standalone, self-signed service certificates SHOULD NOT be used; rather, an entity that wishes to generate a self-signed service certificate SHOULD first generate a self-signed Root CA certificate and then generate a signed service certificate. Entities that communicate with the service SHOULD be configured with the Root CA certificate rather than the service certificate; this avoids problems associated with simple comparison of service certificates. If a self-signed service certificate is used, an entity SHOULD NOT trust it if it is changed to another self-signed certificate or a certificate signed by an unrecognized authority.

Implementations MUST support high security. Service provisioning SHOULD use high security, subject to local security policies.

### 12.2 Client-to-Server Communications

A compliant implementation MUST support both TLS and SASL for connections to a server.

The TLS protocol for encrypting XML streams (defined under Stream Encryption (Section 5)) provides a reliable mechanism for helping to ensure the confidentiality and data integrity of data exchanged between two entities.

The SASL protocol for authenticating XML streams (defined under Stream Authentication (Section 6)) provides a reliable mechanism for validating that a client connecting to a server is who it claims to be.

The IP address and method of access of clients MUST NOT be made available by a server, nor are any connections other than the original server connection required. This helps to protect the client's server from direct attack or identification by third parties.

### 12.3 Server-to-Server Communications

A compliant implementation MUST support both TLS and SASL for inter-domain communications. For historical reasons, a compliant implementation SHOULD also support Server Dialback (Section 7).

Because service provisioning is a matter of policy, it is OPTIONAL for any given domain to communicate with other domains, and server-to-server communications MAY be disabled by the administrator of any given deployment. If a particular domain enables inter-domain communications, it SHOULD enable high security.

Administrators may want to require use of SASL for server-to-server communications in order to ensure both authentication and confidentiality (e.g., on an organization's private network). Compliant implementations SHOULD support SASL for this purpose.

Inter-domain connections MUST NOT proceed until the DNS hostnames asserted by the servers have been resolved. Such resolutions MUST first attempt to resolve the hostname using an SRV [18] record of _jabber._tcp.server (the use of the string "jabber" for SRV purposes is historical). If the SRV lookup fails, the fallback is a normal A lookup to determine the IP address, using the jabber-server port of 5269 assigned by the Internet Assigned Numbers Authority [5].

Server dialback helps protect against domain spoofing, thus making it more difficult to spoof XML stanzas. It is not a mechanism for authenticating, securing, or encrypting streams between servers as is done via SASL and TLS. Furthermore, it is susceptible to DNS poisoning attacks unless DNSSec [30] is used, and even if the DNS information is accurate, dialback cannot protect from attacks where the attacker is capable of hijacking the IP address of the remote domain. Domains requiring robust security SHOULD use TLS and SASL. If SASL is used for server-to-server authentication, dialback SHOULD NOT be used since it is unnecessary.

### 12.4 Order of Layers

The order of layers in which protocols MUST be stacked is as follows:

1. TCP
2. TLS
3. SASL
4. XMPP

The rationale for this order is that TCP is the base connection layer used by all of the protocols stacked on top of TCP, TLS is often provided at the operating system layer, SASL is often provided at the application layer, and XMPP is the application itself.

### 12.5 Firewalls

Communications using XMPP normally occur over TCP sockets on port 5222 (client-to-server) or port 5269 (server-to-server), as registered with the IANA [5] (see IANA Considerations (Section 10)). Use of these well-known ports allows administrators to easily enable or disable XMPP activity through existing and commonly-deployed firewalls.

### 12.6 Mandatory to Implement Technologies

At a minimum, all implementations MUST support the following mechanisms:

for authentication: the SASL DIGEST-MD5 mechanism

for confidentiality: TLS (using the TLS_RSA_WITH_3DES_EDE_CBC_SHA cipher)

for both: TLS plus SASL EXTERNAL(using the TLS_RSA_WITH_3DES_EDE_CBC_SHA cipher supporting client-side certificates)

Normative References

[1] World Wide Web Consortium, "Extensible Markup Language (XML) 1.0 (Second Edition)", W3C xml, October 2000, <http://www.w3.org/TR/2000/REC-xml-20001006>.

[2] Day, M., Aggarwal, S. and J. Vincent, "Instant Messaging / Presence Protocol Requirements", RFC 2779, February 2000.

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

[4] University of Southern California, "Transmission Control Protocol", RFC 793, September 1981, <http://www.ietf.org/rfc/rfc0793.txt>.

[5] Internet Assigned Numbers Authority, "Internet Assigned Numbers Authority", January 1998, <http://www.iana.org/>.

[6] Harrenstien, K., Stahl, M. and E. Feinler, "DoD Internet host table specification", RFC 952, October 1985.

[7] Braden, R., "Requirements for Internet Hosts - Application and Support", STD 3, RFC 1123, October 1989.

[8] Hoffman, P. and M. Blanchet, "Nameprep: A Stringprep Profile for Internationalized Domain Names (draft-ietf-idn-nameprep-11, work in progress)", June 2002.

[9] Hoffman, P. and M. Blanchet, "Preparation of Internationalized Strings ("stringprep")", RFC 3454, December 2002.

[10] Saint-Andre, P. and J. Hildebrand, "Nodeprep: A Stringprep Profile for Node Identifiers in XMPP", draft-ietf-xmpp-nodeprep-03 (work in progress), June 2003.

[11] Saint-Andre, P. and J. Hildebrand, "Resourceprep: A Stringprep Profile for Resource Identifiers in XMPP", draft-ietf-xmpp-resourceprep-03 (work in progress), June 2003.

[12] World Wide Web Consortium, "Namespaces in XML", W3C xml-names, January 1999, <http://www.w3.org/TR/1999/REC-xml-names-19990114/>.

[13] Dierks, T., Allen, C., Treese, W., Karlton, P., Freier, A. and P. Kocher, "The TLS Protocol Version 1.0", RFC 2246, January 1999.

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

[15] Myers, J., "Simple Authentication and Security Layer (SASL)", RFC 2222, October 1997.

[16] Leach, P. and C. Newman, "Using Digest Authentication as a SASL Mechanism", RFC 2831, May 2000.

[17] Alvestrand, H., "Tags for the Identification of Languages", BCP 47, RFC 3066, January 2001.

[18] Gulbrandsen, A. and P. Vixie, "A DNS RR for specifying the location of services (DNS SRV)", RFC 2052, October 1996.

[19] Yergeau, F., "UTF-8, a transformation format of ISO 10646", RFC 2279, January 1998.

[20] Hoffman, P. and F. Yergeau, "UTF-16, an encoding of ISO 10646", RFC 2781, February 2000.

[21] International Organization for Standardization, "Information Technology - Universal Multiple-octet coded Character Set (UCS) - Amendment 2: UCS Transformation Format 8 (UTF-8)", ISO Standard 10646-1 Addendum 2, October 1996.

[22] Linn, J., "Generic Security Service Application Program Interface, Version 2", RFC 2078, January 1997.

## Informative References

[23] Saint-Andre, P. and J. Miller, "XMPP Instant Messaging", draft-ietf-xmpp-im-12 (work in progress), June 2003.

[24] Berners-Lee, T., Fielding, R. and L. Masinter, "Uniform Resource Identifiers (URI): Generic Syntax", RFC 2396, August 1998, <http://www.ietf.org/rfc/rfc2396.txt>.

[25] Mealling, M., "The IANA XML Registry", draft-mealling-iana-xmlns-registry-04 (work in progress), June 2002.

[26] Crispin, M., "Internet Message Access Protocol - Version 4rev1", RFC 2060, December 1996.

[27] Myers, J. and M. Rose, "Post Office Protocol - Version 3", STD 53, RFC 1939, May 1996.

[28] Newman, C. and J. Myers, "ACAP -- Application Configuration Access Protocol", RFC 2244, November 1997.

[29] Newman, C., "Using TLS with IMAP, POP3 and ACAP", RFC 2595, June 1999.

[30] Eastlake, D., "Domain Name System Security Extensions", RFC 2535, March 1999.

[31] Alvestrand, H., "IETF Policy on Character Sets and Languages", BCP 18, RFC 2277, January 1998.

[32] Fielding, R., Gettys, J., Mogul, J., Nielsen, H., Masinter, L., Leach, P. and T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1", RFC 2616, June 1999.

## Authors' Addresses

Peter Saint-Andre
Jabber Software Foundation

EMail: stpeter@jabber.org

Jeremie Miller
Jabber Software Foundation

EMail: jeremie@jabber.org

## Appendix A. XML Schemas

The following XML schemas are descriptive, not normative.

### A.1 Stream namespace

```
<?xml version='1.0' encoding='UTF-8'?>

<xs:schema
    xmlns:xs='http://www.w3.org/2001/XMLSchema'
    targetNamespace='http://etherx.jabber.org/streams'
    xmlns='http://etherx.jabber.org/streams'
    elementFormDefault='unqualified'>

  <xs:element name='stream'>
    <xs:complexType>
      <xs:sequence>
        <xs:element ref='features' minOccurs='0' maxOccurs='1'/>
        <xs:choice minOccurs='0' maxOccurs='1'>
          <xs:any namespace='jabber:client'
                  minOccurs='0'
                  maxOccurs='unbounded'/>
          <xs:any namespace='jabber:server'
                  minOccurs='0'
                  maxOccurs='unbounded'/>
        </xs:choice>
        <xs:element ref='error' minOccurs='0' maxOccurs='1'/>
      </xs:sequence>
      <xs:attribute name='to' type='xs:string' use='optional'/>
      <xs:attribute name='from' type='xs:string' use='optional'/>
      <xs:attribute name='id' type='xs:NMTOKEN' use='optional'/>
      <xs:attribute name='version' type='xs:decimal' use='optional'/>
    </xs:complexType>
  </xs:element>

  <xs:element name='features'>
    <xs:complexType>
      <xs:sequence>
        <xs:any
            namespace='##other'
            minOccurs='0'
            maxOccurs='unbounded'/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>

  <xs:element name='error'>
    <xs:complexType>
```

```
        <xs:sequence>
          <xs:any namespace='urn:ietf:params:xml:ns:xmpp-streams'
                  maxOccurs='1'/>
          <xs:any
              namespace='##other'
              minOccurs='0'
              maxOccurs='1'/>
        </xs:sequence>
      </xs:complexType>
    </xs:element>

  </xs:schema>
```

### A.2 Stream error namespace

```
  <?xml version='1.0' encoding='UTF-8'?>

  <xs:schema
      xmlns:xs='http://www.w3.org/2001/XMLSchema'
      xmlns:xml='http://www.w3.org/XML/1998/namespace'
      targetNamespace='urn:ietf:params:xml:ns:xmpp-streams'
      xmlns='urn:ietf:params:xml:ns:xmpp-streams'
      elementFormDefault='qualified'>

    <xs:import namespace='http://www.w3.org/XML/1998/namespace'
               schemaLocation='http://www.w3.org/2001/xml.xsd'/>

    <xs:element name='host-gone' type='empty'/>
    <xs:element name='host-unknown' type='empty'/>
    <xs:element name='improper-addressing' type='empty'/>
    <xs:element name='internal-server-error' type='empty'/>
    <xs:element name='invalid-id' type='empty'/>
    <xs:element name='invalid-namespace' type='empty'/>
    <xs:element name='nonmatching-hosts' type='empty'/>
    <xs:element name='not-authorized' type='empty'/>
    <xs:element name='remote-connection-failed' type='empty'/>
    <xs:element name='resource-constraint' type='empty'/>
    <xs:element name='see-other-host' type='xs:string'/>
    <xs:element name='system-shutdown' type='empty'/>
    <xs:element name='unsupported-stanza-type' type='empty'/>
    <xs:element name='unsupported-version' type='xs:string'/>
    <xs:element name='xml-not-well-formed' type='empty'/>

    <xs:element name='text' type='xs:string'>
      <xs:complexType>
        <xs:attribute ref='xml:lang' use='optional'/>
      </xs:complexType>
```

```
    </xs:element>

    <xs:simpleType name='empty'>
      <xs:restriction base='xs:string'>
        <xs:enumeration value=''/>
      </xs:restriction>
    </xs:simpleType>

  </xs:schema>
```

### A.3 TLS namespace

```
  <?xml version='1.0' encoding='UTF-8'?>

  <xs:schema
      xmlns:xs='http://www.w3.org/2001/XMLSchema'
      targetNamespace='urn:ietf:params:xml:ns:xmpp-tls'
      xmlns='urn:ietf:params:xml:ns:xmpp-tls'
      elementFormDefault='qualified'>

    <xs:element name='starttls'>
      <xs:complexType>
        <xs:sequence>
          <xs:element
              ref='required'
              minOccurs='0'
              maxOccurs='1'/>
        </xs:sequence>
      </xs:complexType>
    </xs:element>

    <xs:element name='required' type='empty'/>
    <xs:element name='proceed' type='empty'/>
    <xs:element name='failure' type='empty'/>

    <xs:simpleType name='empty'>
      <xs:restriction base='xs:string'>
        <xs:enumeration value=''/>
      </xs:restriction>
    </xs:simpleType>

  </xs:schema>
```

### A.4 SASL namespace

```
  <?xml version='1.0' encoding='UTF-8'?>
```

```
   <xs:schema
       xmlns:xs='http://www.w3.org/2001/XMLSchema'
       targetNamespace='urn:ietf:params:xml:ns:xmpp-sasl'
       xmlns='urn:ietf:params:xml:ns:xmpp-sasl'
       elementFormDefault='qualified'>

     <xs:element name='mechanisms'>
       <xs:complexType>
         <xs:sequence>
           <xs:element ref='mechanism' maxOccurs='unbounded'/>
         </xs:sequence>
       </xs:complexType>
     </xs:element>

     <xs:element name='mechanism' type='xs:string'/>

     <xs:element name='auth'>
       <xs:complexType>
         <xs:attribute name='mechanism'
                       type='xs:NMTOKEN'
                       use='optional'/>
       </xs:complexType>
     </xs:element>

     <xs:element name='challenge' type='xs:NMTOKEN'/>
     <xs:element name='response' type='xs:NMTOKEN'/>
     <xs:element name='abort' type='empty'/>
     <xs:element name='success' type='empty'/>

     <xs:element name='failure'>
       <xs:complexType>
         <xs:choice maxOccurs='1'>
           <xs:element ref='bad-protocol'/>
           <xs:element ref='encryption-required'/>
           <xs:element ref='invalid-authzid'/>
           <xs:element ref='invalid-mechanism'/>
           <xs:element ref='invalid-realm'/>
           <xs:element ref='mechanism-too-weak'/>
           <xs:element ref='not-authorized'/>
           <xs:element ref='temporary-auth-failure'/>
         </xs:choice>
       </xs:complexType>
     </xs:element>

     <xs:element name='bad-protocol' type='empty'/>
     <xs:element name='encryption-required' type='empty'/>
     <xs:element name='invalid-authzid' type='empty'/>
     <xs:element name='invalid-mechanism' type='empty'/>
```

```
    <xs:element name='invalid-realm' type='empty'/>
    <xs:element name='mechanism-too-weak' type='empty'/>
    <xs:element name='not-authorized' type='empty'/>
    <xs:element name='temporary-auth-failure' type='empty'/>

    <xs:simpleType name='empty'>
      <xs:restriction base='xs:string'>
        <xs:enumeration value=''/>
      </xs:restriction>
    </xs:simpleType>

  </xs:schema>
```

### A.5 Dialback namespace

```
  <?xml version='1.0' encoding='UTF-8'?>

  <xs:schema
      xmlns:xs='http://www.w3.org/2001/XMLSchema'
      targetNamespace='jabber:server:dialback'
      xmlns='jabber:server:dialback'
      elementFormDefault='qualified'>

    <xs:element name='result'>
      <xs:complexType>
        <xs:simpleContent>
          <xs:extension base='xs:NMTOKEN'>
            <xs:attribute name='from' type='xs:string' use='required'/>
            <xs:attribute name='to' type='xs:string' use='required'/>
            <xs:attribute name='type' use='optional'>
              <xs:simpleType>
                <xs:restriction base='xs:NCName'>
                  <xs:enumeration value='invalid'/>
                  <xs:enumeration value='valid'/>
                </xs:restriction>
              </xs:simpleType>
            </xs:attribute>
          </xs:extension>
        </xs:simpleContent>
      </xs:complexType>
    </xs:element>

    <xs:element name='verify'>
      <xs:complexType>
        <xs:simpleContent>
          <xs:extension base='xs:NMTOKEN'>
            <xs:attribute name='from' type='xs:string' use='required'/>
```

```
            <xs:attribute name='to' type='xs:string' use='required'/>
            <xs:attribute name='id' type='xs:NMTOKEN' use='required'/>
            <xs:attribute name='type' use='optional'>
              <xs:simpleType>
                <xs:restriction base='xs:NCName'>
                  <xs:enumeration value='invalid'/>
                  <xs:enumeration value='valid'/>
                </xs:restriction>
              </xs:simpleType>
            </xs:attribute>
          </xs:extension>
        </xs:simpleContent>
      </xs:complexType>
    </xs:element>

  </xs:schema>
```

### A.6 Client namespace

```
  <?xml version='1.0' encoding='UTF-8'?>

  <xs:schema
      xmlns:xs='http://www.w3.org/2001/XMLSchema'
      xmlns:xml='http://www.w3.org/XML/1998/namespace'
      targetNamespace='jabber:client'
      xmlns='jabber:client'
      elementFormDefault='qualified'>

    <xs:import namespace='http://www.w3.org/XML/1998/namespace'
               schemaLocation='http://www.w3.org/2001/xml.xsd'/>

    <xs:element name='message'>
       <xs:complexType>
          <xs:sequence>
             <xs:element ref='subject'
                         minOccurs='0'
                         maxOccurs='unbounded'/>
             <xs:element ref='body'
                         minOccurs='0'
                         maxOccurs='unbounded'/>
             <xs:element ref='thread'
                         minOccurs='0'
                         maxOccurs='1'/>
             <xs:any     namespace='##other'
                         minOccurs='0'
                         maxOccurs='unbounded'/>
             <xs:element ref='error'
```

```
                        minOccurs='0'
                        maxOccurs='1'/>
          </xs:sequence>
          <xs:attribute name='to'
                        type='xs:string'
                        use='optional'/>
          <xs:attribute name='from'
                        type='xs:string'
                        use='optional'/>
          <xs:attribute name='id'
                        type='xs:NMTOKEN'
                        use='optional'/>
          <xs:attribute ref='xml:lang' use='optional'/>
          <xs:attribute name='type' use='optional'>
            <xs:simpleType>
              <xs:restriction base='xs:NCName'>
                <xs:enumeration value='chat'/>
                <xs:enumeration value='error'/>
                <xs:enumeration value='groupchat'/>
                <xs:enumeration value='headline'/>
                <xs:enumeration value='normal'/>
              </xs:restriction>
            </xs:simpleType>
          </xs:attribute>
       </xs:complexType>
    </xs:element>

    <xs:element name='body' type='xs:string'>
      <xs:complexType>
        <xs:attribute ref='xml:lang' use='optional'/>
      </xs:complexType>
    </xs:element>

    <xs:element name='subject' type='xs:string'>
      <xs:complexType>
        <xs:attribute ref='xml:lang' use='optional'/>
      </xs:complexType>
    </xs:element>

    <xs:element name='thread' type='xs:NMTOKEN'/>

    <xs:element name='presence'>
      <xs:complexType>
        <xs:sequence>
          <xs:element ref='show'
                      minOccurs='0'
                      maxOccurs='1'/>
          <xs:element ref='status'
```

```
                    minOccurs='0'
                    maxOccurs='unbounded'/>
        <xs:element ref='priority'
                    minOccurs='0'
                    maxOccurs='1'/>
        <xs:any     namespace='##other'
                    minOccurs='0'
                    maxOccurs='unbounded'/>
        <xs:element ref='error'
                    minOccurs='0'
                    maxOccurs='1'/>
      </xs:sequence>
      <xs:attribute name='to'
                    type='xs:string'
                    use='optional'/>
      <xs:attribute name='from'
                    type='xs:string'
                    use='optional'/>
      <xs:attribute name='id'
                    type='xs:NMTOKEN'
                    use='optional'/>
      <xs:attribute ref='xml:lang' use='optional'/>
      <xs:attribute name='type' use='optional'>
        <xs:simpleType>
          <xs:restriction base='xs:NCName'>
            <xs:enumeration value='subscribe'/>
            <xs:enumeration value='subscribed'/>
            <xs:enumeration value='unsubscribe'/>
            <xs:enumeration value='unsubscribed'/>
            <xs:enumeration value='unavailable'/>
            <xs:enumeration value='error'/>
          </xs:restriction>
        </xs:simpleType>
      </xs:attribute>
    </xs:complexType>
  </xs:element>

  <xs:element name='show'>
    <xs:simpleType>
      <xs:restriction base='xs:NCName'>
        <xs:enumeration value='away'/>
        <xs:enumeration value='chat'/>
        <xs:enumeration value='dnd'/>
        <xs:enumeration value='xa'/>
      </xs:restriction>
    </xs:simpleType>
  </xs:element>
```

```
    <xs:element name='status' type='xs:string'>
      <xs:complexType>
        <xs:attribute ref='xml:lang' use='optional'/>
      </xs:complexType>
    </xs:element>

    <xs:element name='priority' type='xs:byte'/>

    <xs:element name='iq'>
      <xs:complexType>
        <xs:sequence>
          <xs:any     namespace='##other'
                      minOccurs='0'
                      maxOccurs='1'/>
          <xs:element ref='error'
                      minOccurs='0'
                      maxOccurs='1'/>
        </xs:sequence>
        <xs:attribute name='to'
                      type='xs:string'
                      use='optional'/>
        <xs:attribute name='from'
                      type='xs:string'
                      use='optional'/>
        <xs:attribute name='id'
                      type='xs:NMTOKEN'
                      use='optional'/>
        <xs:attribute ref='xml:lang' use='optional'/>
        <xs:attribute name='type' use='required'>
          <xs:simpleType>
            <xs:restriction base='xs:NCName'>
              <xs:enumeration value='get'/>
              <xs:enumeration value='set'/>
              <xs:enumeration value='result'/>
              <xs:enumeration value='error'/>
            </xs:restriction>
          </xs:simpleType>
        </xs:attribute>
      </xs:complexType>
    </xs:element>

    <xs:element name='error'>
      <xs:complexType>
        <xs:sequence>
          <xs:any namespace='urn:ietf:params:xml:ns:xmpp-stanzas'
                  maxOccurs='1'/>
          <text   namespace='urn:ietf:params:xml:ns:xmpp-stanzas'
                  minOccurs='0'
```

```
                maxOccurs='1'/>
          <xs:any
              namespace='##other'
              minOccurs='0'
              maxOccurs='1'/>
        </xs:sequence>
        <xs:attribute name='type' use='required'/>
          <xs:simpleType>
            <xs:restriction base='xs:NCName'>
              <xs:enumeration value='cancel'/>
              <xs:enumeration value='continue'/>
              <xs:enumeration value='modify'/>
              <xs:enumeration value='auth'/>
              <xs:enumeration value='wait'/>
            </xs:restriction>
          </xs:simpleType>
        </xs:attribute>
      </xs:complexType>
    </xs:element>

  </xs:schema>
```

### A.7 Server namespace

```
  <?xml version='1.0' encoding='UTF-8'?>

  <xs:schema
      xmlns:xs='http://www.w3.org/2001/XMLSchema'
      xmlns:xml='http://www.w3.org/XML/1998/namespace'
      targetNamespace='jabber:server'
      xmlns='jabber:server'
      elementFormDefault='qualified'>

    <xs:import namespace='http://www.w3.org/XML/1998/namespace'
               schemaLocation='http://www.w3.org/2001/xml.xsd'/>

    <xs:element name='message'>
       <xs:complexType>
          <xs:sequence>
             <xs:element ref='subject'
                         minOccurs='0'
                         maxOccurs='unbounded'/>
             <xs:element ref='body'
                         minOccurs='0'
                         maxOccurs='unbounded'/>
             <xs:element ref='thread'
                         minOccurs='0'
```

```
                        maxOccurs='1'/>
            <xs:any     namespace='##other'
                        minOccurs='0'
                        maxOccurs='unbounded'/>
            <xs:element ref='error'
                        minOccurs='0'
                        maxOccurs='1'/>
          </xs:sequence>
          <xs:attribute name='to'
                        type='xs:string'
                        use='required'/>
          <xs:attribute name='from'
                        type='xs:string'
                        use='required'/>
          <xs:attribute name='id'
                        type='xs:NMTOKEN'
                        use='optional'/>
          <xs:attribute ref='xml:lang' use='optional'/>
          <xs:attribute name='type' use='optional'>
            <xs:simpleType>
              <xs:restriction base='xs:NCName'>
                <xs:enumeration value='chat'/>
                <xs:enumeration value='error'/>
                <xs:enumeration value='groupchat'/>
                <xs:enumeration value='headline'/>
                <xs:enumeration value='normal'/>
              </xs:restriction>
            </xs:simpleType>
          </xs:attribute>
       </xs:complexType>
    </xs:element>

    <xs:element name='body' type='xs:string'>
      <xs:complexType>
        <xs:attribute ref='xml:lang' use='optional'/>
      </xs:complexType>
    </xs:element>

    <xs:element name='subject' type='xs:string'>
      <xs:complexType>
        <xs:attribute ref='xml:lang' use='optional'/>
      </xs:complexType>
    </xs:element>

    <xs:element name='thread' type='xs:NMTOKEN'/>

    <xs:element name='presence'>
      <xs:complexType>
```

```
        <xs:sequence>
          <xs:element ref='show'
                      minOccurs='0'
                      maxOccurs='1'/>
          <xs:element ref='status'
                      minOccurs='0'
                      maxOccurs='unbounded'/>
          <xs:element ref='priority'
                      minOccurs='0'
                      maxOccurs='1'/>
          <xs:any     namespace='##other'
                      minOccurs='0'
                      maxOccurs='unbounded'/>
          <xs:element ref='error'
                      minOccurs='0'
                      maxOccurs='1'/>
        </xs:sequence>
        <xs:attribute name='to'
                      type='xs:string'
                      use='required'/>
        <xs:attribute name='from'
                      type='xs:string'
                      use='required'/>
        <xs:attribute name='id'
                      type='xs:NMTOKEN'
                      use='optional'/>
        <xs:attribute ref='xml:lang' use='optional'/>
        <xs:attribute name='type' use='optional'>
          <xs:simpleType>
            <xs:restriction base='xs:NCName'>
              <xs:enumeration value='subscribe'/>
              <xs:enumeration value='subscribed'/>
              <xs:enumeration value='unsubscribe'/>
              <xs:enumeration value='unsubscribed'/>
              <xs:enumeration value='unavailable'/>
              <xs:enumeration value='error'/>
            </xs:restriction>
          </xs:simpleType>
        </xs:attribute>
      </xs:complexType>
    </xs:element>

    <xs:element name='show'>
      <xs:simpleType>
        <xs:restriction base='xs:NCName'>
          <xs:enumeration value='away'/>
          <xs:enumeration value='chat'/>
          <xs:enumeration value='dnd'/>
```

```
          <xs:enumeration value='xa'/>
        </xs:restriction>
      </xs:simpleType>
    </xs:element>

    <xs:element name='status' type='xs:string'>
      <xs:complexType>
        <xs:attribute ref='xml:lang' use='optional'/>
      </xs:complexType>
    </xs:element>

    <xs:element name='priority' type='xs:byte'/>

    <xs:element name='iq'>
      <xs:complexType>
        <xs:sequence>
          <xs:any     namespace='##other'
                      minOccurs='0'
                      maxOccurs='1'/>
          <xs:element ref='error'
                      minOccurs='0'
                      maxOccurs='1'/>
        </xs:sequence>
        <xs:attribute name='to'
                      type='xs:string'
                      use='required'/>
        <xs:attribute name='from'
                      type='xs:string'
                      use='required'/>
        <xs:attribute name='id'
                      type='xs:NMTOKEN'
                      use='optional'/>
        <xs:attribute ref='xml:lang' use='optional'/>
        <xs:attribute name='type' use='required'>
          <xs:simpleType>
            <xs:restriction base='xs:NCName'>
              <xs:enumeration value='get'/>
              <xs:enumeration value='set'/>
              <xs:enumeration value='result'/>
              <xs:enumeration value='error'/>
            </xs:restriction>
          </xs:simpleType>
        </xs:attribute>
      </xs:complexType>
    </xs:element>

    <xs:element name='error'>
      <xs:complexType>
```

```
        <xs:sequence>
          <xs:any namespace='urn:ietf:params:xml:ns:xmpp-stanzas'
                  maxOccurs='1'/>
          <text   namespace='urn:ietf:params:xml:ns:xmpp-stanzas'
                  minOccurs='0'
                  maxOccurs='1'/>
          <xs:any
              namespace='##other'
              minOccurs='0'
              maxOccurs='1'/>
        </xs:sequence>
        <xs:attribute name='type' use='required'/>
          <xs:simpleType>
            <xs:restriction base='xs:NCName'>
              <xs:enumeration value='cancel'/>
              <xs:enumeration value='continue'/>
              <xs:enumeration value='modify'/>
              <xs:enumeration value='auth'/>
              <xs:enumeration value='wait'/>
            </xs:restriction>
          </xs:simpleType>
        </xs:attribute>
      </xs:complexType>
    </xs:element>

  </xs:schema>
```

### A.8 Stanza error namespace

```
  <?xml version='1.0' encoding='UTF-8'?>

  <xs:schema
      xmlns:xs='http://www.w3.org/2001/XMLSchema'
      xmlns:xml='http://www.w3.org/XML/1998/namespace'
      targetNamespace='urn:ietf:params:xml:ns:xmpp-stanzas'
      xmlns='urn:ietf:params:xml:ns:xmpp-stanzas'
      elementFormDefault='qualified'>

    <xs:import namespace='http://www.w3.org/XML/1998/namespace'
               schemaLocation='http://www.w3.org/2001/xml.xsd'/>

    <xs:element name='bad-request' type='empty'/>
    <xs:element name='conflict' type='empty'/>
    <xs:element name='feature-not-implemented' type='empty'/>
    <xs:element name='forbidden' type='empty'/>
    <xs:element name='internal-server-error' type='empty'/>
    <xs:element name='item-not-found' type='empty'/>
```

```
    <xs:element name='jid-malformed' type='empty'/>
    <xs:element name='not-allowed' type='empty'/>
    <xs:element name='recipient-unavailable' type='empty'/>
    <xs:element name='registration-required' type='empty'/>
    <xs:element name='remote-server-not-found' type='empty'/>
    <xs:element name='remote-server-timeout' type='empty'/>
    <xs:element name='resource-constraint' type='empty'/>
    <xs:element name='service-unavailable' type='empty'/>
    <xs:element name='subscription-required' type='empty'/>
    <xs:element name='undefined-condition' type='empty'/>
    <xs:element name='unexpected-request' type='empty'/>

    <xs:element name='text' type='xs:string'>
      <xs:complexType>
        <xs:attribute ref='xml:lang' use='optional'/>
      </xs:complexType>
    </xs:element>

    <xs:simpleType name='empty'>
      <xs:restriction base='xs:string'>
        <xs:enumeration value=''/>
      </xs:restriction>
    </xs:simpleType>

  </xs:schema>
```

## Appendix B. Revision History

Note to RFC Editor: please remove this entire appendix, and the corresponding entries in the table of contents, prior to publication.

### B.1 Changes from draft-ietf-xmpp-core-13

- Clarified stream restart after successful TLS and SASL negotiation.
- Clarified requirement for resolution of DNS hostnames.
- Clarified text regarding namespaces.
- Clarified examples regarding empty <stream:features/> element.
- Added several more SASL error conditions.
- Changed <invalid-xml/> stream error to <improper-addressing/> and added to schema.
- Made small editorial changes and fixed several schema errors.

### B.2 Changes from draft-ietf-xmpp-core-12

- Moved server dialback to a separate section; clarified its security characteristics and its role in the protocol.
- Adjusted error handling syntax and semantics per list discussion.
- Further clarified length of node identifiers and total length of JIDs.
- Documented message type='normal'.
- Corrected several small errors in the TLS and SASL sections.
- Corrected several errors in the schemas.

### B.3 Changes from draft-ietf-xmpp-core-11

- Corrected several small errors in the TLS and SASL sections.
- Made small editorial changes and fixed several schema errors.

### B.4 Changes from draft-ietf-xmpp-core-10

- Adjusted TLS content regarding certificate validation process.
- Specified that stanza error extensions for specific applications are to be properly namespaced children of the relevant descriptive element.
- Clarified rules for inclusion of the 'id' attribute.
- Specified that the 'xml:lang' attribute SHOULD be included (per list discussion).
- Made small editorial changes and fixed several schema errors.

### B.5 Changes from draft-ietf-xmpp-core-09

- Fixed several dialback error conditions.
- Cleaned up rules regarding TLS and certificate processing based on off-list feedback.
- Changed <stream-condition/> and <stanza-condition/> elements to <condition/>.
- Added or modified several stream and stanza error conditions.
- Specified only one child allowed for IQ, or two if type="error".
- Fixed several errors in the schemas.

### B.6 Changes from draft-ietf-xmpp-core-08

- Incorporated list discussion regarding addressing, SASL, TLS, TCP, dialback, namespaces, extensibility, and the meaning of 'ignore' for routers and recipients.
- Specified dialback error conditions.
- Made small editorial changes to address RFC Editor requirements.

### B.7 Changes from draft-ietf-xmpp-core-07

- Made several small editorial changes.

### B.8 Changes from draft-ietf-xmpp-core-06

- Added text regarding certificate validation in TLS negotiation per list discussion.
- Clarified nature of XML restrictions per discussion with W3C, and moved XML Restrictions subsection under "XML Usage within XMPP".
- Further clarified that XML streams are unidirectional.
- Changed stream error and stanza error namespace names to conform to the format defined in The IETF XML Registry [25].
- Removed note to RFC Editor regarding provisional namespace names.

### B.9 Changes from draft-ietf-xmpp-core-05

- Added <invalid-namespace/> as a stream error condition.
- Adjusted security considerations per discussion at IETF 56 and on list.

### B.10 Changes from draft-ietf-xmpp-core-04

- Added server-to-server examples for TLS and SASL.
- Changed error syntax, rules, and examples based on list discussion.
- Added schemas for the TLS, stream error, and stanza error namespaces.
- Added note to RFC Editor regarding provisional namespace names.
- Made numerous small editorial changes and clarified text throughout.

### B.11 Changes from draft-ietf-xmpp-core-03

- Clarified rules and procedures for TLS and SASL.
- Amplified stream error code syntax per list discussion.
- Made numerous small editorial changes.

### B.12 Changes from draft-ietf-xmpp-core-02

- Added dialback schema.
- Removed all DTDs since schemas provide more complete definitions.
- Added stream error codes.
- Clarified error code "philosophy".

### B.13 Changes from draft-ietf-xmpp-core-01

- Updated the addressing restrictions per list discussion and added references to the new nodeprep and resourceprep profiles.
- Corrected error in Stream Authentication regarding 'version' attribute.
- Made numerous small editorial changes.

### B.14 Changes from draft-ietf-xmpp-core-00

- Added information about TLS from list discussion.
- Clarified meaning of "ignore" based on list discussion.
- Clarified information about Universal Character Set data and character encodings.
- Provided base64-decoded information for examples.
- Fixed several errors in the schemas.
- Made numerous small editorial fixes.

### B.15 Changes from draft-miller-xmpp-core-02

- Brought Streams Authentication section into line with discussion on list and at IETF 55 meeting.
- Added information about the optional 'xml:lang' attribute per discussion on list and at IETF 55 meeting.
- Specified that validation is neither required nor recommended, and that the formal definitions (DTDs and schemas) are included for

descriptive purposes only.

- Specified that the response to an IQ stanza of type "get" or "set" must be an IQ stanza of type "result" or "error".

- Specified that compliant server implementations must process stanzas in order.

- Specified that for historical reasons some server implementations may accept 'stream:' as the only valid namespace prefix on the root stream element.

- Clarified the difference between 'jabber:client' and 'jabber:server' namespaces, namely, that 'to' and 'from' attributes are required on all stanzas in the latter but not the former.

- Fixed typo in Step 9 of the dialback protocol (changed db:result to db:verify).

- Removed references to TLS pending list discussion.

- Removed the non-normative appendix on OpenPGP usage pending its inclusion in a separate I-D.

- Simplified the architecture diagram, removed most references to services, and removed references to the 'jabber:component:*' namespaces.

- Noted that XMPP activity respects firewall administration policies.

- Further specified the scope and uniqueness of the 'id' attribute in all stanza types and the <thread/> element in message stanzas.

- Nomenclature changes: (1) from "chunks" to "stanzas"; (2) from "host" to "server" and from "node" to "client" (except with regard to definition of the addressing scheme).

## Intellectual Property Statement



## Full Copyright Statement

## Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.