An XCON Client Conference Control Package for the Media Control Channel Framework

draft-boulton-dispatch-conference-control-package-01

Abstract

The Centralized Conferencing (XCON) framework defines a model whereby client initiated interactions are required for creation, deletion, manipulation and querying the state of a conference. This document defines a Media Control Channel Package for XCON conferencing client initiated Conference Control. The Package is based on the Media Control Channel Framework, which is also used for media server control, thus optimizing the implementation for some entities participating in an XCON system.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on January 16, 2014.

Copyright Notice

Copyright (c) 2013 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents
carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction ................................................. 3
2. Conventions ................................................ 4
3. Terminology ............................................... 4
4. Overview .................................................. 4
5. Control Package Detail ..................................... 6
   5.1. Control Package Name .................................. 6
   5.2. Framework Message Usage ............................... 6
   5.3. Common XML Support .................................... 6
   5.4. Control Message Bodies ................................. 6
   5.5. REPORT Message Bodies ................................. 7
   5.6. Examples ............................................... 7
6. IANA Considerations ......................................... 7
   6.1. Control Package Registration .......................... 7
7. Security Considerations .................................... 7
8. Acknowledgments ............................................ 9
9. Change History .............................................. 9
10. References .................................................. 10
   10.1. Normative References ................................. 10
   10.2. Informative References ............................... 10
Authors' Addresses ............................................. 10
1. Introduction

The Conference Control Manipulation Protocol (CCMP) [RFC6503] provides a standards based mechanism to enable third party conference clients participating to interoperate with conference servers and manipulate conference parameters using HTTP as a transport. A Data Model [RFC6501] provides the data associated with a conference instance that is the target for the CCMP protocol operations.

A Control Channel Framework [RFC6230] has been created based on the Session Initiation protocol (SIP). It uses SIP to setup, maintain and terminate a reliable control channel for the purpose of exchanging control based interactions. While the control of media was the original problem domain for which this framework was developed, the Control Framework provides an extension template for creating extensions that specify the semantic detail associated with the control channel operations. The extension documents are known as Control Packages and an example is the 'Basic Mixer Control Package' [RFC6505].

This document will specify a Control Package for XCON conference control using the SIP Control Framework. The target for these operations is the same data, associated with conference instances per the data model, as CCMP. It should be noted that this mechanism is a complementary approach to CCMP [RFC6503]. In fact this specification simply provides a different transport mechanism. While the use of HTTP as a transport for CCMP is ideal for certain network deployments (for example Service Orientated Architectures), it is important to offer an alternative access method for clients with non SOA based technologies.

The Media Control Channel Framework provides the ideal mechanism for reliably exchanging control messages between a conferencing client and conference server. It provides inherent properties such as:

- Reliable delivery of control messages.
- Lightweight Protocol Data Units (PDU).
- Linked asynchronous transactional mechanism.
- Asynchronous event mechanism.

The SIP Control Framework uses SIP as its overlying rendezvous mechanism. This provides all the inherent benefits like:

- SIP Service Location - Use SIP Proxies or Back-to-Back User Agents for discovering Control Servers.
- SIP Security Mechanisms - Leverage established security mechanisms such as Transport Layer Security (TLS) and Client Authentication.
o Connection Maintenance - The ability to re-negotiate a connection, ensure it is active, audit parameters, and so forth.
o Agnostic - Allows for ease of extension.

Not only is the Media Control Channel Framework an ideal mechanism for controlling conference instances by participating clients, it also provides the property of re-use by conferencing systems of functionality implemented for controlling Media Servers etc. This includes re-using the SIP stack for control channel setup as well as the Control Channel Framework stack for receiving/sending the PDUs for multiple control packages in a conference system.

2. Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

3. Terminology

This document reuses the terminology defined and used in the framework and data model for centralized conferencing [RFC5239], [RFC6501] and [RFC6503].

4. Overview

The use of the Media Control Channel Framework offers an ideal mechanism for creating, deleting and manipulating XCON conference instances by participating clients. As the Control Channel Framework is a generic mechanism, this section provides non-normative detail showing how the Control Channel Framework can be applied to this particular use-case.

In [RFC6230], two distinct roles are defined - A Control Client and a Control Server. Such roles are interchangeable between entities within a session depending on package requirements. A simple diagram is illustrated in Figure 1
The XCON Conference Control package will cast a participating compliant XCON conferencing client that wishes to control a conference instance as a Control Client as defined in the SIP Control Framework. The conferencing client will have permission to generate and issue commands in CONTROL messages as defined in Section 5.2 of this document. It will also have the ability to receive responses to Conference Package CONTROL requests that are contained in either appropriate responses or subsequent REPORT messages, also specified in Section 5.2. The previous diagram can be updated as illustrated in Figure 2.

Figure 2: Conference Control Architecture

The specific format of the conference control messages and responses are defined in Section 5.4 and Section 5.5. They content of the control messages and responses is in the format specified in CCMP [RFC6503]. This allows a conferencing client to manage the same data
and message format independent of whether CCMP or the Control Framework messages are used to transport the information.

5. Control Package Detail

The Media Control Channel Framework defines rules that Control Package extensions must provide mandatory information as described in section 10 of [RFC6230]. This section fulfils the obligation.

5.1. Control Package Name

The SIP Control Framework requires a Control Package definition to specify and register a unique package name. The name and version of this Control Package is "xcon-conf-control/1.0".

5.2. Framework Message Usage

The Conference Control package uses the XML schema defined in CCMP [RFC6503]. To maintain the consistency with the design of the XML schema, the SIP Control Framework messages will be applied in a similar manner. The CONTROL message will be used to contain requests that enable conference manipulation - as specified in Section 5.4 and can only be sent from the conferencing client to a conference server. Responses, as specified in Section 5.5, can only be sent from the conference server to the conferencing client that initiated the request. Depending on the time it takes to process the request (as specified in [RFC6230]), responses can either be contained in a Control Framework 200 response or subsequent REPORT method.

5.3. Common XML Support

The Control Framework requires a Control Package definition to specify if the attributes for media dialog or conference references are required.

This package requires that the XML Schema in Section 16.1 of [RFC6230] MUST NOT be supported for media dialogs and conferences. But rather this package SHOULD use the XML schema as defined in [RFC6503], which is the same schema used for CCMP.

5.4. Control Message Bodies

A valid CONTROL body message MUST conform to the XML schema defined in [RFC6503] for the conference control. To be precise, the CONTROL message body MUST comply only to the 'ccmp-request-type' complexType.
5.5. REPORT Message Bodies

A valid CONTROL body message MUST conform to the XML schema defined in [RFC6503]. To be precise, the REPORT message body MUST comply only to the 'ccmp-response-type' complexType.

5.6. Examples

TODO

6. IANA Considerations

6.1. Control Package Registration

This section registers a new Media Control Channel Framework package, per the instructions in Section 12.1 of [RFC6230].

To: ietf-sip-control@iana.org
Subject: Registration of new Media Control Channel Framework package
Package Name: xcon-conf-control/1.0
[NOTE TO IANA/RFC-EDITOR: Please replace XXXX with the RFC number for this specification.] Published Specification(s): RFCXXXX
Person & email address to contact for further information: IETF, DISPATCH working group, (dispatch@ietf.org), Mary Barnes (mary.iets.barnes@gmail.com).

7. Security Considerations

As this Control Package processes XML markup, implementations MUST address the security considerations of [RFC3203].

As a Control Package of the Media Control Channel Framework, security, confidentiality, and integrity of messages transported over the Control Channel MUST be addressed as described in Section 12 of the Media Control Channel Framework [RFC6230], including transport-level protection, Control Channel policy management, and session establishment.

The Framework for Centralized Conferencing [RFC5239] specifies that the protocols used for manipulation and retrieval of confidential information MUST support a confidentiality and integrity mechanism. The XCON Data model [RFC6501] describes the requirements for ensuring the conference data is secured by the conference server (section 8). To support the confidentiality and integrity requirements, all conference control information included in the package defined in this document MUST have transport level protection; see [RFC6230], section 12.2 for further details on this topic. Adequate transport...
protection and authentication are critical, especially when the implementation is deployed in open networks. If the implementation fails to correctly address these issues, it risks exposure to malicious attacks, including (but not limited to):

Denial of Service: An attacker could insert a request message into the transport stream causing specific conferences on the conference server to be deleted. For example, a confRequest message with an operation of "delete" with a "<confObjID>" of "xcon:XXXX@example.com", where the value of "XXXX" could be guessed or discovered by registering for the 'conference' [RFC4575]. Likewise, an attacker could impersonate the conference server and insert error responses into the transport stream thereby denying the conferencing client access to package capabilities.

Resource Exhaustion: An attacker could insert into the Control Channel new request messages such as a confRequest message with an operation of "create" causing large numbers of conference resources to be allocated. At some point, this will exhaust the number of conference resources that the conference server is able to allocate.

The Media Control Channel Framework permits additional policy management (beyond that specified for the Media Control Channel Framework), including resource access and Control Channel usage, to be specified at the Control Package level. (See Section 12.3 of [RFC6230].)

Since creation of conference instances is associated with resources on the conference server, the security policy for this Control Package needs to address how such conference instances are securely managed across more than one Control Channel. Such a security policy is only useful for secure, confidential, and integrity-protected channels. The identity of Control Channels is determined by the channel identifier, i.e., the value of the 'cfw-id' attribute in the SDP and Dialog-ID header in the channel protocol per [RFC6230]. Channels are the same if they have the same identifier; otherwise, they are different. This Control Package imposes the following additional security policies:

Responses: The conference server MUST only send a response to a conference control request using the same Control Channel as the one used to send the request.

Notifications: The conference server MUST only send notification events for conference instances using the same Control Channel as it received the request creating the conference instance.
Rejection: The conference server SHOULD reject requests to manipulate an existing conference on the conference server if the channel is not the same as the one used when the mixer was created. The conference server rejects a request by sending a Control Framework 403 response (see Sections 7.4 and 12.3 of [RFC6230]). For example, if a channel with identifier 'cfw1234' has been used to send a request to create a particular conference instance and the conference server receives on channel 'cfw98969' a request to "delete" this particular conference instance, then the conference server sends a Control Framework 403 response.

There can be valid reasons why an implementation does not reject an manipulation request on a different channel from the one that created the mixer. For example, a system administrator might require a separate channel to delete conferences consuming excessive system resources. However, the full implications need to be understood by the implementation and carefully weighed before accepting these reasons as valid. If the reasons are not valid in their particular circumstances, the conference server rejects such requests.

There can also be valid reasons for 'channel handover' including high availability support or when one conference server needs to take over management of conference instances after the conference server that created them has failed. This could be achieved by the Control Channels using the same channel identifier, one after another. For example, assume a channel is created with the identifier 'cfw1234', and the channel is used to create conference instances on the conference server. This channel (and associated SIP dialog) then terminates due to a failure on the conference server. As permitted by the Control Framework, the channel identifier 'cfw1234' could then be reused so that another channel is created with the same identifier 'cfw1234', allowing it to 'take over' management of the conference instances on the conference server. Again, the implementation needs to understand the full implications and carefully weigh them before accepting these reasons as valid. If the reasons are not valid for their particular circumstances, the conference server uses the appropriate SIP mechanisms to prevent session establishment when the same channel identifier is used in setting up another Control Channel (see Section 4 of [RFC6230]).

8. Acknowledgments

9. Change History

Note to RFC Editor: Please delete this section prior to publication.
Changes between 00 and 01:

1. Updating terminology to be consistent with RFC 6503 - i.e., conferencing client and conference server.
2. Updates to security section to be consistent with requirements for a control package per RFC6230.
3. Minor editorial changes.

10. References

10.1. Normative References


10.2. Informative References

Authors' Addresses

Chris Boulton
NS-Technologies

Email: chris@ns-technologies.com

Mary Barnes
Polycom
TX

Email: mary.ietf.barnes@gmail.com