BFCPbis Working Group
Internet-Draft
Obsoletes: 4582 (if approved)
Intended status: Standards Track
Expires: January 15, 2013

G. Camarillo
Ericsson
K. Drage
Alcatel-Lucent
T. Kristensen, Ed.
Cisco
J. Ott
Aalto University
C. Eckel
Cisco

July 14, 2012

The Binary Floor Control Protocol (BFCP) draft-ietf-bfcpbis-rfc4582bis-04

Abstract

Floor control is a means to manage joint or exclusive access to shared resources in a (multiparty) conferencing environment. Thereby, floor control complements other functions -- such as conference and media session setup, conference policy manipulation, and media control -- that are realized by other protocols.

This document specifies the Binary Floor Control Protocol (BFCP). BFCP is used between floor participants and floor control servers, and between floor chairs (i.e., moderators) and floor control servers.

This document obsoletes RFC 4582. Changes from RFC 4582 are summarized in section 16.

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 15, 2013.

Table of Contents

1. Introduction

Within a conference, some applications need to manage the access to a set of shared resources, such as the right to send media to a particular media session. Floor control enables such applications to provide users with coordinated (shared or exclusive) access to these resources.

The Requirements for Floor Control Protocol [13] list a set of requirements that need to be met by floor control protocols. The Binary Floor Control Protocol (BFCP), which is specified in this document, meets these requirements.

In addition, BFCP has been designed so that it can be used in low-bandwidth environments. The binary encoding used by BFCP achieves a small message size (when message signatures are not used) that keeps the time it takes to transmit delay-sensitive BFCP messages to a minimum. Delay-sensitive BFCP messages include FloorRequest, FloorRelease, FloorRequestStatus, and ChairAction. It is expected that future extensions to these messages will not increase the size of these messages in a significant way.

The remainder of this document is organized as follows: Section 2 defines the terminology used throughout this document, Section 3 discusses the scope of BFCP (i.e., which tasks fall within the scope of BFCP and which ones are performed using different mechanisms), Section 4 provides a non-normative overview of BFCP operation, and subsequent sections provide the normative specification of BFCP.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14, RFC 2119 [1] and indicate requirement levels for compliant implementations.

Media Participant: An entity that has access to the media resources of a conference (e.g., it can receive a media stream). In floor-controlled conferences, a given media participant is typically colocated with a floor participant, but it does not need to be. Third-party floor requests consist of having a floor participant request a floor for a media participant when they are not colocated. The protocol between a floor participant and a media participant (that are not colocated) is outside the scope of this document.

Client: A floor participant or a floor chair that communicates with a

floor control server using BFCP.

Floor: A temporary permission to access or manipulate a specific shared resource or set of resources.

Floor Chair: A logical entity that manages one floor (grants, denies, or revokes a floor). An entity that assumes the logical role of a floor chair for a given transaction may assume a different role (e.g., floor participant) for a different transaction. The roles of floor chair and floor participant are defined on a transaction-by-transaction basis. BFCP transactions are defined in Section 8.

Floor Control: A mechanism that enables applications or users to gain safe and mutually exclusive or non-exclusive input access to the shared object or resource.

Floor Control Server: A logical entity that maintains the state of the floor(s), including which floors exists, who the floor chairs are, who holds a floor, etc. Requests to manipulate a floor are directed at the floor control server. The floor control server of a conference may perform other logical roles (e.g., floor participant) in another conference.

Floor Participant: A logical entity that requests floors, and possibly information about them, from a floor control server. An entity that assumes the logical role of a floor participant for a given transaction may assume a different role (e.g., a floor chair) for a different transaction. The roles of floor participant and floor chair are defined on a transaction-by-transaction basis. BFCP transactions are defined in Section 8. In floor-controlled conferences, a given floor participant is typically colocated with a media participant, but it does not need to be. Third-party floor requests consist of having a floor participant request a floor for a media participant when they are not colocated.

Participant: An entity that acts as a floor participant, as a media participant, or as both.

3. Scope

As stated earlier, BFCP is a protocol to coordinate access to shared resources in a conference following the requirements defined in [13]. Floor control complements other functions defined in the XCON conferencing framework [14]. The floor control protocol BFCP defined in this document only specifies a means to arbitrate access to floors. The rules and constraints for floor arbitration and the results of floor assignments are outside the scope of this document

and are defined by other protocols [14].

Figure 1 shows the tasks that BFCP can perform.

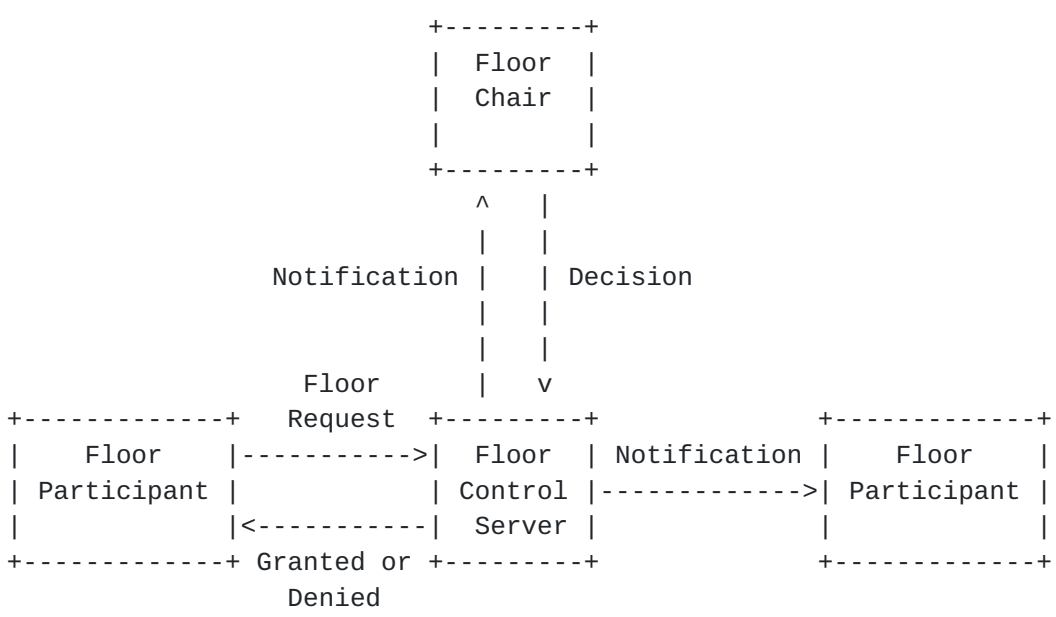


Figure 1: Functionality provided by BFCP

BFCP provides a means:

- for floor participants to send floor requests to floor control servers.
- for floor control servers to grant or deny requests to access a given resource from floor participants.
- for floor chairs to send floor control servers decisions regarding floor requests.
- for floor control servers to keep floor participants and floor chairs informed about the status of a given floor or a given floor request.

Even though tasks that do not belong to the previous list are outside the scope of BFCP, some of these out-of-scope tasks relate to floor control and are essential for creating floors and establishing BFCP connections between different entities. In the following subsections, we discuss some of these tasks and mechanisms to perform them.

3.1. Floor Creation

The association of a given floor with a resource or a set of resources (e.g., media streams) is out of the scope of BFCP as described in [14]. Floor creation and termination are also outside the scope of BFCP; these aspects are handled using the conference control protocol for manipulating the conference object. Consequently, the floor control server needs to stay up to date on changes to the conference object (e.g., when a new floor is created).

3.2. Obtaining Information to Contact a Floor Control Server

A client needs a set of data in order to establish a BFCP connection to a floor control server. These data include the transport address of the server, the conference identifier, and a user identifier.

Clients can obtain this information in different ways. One is to use an SDP offer/answer [12] exchange, which is described in [7]. Other mechanisms are described in the XCON framework [14] (and other related documents).

3.3. Obtaining Floor-Resource Associations

Floors are associated with resources. For example, a floor that controls who talks at a given time has a particular audio session as its associated resource. Associations between floors and resources are part of the conference object.

Floor participants and floor chairs need to know which resources are associated with which floors. They can obtain this information by using different mechanisms, such as an SDP offer/answer [12] exchange. How to use an SDP offer/answer exchange to obtain these associations is described in [7].

> Note that floor participants perform SDP offer/answer exchanges with the conference focus of the conference. So, the conference focus needs to obtain information about associations between floors and resources in order to be able to provide this information to a floor participant in an SDP offer/answer exchange.

Other mechanisms for obtaining this information, including discussion of how the information is made available to a (SIP) Focus, are described in the XCON framework [14] (and other related documents).

3.4. Privileges of Floor Control

A participant whose floor request is granted has the right to use (in a certain way) the resource or resources associated with the floor that was requested. For example, the participant may have the right to send media over a particular audio stream.

Nevertheless, holding a floor does not imply that others will not be able to use its associated resources at the same time, even if they do not have the right to do so. Determination of which media participants can actually use the resources in the conference is discussed in the XCON Framework [14].

4. Overview of Operation

This section provides a non-normative description of BFCP operations. Section 4.1 describes the interface between floor participants and floor control servers, and Section 4.2 describes the interface between floor chairs and floor control servers.

BFCP messages, which use a TLV (Type-Length-Value) binary encoding, consist of a common header followed by a set of attributes. The common header contains, among other information, a 32-bit conference identifier. Floor participants, media participants, and floor chairs are identified by 16-bit user identifiers.

BFCP supports nested attributes (i.e., attributes that contain attributes). These are referred to as grouped attributes.

There are two types of transaction in BFCP: client-initiated transactions and server-initiated transactions. Client-initiated transactions consist of a message from a client to the floor control server and a response from the floor control server to the client. Correspondingly, server-initiated transactions consist of a message from the floor control server to a client and the associated acknowledgement message from the client to the floor control server. Both messages can be related because they carry the same Transaction ID value in their common headers.

4.1. Floor Participant to Floor Control Server Interface

Floor participants request a floor by sending a FloorRequest message to the floor control server. BFCP supports third-party floor requests. That is, the floor participant sending the floor request need not be colocated with the media participant that will get the floor once the floor request is granted. FloorRequest messages carry the identity of the requester in the User ID field of the common

header, and the identity of the beneficiary of the floor (in third-party floor requests) in a BENEFICIARY-ID attribute.

> Third-party floor requests can be sent, for example, by floor participants that have a BFCP connection to the floor control server but that are not media participants (i.e., they do not handle any media).

FloorRequest messages identify the floor or floors being requested by carrying their 16-bit floor identifiers in FLOOR-ID attributes. If a FloorRequest message carries more than one floor identifier, the floor control server treats all the floor requests as an atomic package. That is, the floor control server either grants or denies all the floors in the FloorRequest message.

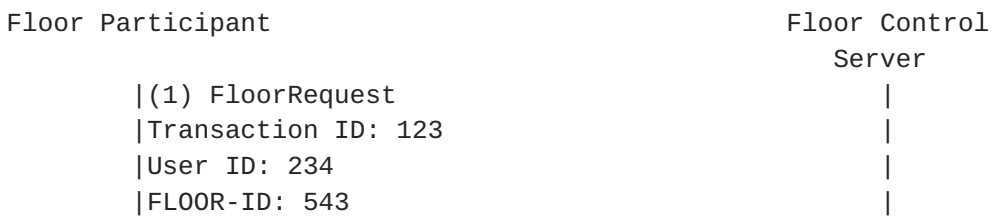
Floor control servers respond to FloorRequest messages with FloorRequestStatus messages, which provide information about the status of the floor request. The first FloorRequestStatus message is the response to the FloorRequest message from the client, and therefore has the same Transaction ID as the FloorRequest.

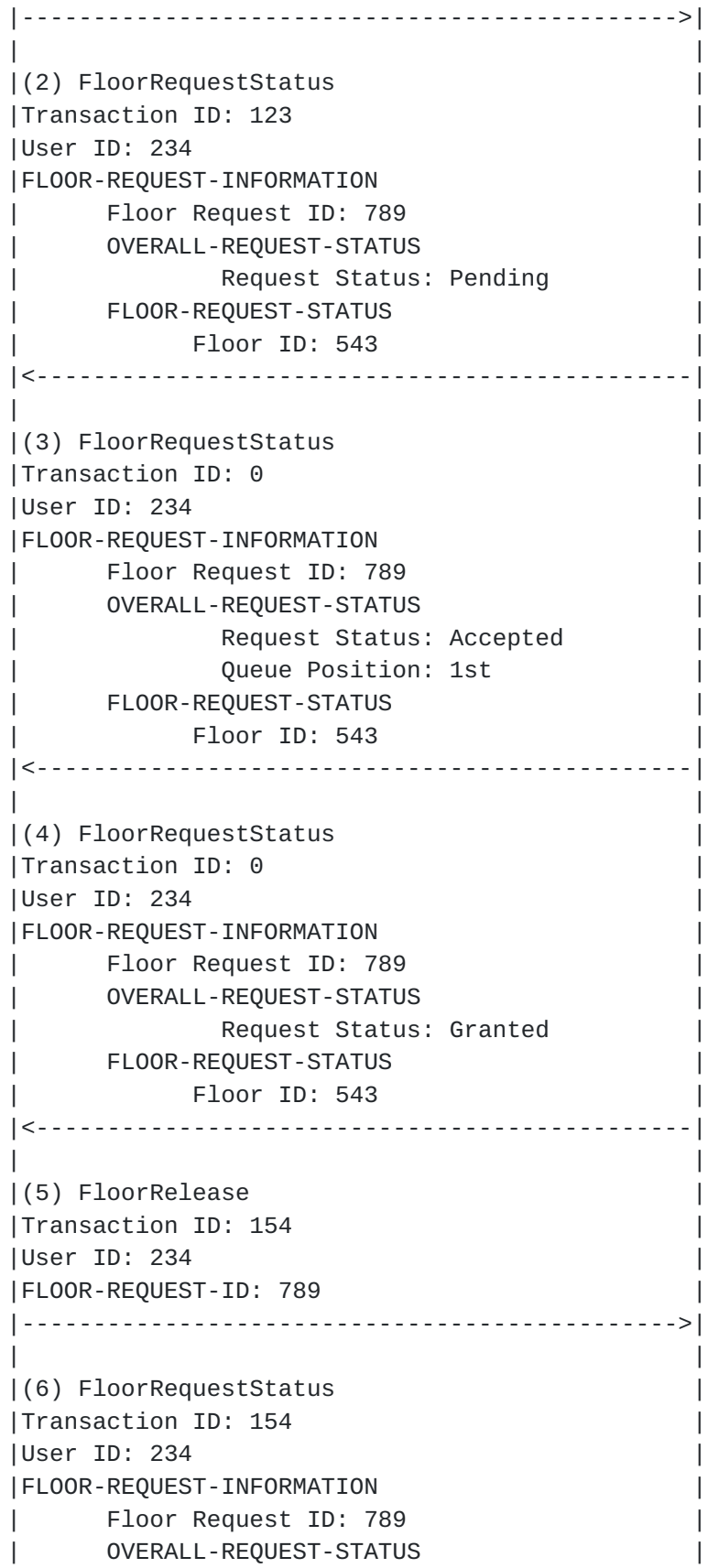
Additionally, the first FloorRequestStatus message carries the Floor Request ID in a FLOOR-REQUEST-INFORMATION attribute. Subsequent FloorRequestStatus messages related to the same floor request will carry the same Floor Request ID. This way, the floor participant can associate them with the appropriate floor request.

Messages from the floor participant related to a particular floor request also use the same Floor Request ID as the first FloorRequestStatus Message from the floor control server.

Figures 2 and 3 below show call flows for two sample BFCP interactions when used over reliable transport. Appendix A shows the same sample interactions but over an unreliable transport.

Figure 2 shows how a floor participant requests a floor, obtains it, and, at a later time, releases it. This figure illustrates the use, among other things, of the Transaction ID and the FLOOR-REQUEST-ID attribute.




(2) FloorRequestStatus
Transaction ID: 123
User ID: 234
FLOOR-REQUEST-INFORMATION
Floor Request ID: 789
OVERALL-REQUEST-STATUS
Request Status: Pending
FLOOR-REQUEST-STATUS
Floor ID: 543
(3) FloorRequestStatus
Transaction ID: 0
User ID: 234
FLOOR-REQUEST-INFORMATION
Floor Request ID: 789
OVERALL-REQUEST-STATUS
Request Status: Accepted
Queue Position: 1st
FLOOR-REQUEST-STATUS
Floor ID: 543
(4) FloorRequestStatus
Transaction ID: 0
User ID: 234
FLOOR-REQUEST-INFORMATION
Floor Request ID: 789
OVERALL-REQUEST-STATUS
Request Status: Granted
FLOOR-REQUEST-STATUS
Floor ID: 543
(5) FloorRelease
Transaction ID: 154
User ID: 234
FLOOR-REQUEST-ID: 789
(6) FloorRequestStatus
Transaction ID: 154
User ID: 234
FLOOR-REQUEST-INFORMATION
Floor Request ID: 789
OVERALL-REQUEST-STATUS

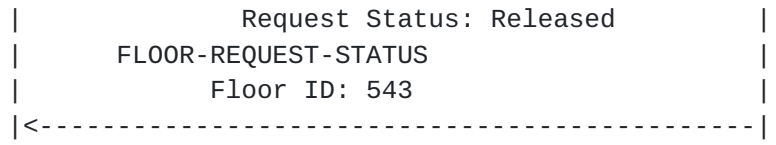
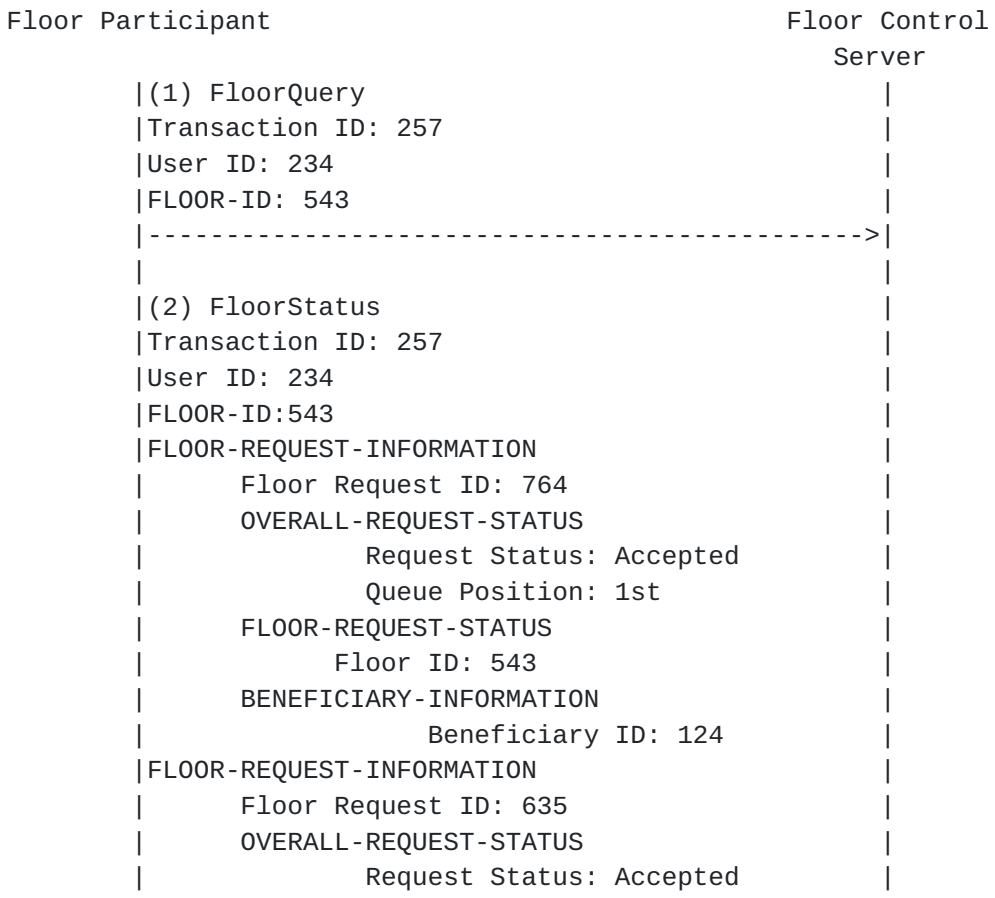


Figure 2: Requesting and releasing a floor

Figure 3 shows how a floor participant requests to be informed on the status of a floor. The first FloorStatus message from the floor control server is the response to the FloorQuery message and, as such, has the same Transaction ID as the FloorQuery message.

Subsequent FloorStatus messages consist of server-initiated transactions, and therefore their Transaction ID is 0. FloorStatus message (2) indicates that there are currently two floor requests for the floor whose Floor ID is 543. FloorStatus message (3) indicates that the floor requests with Floor Request ID 764 has been granted, and the floor request with Floor Request ID 635 is the first in the queue. FloorStatus message (4) indicates that the floor request with Floor Request ID 635 has been granted.



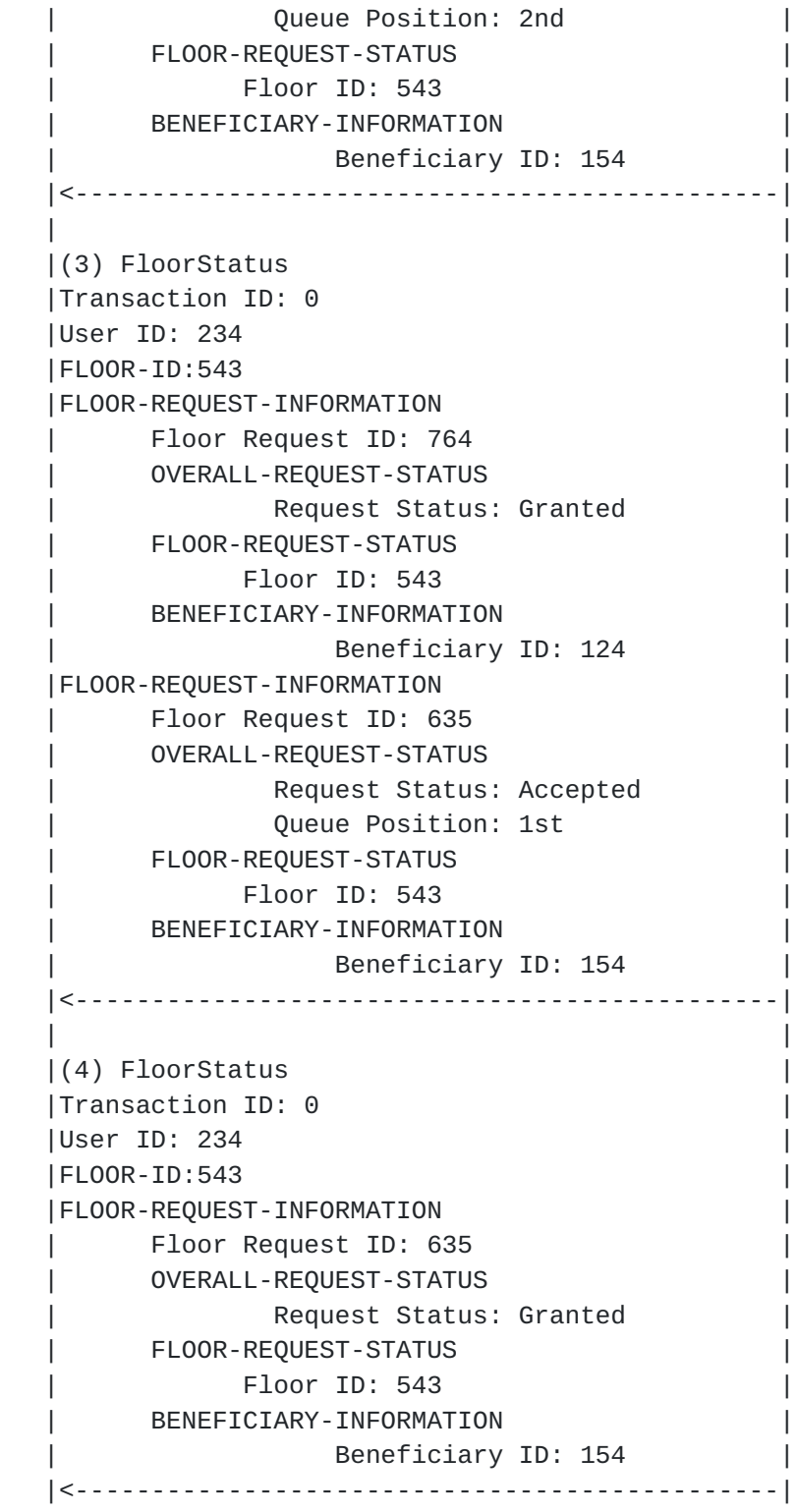


Figure 3: Obtaining status information about a floor

FloorStatus messages contain information about the floor requests they carry. For example, FloorStatus message (4) indicates that the

floor request with Floor Request ID 635 has as the beneficiary (i.e., the participant that holds the floor when a particular floor request is granted) the participant whose User ID is 154. The floor request applies only to the floor whose Floor ID is 543. That is, this is not a multi-floor floor request.

> A multi-floor floor request applies to more than one floor (e.g., a participant wants to be able to speak and write on the whiteboard at the same time). The floor control server treats a multi-floor floor request as an atomic package. That is, the floor control server either grants the request for all floors or denies the request for all floors.

4.2. Floor Chair to Floor Control Server Interface

Figure 4 shows a floor chair instructing a floor control server to grant a floor.

> Note, however, that although the floor control server needs to take into consideration the instructions received in ChairAction messages (e.g., granting a floor), it does not necessarily need to perform them exactly as requested by the floor chair. The operation that the floor control server performs depends on the ChairAction message and on the internal state of the floor control server.

For example, a floor chair may send a ChairAction message granting a floor that was requested as part of an atomic floor request operation that involved several floors. Even if the chair responsible for one of the floors instructs the floor control server to grant the floor, the floor control server will not grant it until the chairs responsible for the other floors agree to grant them as well. In another example, a floor chair may instruct the floor control server to grant a floor to a participant. The floor control server needs to revoke the floor from its current holder before granting it to the new participant.

So, the floor control server is ultimately responsible for keeping a coherent floor state using instructions from floor chairs as input to this state.

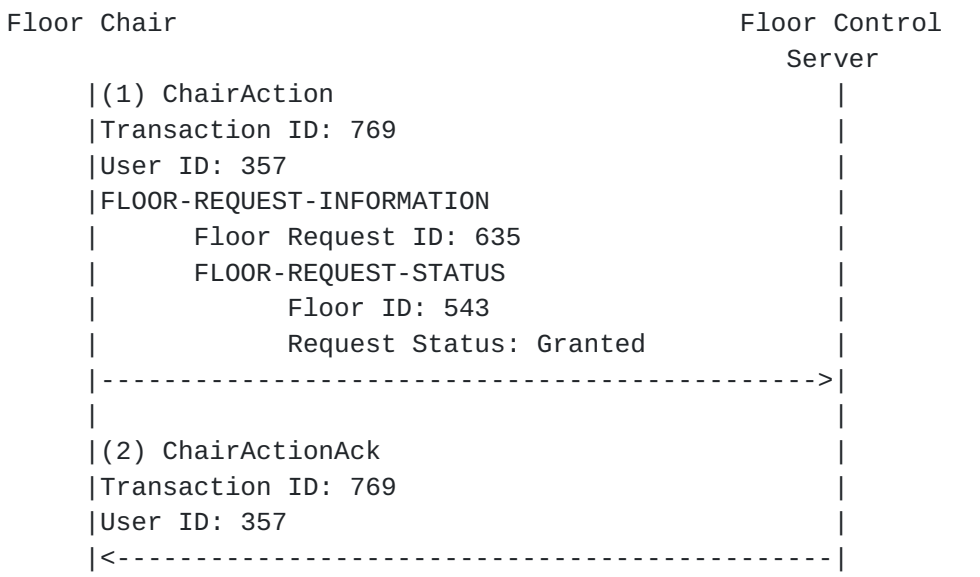


Figure 4: Chair instructing the floor control server

5. Packet Format

BFCP packets consist of a 12-octet common header followed by attributes. All the protocol values MUST be sent in network byte order.

5.1. COMMON-HEADER Format

The following is the format of the common header.

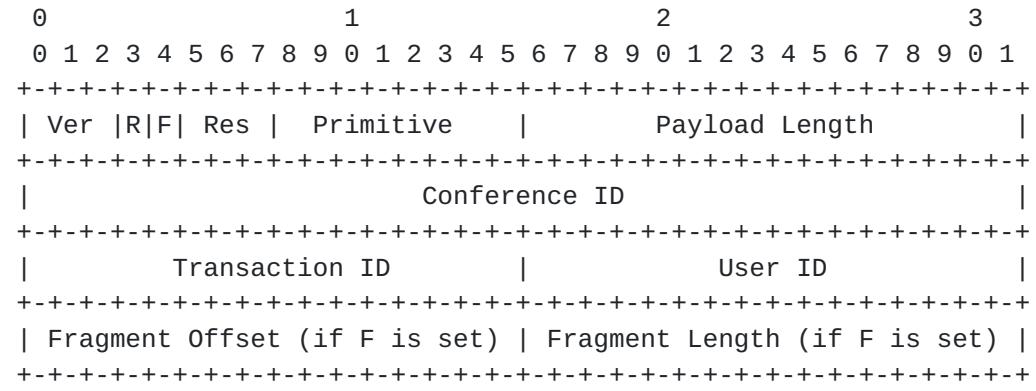


Figure 5: COMMON-HEADER format

Ver: The 3-bit version field MUST be set to 1 when using BFCP over reliable transport, i.e. as in [17]. The 3-bit version field MUST be set to 2 when using BFCP over unreliable transport, with the

extensions specified in this document. If a Floor Control Server receives a message with an unsupported version field value, the receiving server MAY send an Error message with parameter value 12 (Unsupported Version) to indicate this.

R: The Transaction Responder (R) flag-bit has relevance only for use of BFCP over unreliable transport. When cleared, it indicates that this message is a request initiating a new transaction, and the Transaction ID that follows has been generated for this transaction. When set, it indicates that this message is a response to a previous request, and the Transaction ID that follows is the one associated with that request. When BFCP is used over reliable transports, the flag has no significance and SHOULD be cleared.

F: The Fragmentation (F) flag-bit has relevance only for use of BFCP over unreliable transport. When cleared, the message is not fragmented. When set, it indicates that the message is a fragment of a large fragmented BFCP message. (The optional fields Fragment Offset and Fragment Length described below are present only if the F flag is set). When BFCP is used over reliable transports, the flag has no significance and SHOULD be cleared.

Res: At this point, the 3 bits in the reserved field SHOULD be set to zero by the sender of the message and MUST be ignored by the receiver.

Primitive: This 8-bit field identifies the main purpose of the message. The following primitive values are defined:

Value	Primitive	Direction
1	FloorRequest	P -> S
2	FloorRelease	P -> S
3	FloorRequestQuery	P -> S ; Ch -> S
4	FloorRequestStatus	P <- S ; Ch <- S
5	UserQuery	P -> S ; Ch -> S
6	UserStatus	P <- S ; Ch <- S
7	FloorQuery	P -> S ; Ch -> S
8	FloorStatus	P <- S ; Ch <- S
9	ChairAction	Ch -> S
10	ChairActionAck	Ch <- S
11	Hello	P -> S ; Ch -> S
12	HelloAck	P <- S ; Ch <- S
13	Error	P <- S ; Ch <- S
14	FloorRequestStatusAck	P -> S ; Ch -> S
15	FloorStatusAck	P -> S ; Ch -> S
16	Goodbye	P -> S ; Ch -> S ;
		P <- S ; Ch <- S
17	GoodbyeAck	P -> S ; Ch -> S ;
		P <- S ; Ch <- S

S: Floor Control Server / P: Floor Participant / Ch: Floor Chair

Table 1: BFCP primitives

Payload Length: This 16-bit field contains the length of the message in 4-octet units, excluding the common header. If a Floor Control Server receives a message with an incorrect payload length field value, the receiving server MAY send an Error message with parameter value 13 (Incorrect Message Length) to indicate this.

Conference ID: This 32-bit unsigned integer field identifies the conference the message belongs to.

Transaction ID: This field contains a 16-bit value that allows users to match a given message with its response (see Section 8).

User ID: This field contains a 16-bit unsigned integer that uniquely identifies a participant within a conference.

The identity used by a participant in BFCP, which is carried in the User ID field, is generally mapped to the identity used by the same participant in the session establishment protocol (e.g., in SIP). The way this mapping is performed is outside the scope of this specification.

Fragment Offset: This optional field is present only if the F flag is set and contains a 16-bit value that specifies the number of 4-octet units contained in previous fragments, excluding the common header.

Fragment Length: This optional field is present only if the F flag is set and contains a 16-bit value that specifies the number of 4-octet units contained in this fragment, excluding the common header.

5.2. Attribute Format

BFCP attributes are encoded in TLV (Type-Length-Value) format. Attributes are 32-bit aligned.

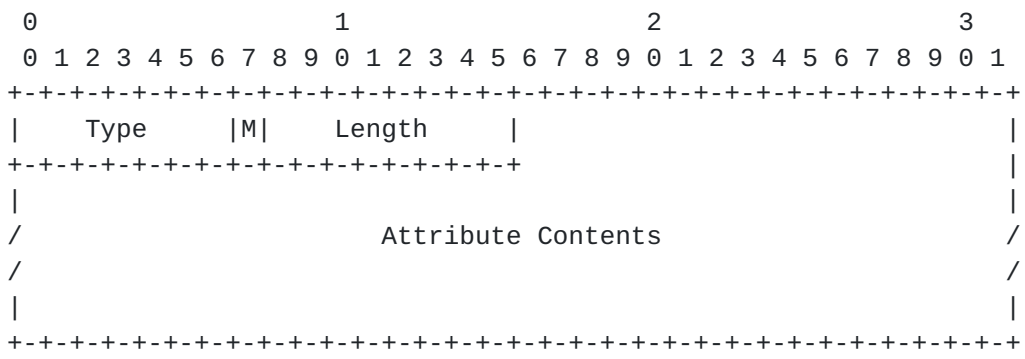


Figure 6: Attribute format

Type: This 7-bit field contains the type of the attribute. Each attribute, identified by its type, has a particular format. The attribute formats defined are:

Unsigned16: The contents of the attribute consist of a 16-bit unsigned integer.

OctetString16: The contents of the attribute consist of 16 bits of arbitrary data.

OctetString: The contents of the attribute consist of arbitrary data of variable length.

Grouped: The contents of the attribute consist of a sequence of attributes.

Note that extension attributes defined in the future may define new attribute formats.

The following attribute types are defined:

Type	Attribute	Format
1	BENEFICIARY-ID	Unsigned16
2	FLOOR-ID	Unsigned16
3	FLOOR-REQUEST-ID	Unsigned16
4	PRIORITY	OctetString16
5	REQUEST-STATUS	OctetString16
6	ERROR-CODE	OctetString
7	ERROR-INFO	OctetString
8	PARTICIPANT-PROVIDED-INFO	OctetString
9	STATUS-INFO	OctetString
10	SUPPORTED-ATTRIBUTES	OctetString
11	SUPPORTED-PRIMITIVES	OctetString
12	USER-DISPLAY-NAME	OctetString
13	USER-URI	OctetString
14	BENEFICIARY-INFORMATION	Grouped
15	FLOOR-REQUEST-INFORMATION	Grouped
16	REQUESTED-BY-INFORMATION	Grouped
17	FLOOR-REQUEST-STATUS	Grouped
18	OVERALL-REQUEST-STATUS	Grouped

Table 2: BFCP attributes

M: The 'M' bit, known as the Mandatory bit, indicates whether support of the attribute is required. If a Floor Control Server receives an unrecognized attribute with the 'M' bit set the server MAY send an Error message with parameter value 4 (Unknown Mandatory Attribute) to indicate this. The 'M' bit is significant for extension attributes defined in other documents only. All attributes specified in this document MUST be understood by the receiver so that the setting of the 'M' bit is irrelevant for these. In all other cases, the unrecognized attribute is ignored but the message is processed.

Length: This 8-bit field contains the length of the attribute in octets, excluding any padding defined for specific attributes. The length of attributes that are not grouped includes the Type, 'M' bit, and Length fields. The Length in grouped attributes is the length of the grouped attribute itself (including Type, 'M' bit, and Length fields) plus the total length (including padding) of all the included attributes.

Attribute Contents: The contents of the different attributes are defined in the following sections.

5.2.1. BENEFICIARY-ID

The following is the format of the BENEFICIARY-ID attribute.

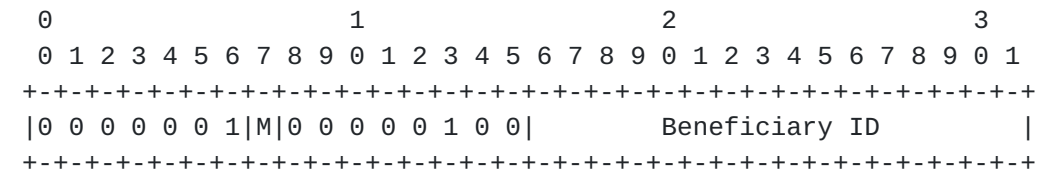


Figure 7: BENEFICIARY-ID format

Beneficiary ID: This field contains a 16-bit value that uniquely identifies a user within a conference.

> Note that although the formats of the Beneficiary ID and of the User ID field in the common header are similar, their semantics are different. The Beneficiary ID is used in third-party floor requests and to request information about a particular participant.

5.2.2. FLOOR-ID

The following is the format of the FLOOR-ID attribute.

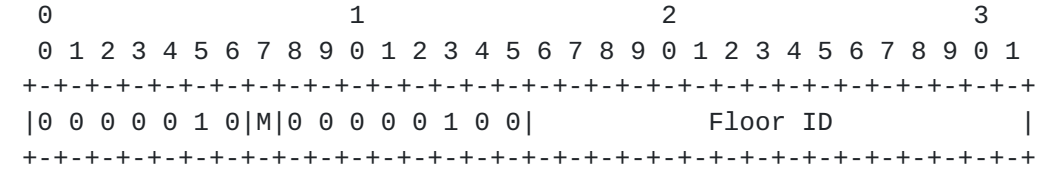


Figure 8: FLOOR-ID format

Floor ID: This field contains a 16-bit value that uniquely identifies a floor within a conference.

5.2.3. FLOOR-REQUEST-ID

The following is the format of the FLOOR-REQUEST-ID attribute.

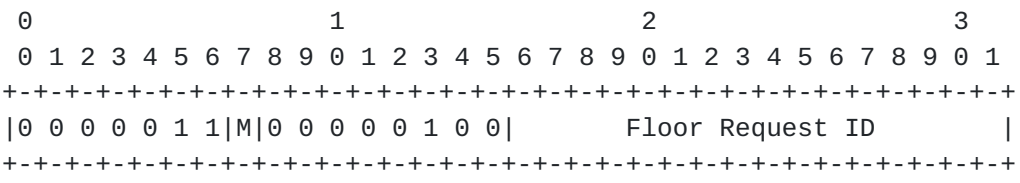


Figure 9: FLOOR-REQUEST-ID format

Floor Request ID: This field contains a 16-bit value that identifies a floor request at the floor control server.

5.2.4. PRIORITY

The following is the format of the PRIORITY attribute.

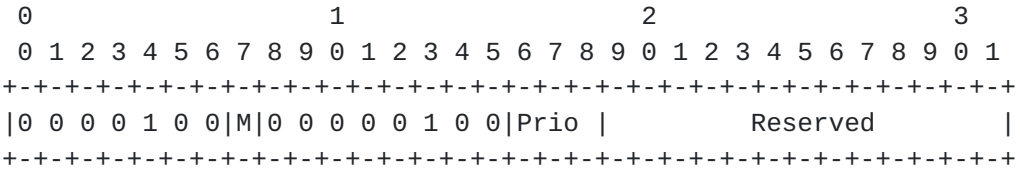


Figure 10: PRIORITY format

Prio: This field contains a 3-bit priority value, as shown in Table 3. Senders SHOULD NOT use values higher than 4 in this field. Receivers MUST treat values higher than 4 as if the value received were 4 (Highest). The default priority value when the PRIORITY attribute is missing is 2 (Normal).

Value	Priority
0	Lowest
1	Low
2	Normal
3	High
4	Highest

Table 3: Priority values

Reserved: At this point, the 13 bits in the reserved field SHOULD be set to zero by the sender of the message and MUST be ignored by the receiver.

5.2.5. REQUEST-STATUS

The following is the format of the REQUEST-STATUS attribute.

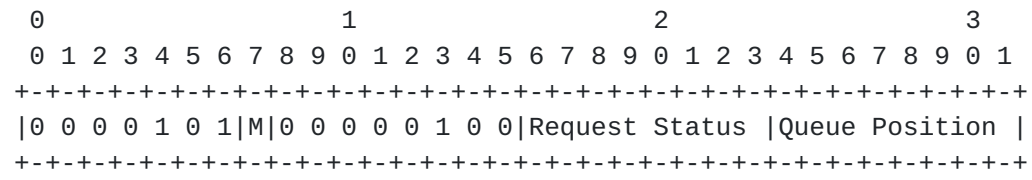


Figure 11: REQUEST-STATUS format

Request Status: This 8-bit field contains the status of the request, as described in the following table.

Value	Status
1	Pending
2	Accepted
3	Granted
4	Denied
5	Cancelled
6	Released
7	Revoked

Table 4: Request Status values

Queue Position: This 8-bit field contains, when applicable, the position of the floor request in the floor request queue at the server. If the Request Status value is different from Accepted, if the floor control server does not implement a floor request queue, or if the floor control server does not want to provide the client with this information, all the bits of this field SHOULD be set to zero.

A floor request is in Pending state if the floor control server needs to contact a floor chair in order to accept the floor request, but has not done it yet. Once the floor control chair accepts the floor request, the floor request is moved to the Accepted state.

5.2.6. ERROR-CODE

The following is the format of the ERROR-CODE attribute.

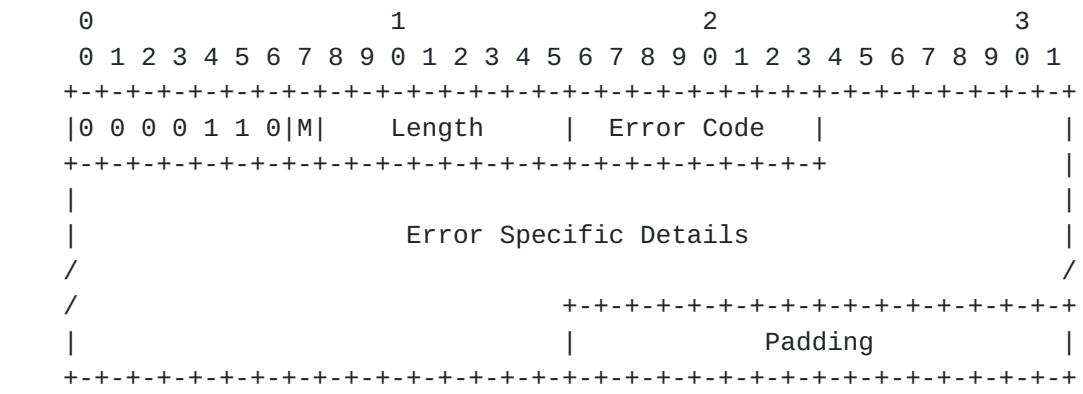


Figure 12: ERROR-CODE format

Error Code: This 8-bit field contains an error code from the following table. If an error code is not recognized by the receiver, then the receiver MUST assume that an error exists, and therefore that the original message that triggered the Error message to be sent is processed, but the nature of the error is unclear.

Value	Meaning
1	Conference does not Exist
2	User does not Exist
3	Unknown Primitive
4	Unknown Mandatory Attribute
5	Unauthorized Operation
6	Invalid Floor ID
7	Floor Request ID Does Not Exist
8	You have Already Reached the Maximum Number of Ongoing Floor Requests for this Floor
9	Use TLS
10	Unable to Parse Message
11	Use DTLS
12	Unsupported Version
13	Incorrect Message Length
14	Generic Error

Table 5: Error Code meaning

Note: The Generic Error error code is intended being used by a BFCP entity when an error occurs and the other specific error codes do not apply.

Error Specific Details: Present only for certain Error Codes. In this document, only for Error Code 4 (Unknown Mandatory Attribute).

See Section 5.2.6.1 for its definition.

Padding: One, two, or three octets of padding added so that the contents of the ERROR-CODE attribute is 32-bit aligned. If the attribute is already 32-bit aligned, no padding is needed.

The Padding bits SHOULD be set to zero by the sender and MUST be ignored by the receiver.

5.2.6.1. Error-Specific Details for Error Code 4

The following is the format of the Error-Specific Details field for Error Code 4.

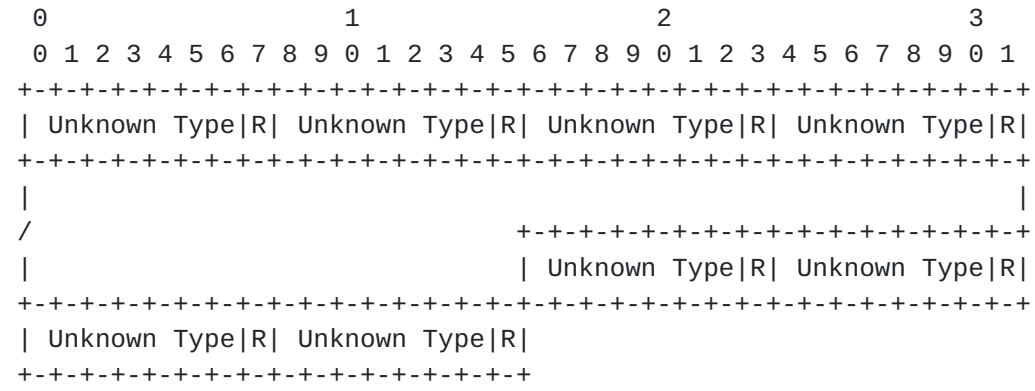


Figure 13: Unknown attributes format

Unknown Type: These 7-bit fields contain the Types of the attributes (which were present in the message that triggered the Error message) that were unknown to the receiver.

R: At this point, this bit is reserved. It SHOULD be set to zero by the sender of the message and MUST be ignored by the receiver.

5.2.7. ERROR-INFO

The following is the format of the ERROR-INFO attribute.

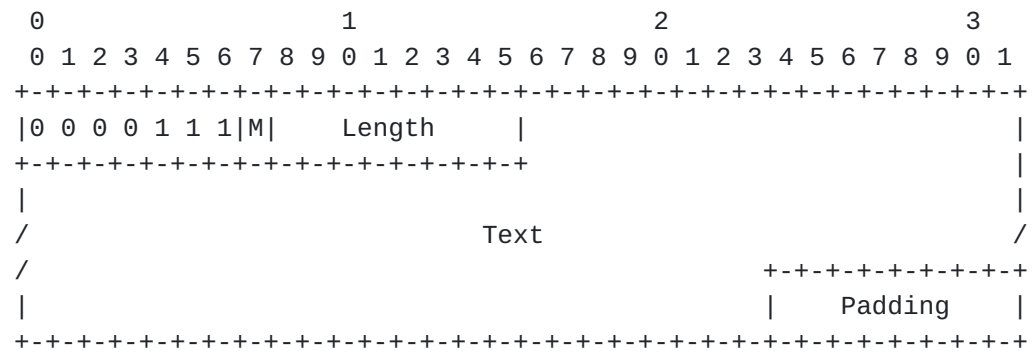


Figure 14: ERROR-INFO format

Text: This field contains UTF-8 [6] encoded text.

In some situations, the contents of the Text field may be generated by an automaton. If this automaton has information about the preferred language of the receiver of a particular ERROR-INFO attribute, it MAY use this language to generate the Text field.

Padding: One, two, or three octets of padding added so that the contents of the ERROR-INFO attribute is 32-bit aligned. The Padding bits SHOULD be set to zero by the sender and MUST be ignored by the receiver. If the attribute is already 32-bit aligned, no padding is needed.

5.2.8. PARTICIPANT-PROVIDED-INFO

The following is the format of the PARTICIPANT-PROVIDED-INFO attribute.

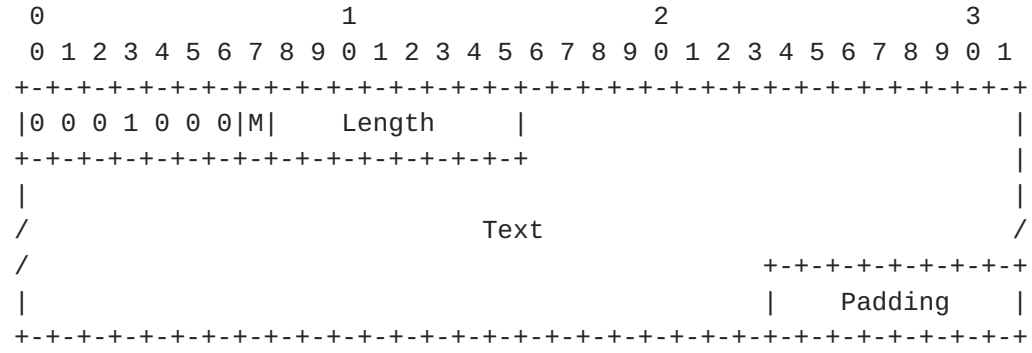


Figure 15: PARTICIPANT-PROVIDED-INFO format

Text: This field contains UTF-8 [6] encoded text.

Padding: One, two, or three octets of padding added so that the

contents of the PARTICIPANT-PROVIDED-INFO attribute is 32-bit aligned. The Padding bits SHOULD be set to zero by the sender and MUST be ignored by the receiver. If the attribute is already 32-bit aligned, no padding is needed.

5.2.9. STATUS-INFO

The following is the format of the STATUS-INFO attribute.

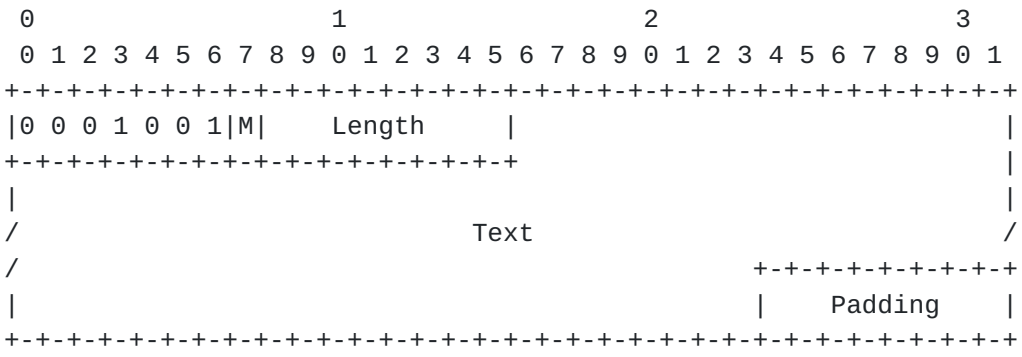


Figure 16: STATUS-INFO format

Text: This field contains UTF-8 [6] encoded text.

In some situations, the contents of the Text field may be generated by an automaton. If this automaton has information about the preferred language of the receiver of a particular STATUS-INFO attribute, it MAY use this language to generate the Text field.

Padding: One, two, or three octets of padding added so that the contents of the STATUS-INFO attribute is 32-bit aligned. The Padding bits SHOULD be set to zero by the sender and MUST be ignored by the receiver. If the attribute is already 32-bit aligned, no padding is needed.

5.2.10. SUPPORTED-ATTRIBUTES

The following is the format of the SUPPORTED-ATTRIBUTES attribute.

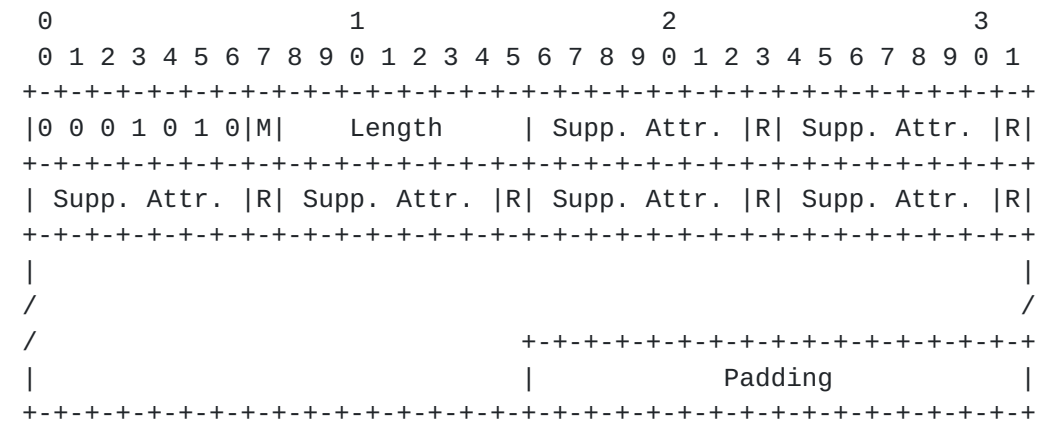


Figure 17: SUPPORTED-ATTRIBUTES format

Supp. Attr.: These fields contain the Types of the attributes that are supported by the floor control server in the following format:

R: Reserved: This bit MUST be set to zero upon transmission and MUST be ignored upon reception.

Padding: One, two, or three octets of padding added so that the contents of the SUPPORTED-ATTRIBUTES attribute is 32-bit aligned. If the attribute is already 32-bit aligned, no padding is needed.

The Padding bits SHOULD be set to zero by the sender and MUST be ignored by the receiver.

5.2.11. SUPPORTED-PRIMITIVES

The following is the format of the SUPPORTED-PRIMITIVES attribute.

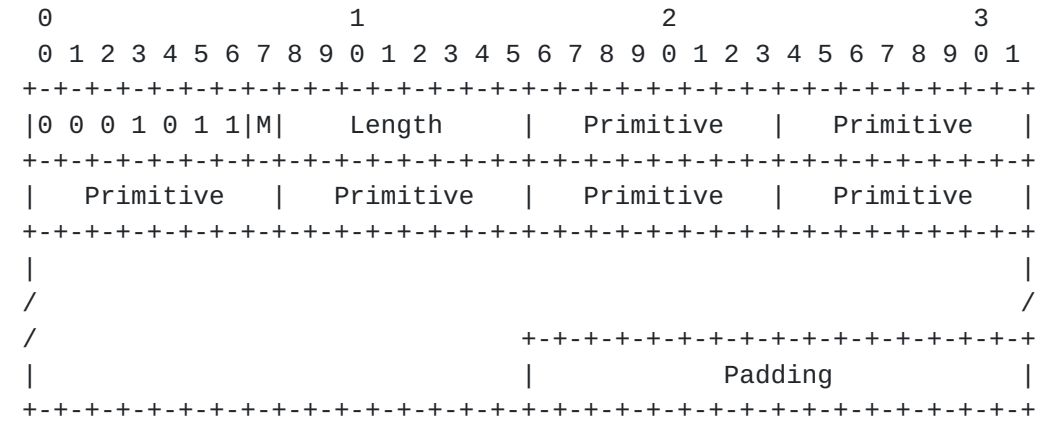


Figure 18: SUPPORTED-PRIMITIVES format

Primitive: These fields contain the types of the BFCP messages that are supported by the floor control server. See Table 1 for the list of BFCP primitives.

Padding: One, two, or three octets of padding added so that the contents of the SUPPORTED-PRIMITIVES attribute is 32-bit aligned. If the attribute is already 32-bit aligned, no padding is needed.

The Padding bits SHOULD be set to zero by the sender and MUST be ignored by the receiver.

5.2.12. USER-DISPLAY-NAME

The following is the format of the USER-DISPLAY-NAME attribute.

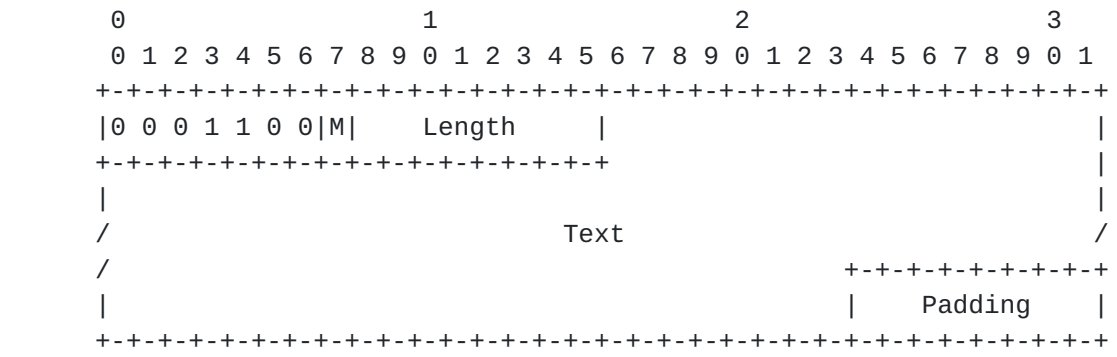


Figure 19: USER-DISPLAY-NAME format

Text: This field contains the UTF-8 encoded name of the user.

Padding: One, two, or three octets of padding added so that the contents of the USER-DISPLAY-NAME attribute is 32-bit aligned. The Padding bits SHOULD be set to zero by the sender and MUST be ignored by the receiver. If the attribute is already 32-bit aligned, no padding is needed.

5.2.13. USER-URI

The following is the format of the USER-URI attribute.

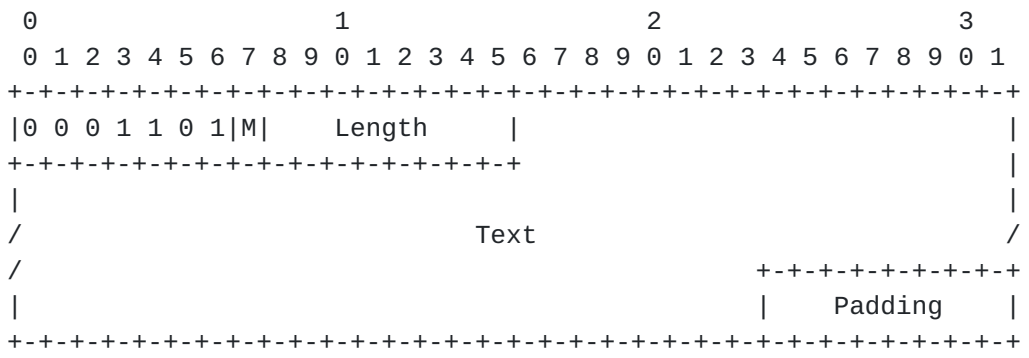


Figure 20: USER-URI format

Text: This field contains the UTF-8 encoded user's contact URI, that is, the URI used by the user to set up the resources (e.g., media streams) that are controlled by BFCP. For example, in the context of a conference set up by SIP, the USER-URI attribute would carry the SIP URI of the user.

> Messages containing a user's URI in a USER-URI attribute also contain the user's User ID. This way, a client receiving such a message can correlate the user's URI (e.g., the SIP URI the user used to join a conference) with the user's User ID.

Padding: One, two, or three octets of padding added so that the contents of the USER-URI attribute is 32-bit aligned. The Padding bits SHOULD be set to zero by the sender and MUST be ignored by the receiver. If the attribute is already 32-bit aligned, no padding is needed.

5.2.14. BENEFICIARY-INFORMATION

The BENEFICIARY-INFORMATION attribute is a grouped attribute that consists of a header, which is referred to as BENEFICIARY-INFORMATION-HEADER, followed by a sequence of attributes. The following is the format of the BENEFICIARY-INFORMATION-HEADER:

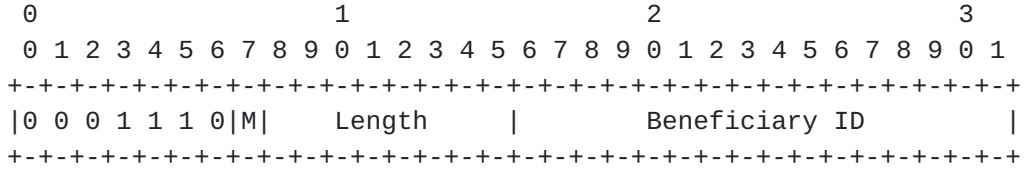


Figure 21: BENEFICIARY-INFORMATION-HEADER format

Beneficiary ID: This field contains a 16-bit value that uniquely identifies a user within a conference.

The following is the ABNF (Augmented Backus-Naur Form) [2] of the BENEFICIARY-INFORMATION grouped attribute. (EXTENSION-ATTRIBUTE refers to extension attributes that may be defined in the future.)

```
BENEFICIARY-INFORMATION =   (BENEFICIARY-INFORMATION-HEADER)
                            [USER-DISPLAY-NAME]
                            [USER-URI]
                           *(EXTENSION-ATTRIBUTE)
```

Figure 22: BENEFICIARY-INFORMATION format

5.2.15. FLOOR-REQUEST-INFORMATION

The FLOOR-REQUEST-INFORMATION attribute is a grouped attribute that consists of a header, which is referred to as FLOOR-REQUEST-INFORMATION-HEADER, followed by a sequence of attributes. The following is the format of the FLOOR-REQUEST-INFORMATION-HEADER:

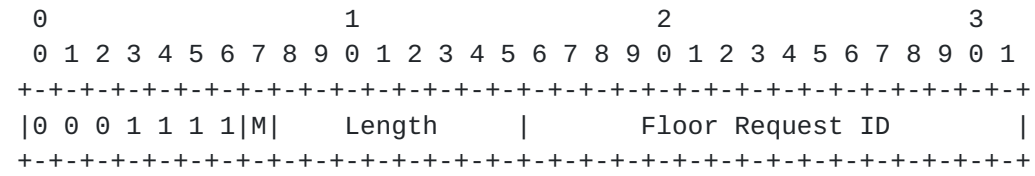


Figure 23: FLOOR-REQUEST-INFORMATION-HEADER format

Floor Request ID: This field contains a 16-bit value that identifies a floor request at the floor control server.

The following is the ABNF of the FLOOR-REQUEST-INFORMATION grouped attribute. (EXTENSION-ATTRIBUTE refers to extension attributes that may be defined in the future.)

```
FLOOR-REQUEST-INFORMATION =   (FLOOR-REQUEST-INFORMATION-HEADER)
                              [OVERALL-REQUEST-STATUS]
                             1*(FLOOR-REQUEST-STATUS)
                              [BENEFICIARY-INFORMATION]
                              [REQUESTED-BY-INFORMATION]
                              [PRIORITY]
                              [PARTICIPANT-PROVIDED-INFO]
                               *(EXTENSION-ATTRIBUTE)
```

Figure 24: FLOOR-REQUEST-INFORMATION format

5.2.16. REQUESTED-BY-INFORMATION

The REQUESTED-BY-INFORMATION attribute is a grouped attribute that consists of a header, which is referred to as REQUESTED-BY-INFORMATION-HEADER, followed by a sequence of attributes. The following is the format of the REQUESTED-BY-INFORMATION-HEADER:

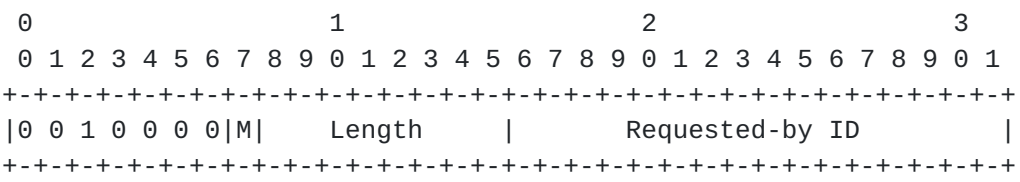


Figure 25: REQUESTED-BY-INFORMATION-HEADER format

Requested-by ID: This field contains a 16-bit value that uniquely identifies a user within a conference.

The following is the ABNF of the REQUESTED-BY-INFORMATION grouped attribute. (EXTENSION-ATTRIBUTE refers to extension attributes that may be defined in the future.)

```
REQUESTED-BY-INFORMATION =   (REQUESTED-BY-INFORMATION-HEADER)
                             [USER-DISPLAY-NAME]
                             [USER-URI]
                            *(EXTENSION-ATTRIBUTE)
```

Figure 26: REQUESTED-BY-INFORMATION format

5.2.17. FLOOR-REQUEST-STATUS

The FLOOR-REQUEST-STATUS attribute is a grouped attribute that consists of a header, which is referred to as FLOOR-REQUEST-STATUS-HEADER, followed by a sequence of attributes. The following is the format of the FLOOR-REQUEST-STATUS-HEADER:

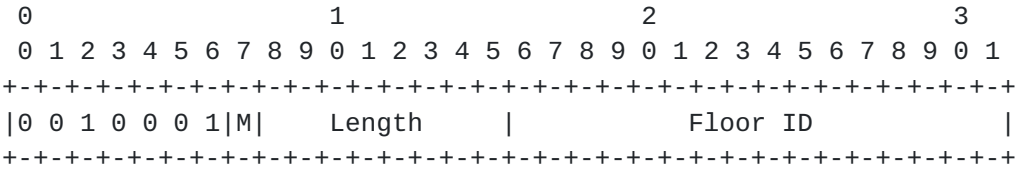


Figure 27: FLOOR-REQUEST-STATUS-HEADER format

Floor ID: this field contains a 16-bit value that uniquely identifies

a floor within a conference.

The following is the ABNF of the FLOOR-REQUEST-STATUS grouped attribute. (EXTENSION-ATTRIBUTE refers to extension attributes that may be defined in the future.)

```
FLOOR-REQUEST-STATUS     =   (FLOOR-REQUEST-STATUS-HEADER)
                             [REQUEST-STATUS]
                             [STATUS-INFO]
                            *(EXTENSION-ATTRIBUTE)
```

Figure 28: FLOOR-REQUEST-STATUS format

5.2.18. OVERALL-REQUEST-STATUS

The OVERALL-REQUEST-STATUS attribute is a grouped attribute that consists of a header, which is referred to as OVERALL-REQUEST-STATUS-HEADER, followed by a sequence of attributes. The following is the format of the OVERALL-REQUEST-STATUS-HEADER:

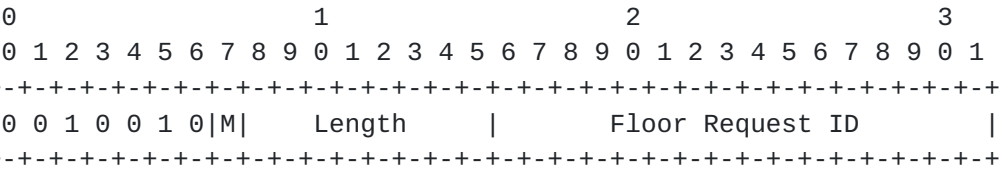


Figure 29: OVERALL-REQUEST-STATUS-HEADER format

Floor Request ID: this field contains a 16-bit value that identifies a floor request at the floor control server.

The following is the ABNF of the OVERALL-REQUEST-STATUS grouped attribute. (EXTENSION-ATTRIBUTE refers to extension attributes that may be defined in the future.)

```
OVERALL-REQUEST-STATUS   =   (OVERALL-REQUEST-STATUS-HEADER)
                             [REQUEST-STATUS]
                             [STATUS-INFO]
                            *(EXTENSION-ATTRIBUTE)
```

Figure 30: OVERALL-REQUEST-STATUS format

5.3. Message Format

This section contains the normative ABNF (Augmented Backus-Naur Form) [2] of the BFCP messages. Extension attributes that may be defined in the future are referred to as EXTENSION-ATTRIBUTE in the ABNF.

5.3.1. FloorRequest

Floor participants request a floor by sending a FloorRequest message to the floor control server. The following is the format of the FloorRequest message:

```
FloorRequest =   (COMMON-HEADER)
                1*(FLOOR-ID)
                  [BENEFICIARY-ID]
                  [PARTICIPANT-PROVIDED-INFO]
                  [PRIORITY]
                 *(EXTENSION-ATTRIBUTE)
```

Figure 31: FloorRequest format

5.3.2. FloorRelease

Floor participants release a floor by sending a FloorRelease message to the floor control server. Floor participants also use the FloorRelease message to cancel pending floor requests. The following is the format of the FloorRelease message:

```
FloorRelease =   (COMMON-HEADER)
                 (FLOOR-REQUEST-ID)
                *(EXTENSION-ATTRIBUTE)
```

Figure 32: FloorRelease format

5.3.3. FloorRequestQuery

Floor participants and floor chairs request information about a floor request by sending a FloorRequestQuery message to the floor control server. The following is the format of the FloorRequestQuery message:

```
FloorRequestQuery =   (COMMON-HEADER)
                      (FLOOR-REQUEST-ID)
                     *(EXTENSION-ATTRIBUTE)
```

Figure 33: FloorRequestQuery format

5.3.4. FloorRequestStatus

The floor control server informs floor participants and floor chairs about the status of their floor requests by sending them FloorRequestStatus messages. The following is the format of the FloorRequestStatus message:

```
FloorRequestStatus =   (COMMON-HEADER)
                       (FLOOR-REQUEST-INFORMATION)
                      *(EXTENSION-ATTRIBUTE)
```

Figure 34: FloorRequestStatus format

5.3.5. UserQuery

Floor participants and floor chairs request information about a participant and the floor requests related to this participant by sending a UserQuery message to the floor control server. The following is the format of the UserQuery message:

```
UserQuery =   (COMMON-HEADER)
              [BENEFICIARY-ID]
             *(EXTENSION-ATTRIBUTE)
```

Figure 35: UserQuery format

5.3.6. UserStatus

The floor control server provides information about participants and their related floor requests to floor participants and floor chairs by sending them UserStatus messages. The following is the format of the UserStatus message:

```
UserStatus =   (COMMON-HEADER)
               [BENEFICIARY-INFORMATION]
              *(FLOOR-REQUEST-INFORMATION)
              *(EXTENSION-ATTRIBUTE)
```

Figure 36: UserStatus format

5.3.7. FloorQuery

Floor participants and floor chairs request information about a floor or floors by sending a FloorQuery message to the floor control server. The following is the format of the FloorRequest message:

```
FloorQuery =   (COMMON-HEADER)
              *(FLOOR-ID)
              *(EXTENSION-ATTRIBUTE)
```

Figure 37: FloorQuery format

5.3.8. FloorStatus

The floor control server informs floor participants and floor chairs about the status (e.g., the current holder) of a floor by sending them FloorStatus messages. The following is the format of the FloorStatus message:

```
FloorStatus        =     (COMMON-HEADER)
                         [FLOOR-ID]
                        *(FLOOR-REQUEST-INFORMATION)
                        *(EXTENSION-ATTRIBUTE)
```

Figure 38: FloorStatus format

5.3.9. ChairAction

Floor chairs send instructions to floor control servers by sending ChairAction messages. The following is the format of the ChairAction message:

```
ChairAction  =   (COMMON-HEADER)
                 (FLOOR-REQUEST-INFORMATION)
                *(EXTENSION-ATTRIBUTE)
```

Figure 39: ChairAction format

5.3.10. ChairActionAck

Floor control servers confirm that they have accepted a ChairAction message by sending a ChairActionAck message. The following is the format of the ChairActionAck message:

```
ChairActionAck  =   (COMMON-HEADER)
                   *(EXTENSION-ATTRIBUTE)
```

Figure 40: ChairActionAck format

5.3.11. Hello

Floor participants and floor chairs check the liveliness of floor control servers by sending a Hello message. The following is the format of the Hello message:

```
Hello         =  (COMMON-HEADER)
                *(EXTENSION-ATTRIBUTE)
```

Figure 41: Hello format

5.3.12. HelloAck

Floor control servers confirm that they are alive on reception of a Hello message by sending a HelloAck message. The following is the format of the HelloAck message:

```
HelloAck      =  (COMMON-HEADER)
                 (SUPPORTED-PRIMITIVES)
                 (SUPPORTED-ATTRIBUTES)
                *(EXTENSION-ATTRIBUTE)
```

Figure 42: HelloAck format

5.3.13. Error

Floor control servers inform floor participants and floor chairs about errors processing requests by sending them Error messages. The following is the format of the Error message:

```
Error              =   (COMMON-HEADER)
                       (ERROR-CODE)
                       [ERROR-INFO]
                      *(EXTENSION-ATTRIBUTE)
```

Figure 43: Error format

5.3.14. FloorRequestStatusAck

Floor participants and chairs acknowledge the receipt of a subsequent FloorRequestStatus message from the floor control server when communicating over unreliable transport. The following is the format of the FloorRequestStatusAck message:

```
FloorRequestStatusAck          =    (COMMON-HEADER)
                                   *(EXTENSION-ATTRIBUTE)
```

Figure 44: FloorRequestStatusAck format

5.3.15. FloorStatusAck

Floor participants and chairs acknowledge the receipt of a subsequent FloorStatus message from the floor control server when communicating over unreliable transport. The following is the format of the FloorStatusAck message:

```
FloorStatusAck                 =    (COMMON-HEADER)
                                   *(EXTENSION-ATTRIBUTE)
```

Figure 45: FloorStatusAck format

5.3.16. Goodbye

BFCP entities communicating over an unreliable transport that wish to dissociate themselves from their remote participant do so through the transmission of a Goodbye. The following is the format of the Goodbye message:

```
Goodbye                        =    (COMMON-HEADER)
                                   *(EXTENSION-ATTRIBUTE)
```

Figure 46: Goodbye format

5.3.17. GoodbyeAck

BFCP entities communicating over an unreliable transport should acknowledge the receipt of a Goodbye message from a peer. The following is the format of the GoodbyeAck message:

```
GoodbyeAck                    =    (COMMON-HEADER)
                                  *(EXTENSION-ATTRIBUTE)
```

Figure 47: GoodbyeAck format

6. Transport

The transport over which BFCP entities exchange messages depends on how clients obtain information to contact the floor control server (e.g. using an SDP offer/answer exchange [7]). Two transports are supported: TCP, appropriate where entities can be sure that their connectivity is not impeded by NAT devices, media relays or firewalls; and UDP for those deployments where TCP may not be applicable or appropriate.

6.1. Reliable Transport

BFCP entities may elect to exchange BFCP messages using TCP connections. TCP provides an in-order reliable delivery of a stream of bytes. Consequently, message framing is implemented in the application layer. BFCP implements application-layer framing using TLV-encoded attributes.

A client MUST NOT use more than one TCP connection to communicate with a given floor control server within a conference. Nevertheless, if the same physical box handles different clients (e.g. a floor chair and a floor participant), which are identified by different User IDs, a separate connection per client is allowed.

If a BFCP entity (a client or a floor control server) receives data that cannot be parsed, the entity MUST close the TCP connection, and the connection SHOULD be reestablished. Similarly, if a TCP connection cannot deliver a BFCP message and times out, the TCP connection SHOULD be reestablished.

The way connection reestablishment is handled depends on how the client obtains information to contact the floor control server. Once the TCP connection is reestablished, the client MAY resend those messages for which it did not get a response from the floor control server.

If a floor control server detects that the TCP connection towards one of the floor participants is lost, it is up to the local policy of the floor control server what to do with the pending floor requests of the floor participant. In any case, it is RECOMMENDED that the floor control server keep the floor requests (i.e., that it does not cancel them) while the TCP connection is reestablished.

If a client wishes to end its BFCP connection with a floor control server, the client closes (i.e., a graceful close) the TCP connection towards the floor control server. If a floor control server wishes to end its BFCP connection with a client (e.g., the Focus of the conference informs the floor control server that the client has been kicked out from the conference), the floor control server closes (i.e., a graceful close) the TCP connection towards the client.

6.2. Unreliable Transport

BFCP entities may elect to exchange BFCP messages using UDP datagrams. UDP is an unreliable transport where neither delivery nor ordering is assured. Each BFCP UDP datagram MUST contain exactly one BFCP message. In the event the size of a BFCP message exceeds the MTU size, the BFCP message will be fragmented at the IP layer. Considerations related to fragmentation are covered in Section 6.3. The message format for exchange of BFCP in UDP datagrams is the same as for a TCP stream above.

Clients MUST announce their presence to the floor control server by transmission of a Hello message. This Hello message MUST be responded to with a HelloAck message and only upon receipt of HelloAck can the client consider the floor control service as present and available.

As described in Section 8, each request sent by a floor participant or chair shall form a client transaction that expects an acknowledgement message back from the floor control server within a retransmission window. Concordantly, messages sent by the floor control server that are not transaction-completing (e.g. FloorStatus announcements as part of a FloorQuery subscription) are server-initiated transactions that require acknowledgement messages from the floor participant and chair entities to which they were sent.

If a Floor Control Server receives data that cannot be parsed, the receiving server MAY send an Error message with parameter value 10 (Unable to parse message) indicating receipt of a malformed message. If the message can be parsed to the extent that it is able to discern that it was a response to an outstanding request transaction, the client MAY discard the message and await retransmission. BFCP entities receiving an Error message with value 10 SHOULD acknowledge the error and act accordingly.

Transaction ID values are non-sequential and entities are at liberty to select values at random. Entities MUST only have at most one outstanding request transaction at any one time. Implicit subscriptions occur for a client-initiated request transaction whose acknowledgement is implied by the first server-initiated response for

that transaction, followed by zero of more subsequent server-initiated messages corresponding to the same transaction. An example is a FloorRequest message for which there are potentially multiple responses from the floor control server as it processes intermediate states until a terminal state (e.g. Granted or Denied) is attained. The subsequent changes in state for the request are new transactions whose Transaction ID is determined by the floor control server and whose receipt by the client participant shall be acknowledged with a FloorRequestStatusAck message.

By restricting entities to having at most one pending transaction open in a BFCP connection, both the out-of-order receipt of messages as well as the possibility for congestion are mitigated. Additional details regarding congestion control are provided in Section 6.2.1. A server-initiated request (e.g. a FloorStatus with an update from the floor control server) received by a participant before the initial FloorRequestStatus message that closes the client-initiated transaction that was instigated by the FloorRequest MUST be treated as superseding the information conveyed in any delinquent response. As the floor control server cannot send a second update to the implicit floor status subscription until the first is acknowledged, ordinality is maintained.

If a client wishes to end its BFCP association with a floor control server, it is RECOMMENDED that the client send a Goodbye message to dissociate itself from any allocated resources. If a floor control server wishes to end its BFCP association with a client (e.g. the Focus of the conference informs the floor control server that the client has been kicked out from the conference), it is RECOMMENDED that the floor control server send a Goodbye message towards the client.

6.2.1. Congestion Control

BFCP may be characterized to generate "low data-volume" traffic, per the classification in [19]. Nevertheless is it necessary to ensure suitable and necessary congestion control mechanisms are used for BFCP over UDP. As described in previous paragraph, within the same BFCP connection, every entity - client or server - is only allowed to send one request at a time, and await the acknowledging response. This way at most one datagram is sent per RTT given the message is not lost during transmission. In case the message is lost, the request retransmission timer T1 specified in Section 8.3.1 will fire and the message is retransmitted up to three times, in addition to the original transmission of the message. The default initial interval is set to 500ms and the interval is doubled after each retransmission attempt, this is identical to the specification of the T1 timer in SIP as described in Section 17.1.1.2 of [16].

6.2.2. ICMP Error Handling

If a BFCP entity receives an ICMP port unreachable message mid-conversation, the entity SHOULD treat the conversation as closed (e.g. an implicit Goodbye message from the peer). The entity MAY attempt to re-establish the conversation afresh. The new connection will appear as a wholly new floor participant, chair or floor control server with all state previously held about that participant lost.

Note: This is because the peer entities cannot rely on IP and port tuple to uniquely identify the participant, nor would extending Hello to include an attribute that advertised what the entity previously was assigned as a User ID be acceptable due to session hijacking.

In deployments where NAT appliances, firewalls or other such devices are present and affecting port reachability for each entity, one possibility is to utilize the peer connectivity checks, relay use and NAT pinhole maintenance mechanisms defined in ICE [15].

6.3. Large Message Considerations

Large messages become a concern when using BFCP if the overall size of a single BFCP message exceeds that representable within the 16-bit Payload Length field of the COMMON-HEADER. When using UDP, there is the added concern that a single BFCP message can be fragmented at the IP layer if its overall size exceeds the MTU threshold of the network.

6.3.1. Fragmentation Handling

When transmitting a BFCP message with size greater than the MTU, the sender should fragment the message into a series of N contiguous data ranges. The sender should then create N BFCP fragment messages (one for each data range) with the same Transaction ID. The size of each of these N messages MUST be smaller than the MTU. The F flag in the COMMON-HEADER is set to indicate fragmentation of the BFCP message.

For each of these fragments the Fragment Offset and Fragment Length fields are included in the COMMON-HEADER. The Fragment Offset field denotes the number of bytes contained in the previous fragments. The Fragment Length contains the length of the fragment itself. Note that the Payload Length field contains the length of the entire, unfragmented message.

When a BFCP implementation receives a BFCP message fragment, it MUST buffer the fragment until it has received the entire BFCP message. The state machine should handle the BFCP message only after all the fragments for the message have been received.

If a fragment of a BFCP message is lost, the sender will not receive an ACK for the message. Therefore the sender will retransmit the message with same transaction ID as specified in Section 8.3. If the ACK sent by the receiver is lost, then the entire message will be resent by the sender. The receiver MUST then retransmit the ACK. The receiver can discard an incomplete buffer utilizing the Response Retransmission Timer, starting the timer after the receipt of the first fragment.

6.3.2. NAT Traversal

One of the key benefits when using UDP for BFCP communication is the ability to leverage the existing NAT traversal infrastructure and strategies deployed to facilitate transport of the media associated with the video conferencing sessions. Depending on the given deployment, this infrastructure typically includes some subset of ICE [15].

In order to facilitate the initial establishment of NAT bindings, and to maintain those bindings once established, BFCP over UDP entities are RECOMMENDED to use STUN [11] for keep-alives, as described for SIP [10]. This results in each BFCP entity sending a packet, both to open the pinhole and to learn what IP/port the NAT assigned for the binding.

> Informational note: Since the version number is set to 2 when BFCP is used over unreliable transport, cf. the Ver field in Section 5.1, it is straight forward to distinguish between STUN and BFCP packets even without checking the STUN magic cookie [11].

In order to facilitate traversal of BFCP packets through NATs, BFCP over UDP entities are RECOMMENDED to use symmetric ports for sending and receiving BFCP packets, as recommended for RTP/RTCP [9].

7. Lower-Layer Security

BFCP relies on lower-layer security mechanisms to provide replay and integrity protection and confidentiality. BFCP floor control servers and clients (which include both floor participants and floor chairs) MUST support TLS for transport over TCP [4] and MUST support DTLS [5] for transport over UDP. Any BFCP entity MAY support other security mechanisms.

BFCP entities MUST support, at a minimum, the TLS_RSA_WITH_AES_128_CBC_SHA ciphersuite [4].

Which party, the client or the floor control server, acts as the TLS/

DTLS server depends on how the underlying TLS/DTLS connection is established. For a TCP/TLS connection established using an SDP offer/answer exchange [7], the answerer (which may be the client or the floor control server) always acts as the TLS server. For a UDP/DTLS connection established using the same exchange, either party can be the DTLS server depending on the setup attributes exchanged; examples can be found in [8].

8. Protocol Transactions

In BFCP, there are two types of transactions: client-initiated transactions and server-initiated transactions (notifications). Client-initiated transactions consist of a request from a client to a floor control server and a response from the floor control server to the client. The request carries a Transaction ID in its common header, which the floor control server copies into the response. Clients use Transaction ID values to match responses with previously issued requests.

Server-initiated transactions consist of a single message from a floor control server to a client. Since they do not trigger any response, their Transaction ID is set to 0 when used over reliable transports, but must be non-zero and unique in the context of outstanding transactions over unreliable transports.

When using BFCP over unreliable transports, all requests will use retransmit timer T1 (see Section 8.3) until the transaction is completed.

8.1. Client Behavior

A client starting a client-initiated transaction MUST set the Conference ID in the common header of the message to the Conference ID for the conference that the client obtained previously.

The client MUST set the Transaction ID value in the common header to a number that is different from 0 and that MUST NOT be reused in another message from the client until a response from the server is received for the transaction. The client uses the Transaction ID value to match this message with the response from the floor control server.

8.2. Server Behavior

A floor control server sending a response within a client-initiated transaction MUST copy the Conference ID, the Transaction ID, and the User ID from the request received from the client into the response.

Server-initiated transactions MUST contain a Transaction ID equal to 0 when BFCP is used over reliable transports. Over unreliable transport, the Transaction ID shall have the same properties as for client-initiated transactions: the server MUST set the Transaction ID value in the common header to a number that is different from 0 and that MUST NOT be reused in another message from the server until the appropriate response from the client is received for the transaction. The server uses the Transaction ID value to match this message with the response from the floor participant or floor chair.

8.3. Timers

When BFCP entities are communicating over an unreliable transport, two retransmission timers are employed to help mitigate against loss of datagrams. Retransmission and response caching are not required when BFCP entities communicate over reliable transports.

8.3.1. Request Retransmission Timer, T1

T1 is a timer that schedules retransmission of a request until an appropriate response is received or until the maximum number of retransmissions have occurred. The timer doubles on each re-transmit, failing after three unacknowledged retransmission attempts.

If a valid response is not received for a client- or server-initiated transaction, the implementation MUST consider the BFCP association as failed. Implementations SHOULD follow the reestablishment procedure described in section 6 (e.g. initiate a new offer/answer [12] exchange). Alternatively, they MAY continue without BFCP and therefore not be participant in any floor control actions.

8.3.2. Response Retransmission Timer, T2

T2 is a timer that, when fires, signals that the BFCP entity can release knowledge of the transaction against which it is running. It is started upon the first transmission of the response to a request and is the only mechanism by which that response is released by the BFCP entity. Any subsequent retransmissions of the same request can be responded to by replaying the cached response, whilst that value is retained until the timer has fired.

T2 shall be set such that it encompasses all legal retransmissions per T1 plus a factor to accommodate network latency between BFCP entities.

8.3.3. Timer Values

The table below defines the different timers required when BFCP entities communicate over an unreliable transport.

Timer	Description	Value/s
T1	Initial request retransmission timer	0.5s
T2	Response retransmission timer	10s

Table 6: Timers

The default value for T1 is 500 ms, this is an estimate of the RTT for completing the transaction. T1 MAY be chosen larger, and this is RECOMMENDED if it is known in advance that the RTT is larger. Regardless of the value of T1, the exponential backoffs on retransmissions described in Section 8.3.1 MUST be used.

9. Authentication and Authorization

BFCP clients SHOULD authenticate the floor control server before sending any BFCP message to it or accepting any BFCP message from it. Similarly, floor control servers SHOULD authenticate a client before accepting any BFCP message from it or sending any BFCP message to it.

BFCP supports TLS/DTLS mutual authentication between clients and floor control servers, as specified in Section 9.1. This is the RECOMMENDED authentication mechanism in BFCP.

Note that future extensions may define additional authentication mechanisms.

In addition to authenticating BFCP messages, floor control servers need to authorize them. On receiving an authenticated BFCP message, the floor control server checks whether the client sending the message is authorized. If the client is not authorized to perform the operation being requested, the floor control server generates an Error message, as described in Section 13.8, with an Error code with a value of 5 (Unauthorized Operation). Messages from a client that cannot be authorized MUST NOT be processed further.

9.1. TLS/DTLS Based Mutual Authentication

BFCP supports TLS/DTLS based mutual authentication between clients and floor control servers. BFCP assumes that there is an integrity-

protected channel between the client and the floor control server that can be used to exchange their self-signed certificates or, more commonly, the fingerprints of these certificates. These certificates are used at TLS/DTLS establishment time.

> The implementation of such an integrity-protected channel using SIP and the SDP offer/answer model is described in [7].

BFCP messages received over an authenticated TLS/DTLS connection are considered authenticated. A floor control server that receives a BFCP message over TCP/UDP (no TLS/DTLS) can request the use of TLS/DTLS by generating an Error message, as described in Section 13.8, with an Error code with a value of 9 (Use TLS) or a value of 11 (Use DTLS) respectively. Clients SHOULD simply ignore unauthenticated messages.

Note that future extensions may define additional authentication mechanisms that may not require an initial integrity-protected channel (e.g., authentication based on certificates signed by a certificate authority).

As described in Section 9, floor control servers need to perform authorization before processing any message. In particular, the floor control server SHOULD check that messages arriving over a given authenticated TLS/DTLS connection use an authorized User ID (i.e., a User ID that the user that established the authenticated TLS/DTLS connection is allowed to use).

10. Floor Participant Operations

This section specifies how floor participants can perform different operations, such as requesting a floor, using the protocol elements described in earlier sections. Section 11 specifies operations that are specific to floor chairs, such as instructing the floor control server to grant or revoke a floor, and Section 12 specifies operations that can be performed by any client (i.e., both floor participants and floor chairs).

10.1. Requesting a Floor

A floor participant that wishes to request one or more floors does so by sending a FloorRequest message to the floor control server.

10.1.1. Sending a FloorRequest Message

The ABNF in Section 5.3.1 describes the attributes that a FloorRequest message can contain. In addition, the ABNF specifies

normatively which of these attributes are mandatory, and which ones are optional.

The floor participant sets the Conference ID and the Transaction ID in the common header following the rules given in Section 8.1.

The floor participant sets the User ID in the common header to the floor participant's identifier. This User ID will be used by the floor control server to authenticate and authorize the request. If the sender of the FloorRequest message (identified by the User ID) is not the participant that would eventually get the floor (i.e., a third-party floor request), the sender SHOULD add a BENEFICIARY-ID attribute to the message identifying the beneficiary of the floor.

> Note that the name space for both the User ID and the Beneficiary ID is the same. That is, a given participant is identified by a single 16-bit value that can be used in the User ID in the common header and in several attributes: BENEFICIARY-ID, BENEFICIARY-INFORMATION, and REQUESTED-BY-INFORMATION.

The floor participant must insert at least one FLOOR-ID attribute in the FloorRequest message. If the client inserts more than one FLOOR-ID attribute, the floor control server will treat all the floor requests as an atomic package. That is, the floor control server will either grant or deny all the floors in the FloorRequest message.

The floor participant may use a PARTICIPANT-PROVIDED-INFO attribute to state the reason why the floor or floors are being requested. The Text field in the PARTICIPANT-PROVIDED-INFO attribute is intended for human consumption.

The floor participant may request that the server handle the floor request with a certain priority using a PRIORITY attribute.

10.1.2. Receiving a Response

A message from the floor control server is considered a response to the FloorRequest message if the message from the floor control server has the same Conference ID, Transaction ID, and User ID as the FloorRequest message, as described in Section 8.1. On receiving such a response, the floor participant follows the rules in Section 9 that relate to floor control server authentication.

The successful processing of a FloorRequest message at the floor control server involves generating one or several FloorRequestStatus messages. The floor participant obtains a Floor Request ID in the Floor Request ID field of a FLOOR-REQUEST-INFORMATION attribute in the first FloorRequestStatus message from the floor control server.

Subsequent FloorRequestStatus messages from the floor control server regarding the same floor request will carry the same Floor Request ID in a FLOOR-REQUEST-INFORMATION attribute as the initial FloorRequestStatus message. This way, the floor participant can associate subsequent incoming FloorRequestStatus messages with the ongoing floor request.

The floor participant obtains information about the status of the floor request in the FLOOR-REQUEST-INFORMATION attribute of each of the FloorRequestStatus messages received from the floor control server. This attribute is a grouped attribute, and as such it includes a number of attributes that provide information about the floor request.

The OVERALL-REQUEST-STATUS attribute provides information about the overall status of the floor request. If the Request Status value is Granted, all the floors that were requested in the FloorRequest message have been granted. If the Request Status value is Denied, all the floors that were requested in the FloorRequest message have been denied. A floor request is considered to be ongoing while it is in the Pending, Accepted, or Granted states. If the floor request value is unknown, then the response is still processed. However, no meaningful value can be reported to the user.

The STATUS-INFO attribute, if present, provides extra information that the floor participant MAY display to the user.

The FLOOR-REQUEST-STATUS attributes provide information about the status of the floor request as it relates to a particular floor. The STATUS-INFO attribute, if present, provides extra information that the floor participant MAY display to the user.

The BENEFICIARY-INFORMATION attribute identifies the beneficiary of the floor request in third-party floor requests. The REQUESTED-BY-INFORMATION attribute need not be present in FloorRequestStatus messages received by the floor participant that requested the floor, as this floor participant is already identified by the User ID in the common header.

The PRIORITY attribute, when present, contains the priority that was requested by the generator of the FloorRequest message.

If the response is an Error message, the floor control server could not process the FloorRequest message for some reason, which is described in the Error message.

10.1.3. Reception of a Subsequent FloorRequestStatus Message

When communicating over unreliable transport and upon receiving a FloorRequestStatus message from a floor control server, the participant MUST respond with a FloorRequestStatusAck message within the transaction failure window to complete the transaction.

10.2. Cancelling a Floor Request and Releasing a Floor

A floor participant that wishes to cancel an ongoing floor request does so by sending a FloorRelease message to the floor control server. The FloorRelease message is also used by floor participants that hold a floor and would like to release it.

10.2.1. Sending a FloorRelease Message

The ABNF in Section 5.3.2 describes the attributes that a FloorRelease message can contain. In addition, the ABNF specifies normatively which of these attributes are mandatory, and which ones are optional.

The floor participant sets the Conference ID and the Transaction ID in the common header following the rules given in Section 8.1. The floor participant sets the User ID in the common header to the floor participant's identifier. This User ID will be used by the floor control server to authenticate and authorize the request.

> Note that the FloorRelease message is used to release a floor or floors that were granted and to cancel ongoing floor requests (from the protocol perspective, both are ongoing floor requests). Using the same message in both situations helps resolve the race condition that occurs when the FloorRelease message and the FloorGrant message cross each other on the wire.

The floor participant uses the FLOOR-REQUEST-ID that was received in the response to the FloorRequest message that the FloorRelease message is cancelling.

> Note that if the floor participant requested several floors as an atomic operation (i.e., in a single FloorRequest message), all the floors are released as an atomic operation as well (i.e., all are released at the same time).

10.2.2. Receiving a Response

A message from the floor control server is considered a response to the FloorRelease message if the message from the floor control server has the same Conference ID, Transaction ID, and User ID as the

FloorRequest message, as described in Section 8.1. On receiving such a response, the floor participant follows the rules in Section 9 that relate to floor control server authentication.

If the response is a FloorRequestStatus message, the Request Status value in the OVERALL-REQUEST-STATUS attribute (within the FLOOR-REQUEST-INFORMATION grouped attribute) will be Cancelled or Released.

If the response is an Error message, the floor control server could not process the FloorRequest message for some reason, which is described in the Error message.

It is possible that the FloorRelease message crosses on the wire with a FloorRequestStatus message from the server with a Request Status different from Cancelled or Released. In any case, such a FloorRequestStatus message will not be a response to the FloorRelease message, as its Transaction ID will not match that of the FloorRelease.

11. Chair Operations

This section specifies how floor chairs can instruct the floor control server to grant or revoke a floor using the protocol elements described in earlier sections.

Floor chairs that wish to send instructions to a floor control server do so by sending a ChairAction message.

11.1. Sending a ChairAction Message

The ABNF in Section 5.3.9 describes the attributes that a ChairAction message can contain. In addition, the ABNF specifies normatively which of these attributes are mandatory, and which ones are optional.

The floor chair sets the Conference ID and the Transaction ID in the common header following the rules given in Section 8.1. The floor chair sets the User ID in the common header to the floor chair's identifier. This User ID will be used by the floor control server to authenticate and authorize the request.

The ChairAction message contains instructions that apply to one or more floors within a particular floor request. The floor or floors are identified by the FLOOR-REQUEST-STATUS attributes and the floor request is identified by the FLOOR-REQUEST-INFORMATION-HEADER, which are carried in the ChairAction message.

For example, if a floor request consists of two floors that depend on

different floor chairs, each floor chair will grant its floor within the floor request. Once both chairs have granted their floor, the floor control server will grant the floor request as a whole. On the other hand, if one of the floor chairs denies its floor, the floor control server will deny the floor request as a whole, regardless of the other floor chair's decision.

The floor chair provides the new status of the floor request as it relates to a particular floor using a FLOOR-REQUEST-STATUS attribute. If the new status of the floor request is Accepted, the floor chair MAY use the Queue Position field to provide a queue position for the floor request. If the floor chair does not wish to provide a queue position, all the bits of the Queue Position field SHOULD be set to zero. The floor chair SHOULD use the Status Revoked to revoke a floor that was granted (i.e., Granted status) and SHOULD use the Status Denied to reject floor requests in any other status (e.g., Pending and Accepted).

The floor chair MAY add an OVERALL-REQUEST-STATUS attribute to the ChairAction message to provide a new overall status for the floor request. If the new overall status of the floor request is Accepted, the floor chair MAY use the Queue Position field to provide a queue position for the floor request.

> Note that a particular floor control server may implement a different queue for each floor containing all the floor requests that relate to that particular floor, a general queue for all floor requests, or both. Also note that a floor request may involve several floors and that a ChairAction message may only deal with a subset of these floors (e.g., if a single floor chair is not authorized to manage all the floors). In this case, the floor control server will combine the instructions received from the different floor chairs in FLOOR-REQUEST-STATUS attributes to come up with the overall status of the floor request.
>
> Note that, while the action of a floor chair may communicate information in the OVERALL-REQUEST-STATUS attribute, the floor control server may override, modify, or ignore this field's content.

The floor chair may use STATUS-INFO attributes to state the reason why the floor or floors are being accepted, granted, or revoked. The Text in the STATUS-INFO attribute is intended for human consumption.

11.2. Receiving a Response

A message from the floor control server is considered a response to the ChairAction message if the message from the server has the same

Conference ID, Transaction ID, and User ID as the ChairAction message, as described in Section 8.1. On receiving such a response, the floor chair follows the rules in Section 9 that relate to floor control server authentication.

A ChairActionAck message from the floor control server confirms that the floor control server has accepted the ChairAction message. An Error message indicates that the floor control server could not process the ChairAction message for some reason, which is described in the Error message.

12. General Client Operations

This section specifies operations that can be performed by any client. That is, they are not specific to floor participants or floor chairs. They can be performed by both.

12.1. Requesting Information about Floors

A client can obtain information about the status of a floor or floors in different ways, which include using BFCP and using out-of-band mechanisms. Clients using BFCP to obtain such information use the procedures described in this section.

Clients request information about the status of one or several floors by sending a FloorQuery message to the floor control server.

12.1.1. Sending a FloorQuery Message

The ABNF in Section 5.3.7 describes the attributes that a FloorQuery message can contain. In addition, the ABNF specifies normatively which of these attributes are mandatory, and which ones are optional.

The client sets the Conference ID and the Transaction ID in the common header following the rules given in Section 8.1. The client sets the User ID in the common header to the client's identifier. This User ID will be used by the floor control server to authenticate and authorize the request.

The client inserts in the message all the Floor IDs it wants to receive information about. The floor control server will send periodic information about all of these floors. If the client does not want to receive information about a particular floor any longer, it sends a new FloorQuery message removing the FLOOR-ID of this floor. If the client does not want to receive information about any floor any longer, it sends a FloorQuery message with no FLOOR-ID attribute.

12.1.2. Receiving a Response

A message from the floor control server is considered a response to the FloorQuery message if the message from the floor control server has the same Conference ID, Transaction ID, and User ID as the FloorRequest message, as described in Section 8.1. On receiving such a response, the client follows the rules in Section 9 that relate to floor control server authentication.

On reception of the FloorQuery message, the floor control server will respond with a FloorStatus message or with an Error message. If the response is a FloorStatus message, it will contain information about one of the floors the client requested information about. If the client did not include any FLOOR-ID attribute in its FloorQuery message (i.e., the client does not want to receive information about any floor any longer), the FloorStatus message from the floor control server will not include any FLOOR-ID attribute either.

FloorStatus messages that carry information about a floor contain a FLOOR-ID attribute that identifies the floor. After this attribute, FloorStatus messages contain information about existing (one or more) floor requests that relate to that floor. The information about each particular floor request is encoded in a FLOOR-REQUEST-INFORMATION attribute. This grouped attribute carries a Floor Request ID that identifies the floor request, followed by a set of attributes that provide information about the floor request.

After the first FloorStatus, the floor control server will continue sending FloorStatus messages, periodically informing the client about changes on the floors the client requested information about.

12.1.3. Reception of a Subsequent FloorStatus Message

When communicating over unreliable transport and upon receiving a FloorStatus message from a floor control server, the participant MUST respond with a FloorStatusAck message within the transaction failure window to complete the transaction.

12.2. Requesting Information about Floor Requests

A client can obtain information about the status of one or several floor requests in different ways, which include using BFCP and using out-of-band mechanisms. Clients using BFCP to obtain such information use the procedures described in this section.

Clients request information about the current status of a floor request by sending a FloorRequestQuery message to the floor control server.

Requesting information about a particular floor request is useful in a number of situations. For example, on reception of a FloorRequest message, a floor control server may choose to return FloorRequestStatus messages only when the floor request changes its state (e.g., from Accepted to Granted), but not when the floor request advances in its queue. In this situation, if the user requests it, the floor participant can use a FloorRequestQuery message to poll the floor control server for the status of the floor request.

12.2.1. Sending a FloorRequestQuery Message

The ABNF in Section 5.3.3 describes the attributes that a FloorRequestQuery message can contain. In addition, the ABNF specifies normatively which of these attributes are mandatory, and which ones are optional.

The client sets the Conference ID and the Transaction ID in the common header following the rules given in Section 8.1. The client sets the User ID in the common header to the client's identifier. This User ID will be used by the floor control server to authenticate and authorize the request.

The client must insert a FLOOR-REQUEST-ID attribute that identifies the floor request at the floor control server.

12.2.2. Receiving a Response

A message from the floor control server is considered a response to the FloorRequestQuery message if the message from the floor control server has the same Conference ID, Transaction ID, and User ID as the FloorRequestQuery message, as described in Section 8.1. On receiving such a response, the client follows the rules in Section 9 that relate to floor control server authentication.

If the response is a FloorRequestStatus message, the client obtains information about the status of the FloorRequest the client requested information about in a FLOOR-REQUEST-INFORMATION attribute.

If the response is an Error message, the floor control server could not process the FloorRequestQuery message for some reason, which is described in the Error message.

12.3. Requesting Information about a User

A client can obtain information about a participant and the floor requests related to this participant in different ways, which include using BFCP and using out-of-band mechanisms. Clients using BFCP to

obtain such information use the procedures described in this section.

Clients request information about a participant and the floor requests related to this participant by sending a UserQuery message to the floor control server.

This functionality may be useful for floor chairs or floor participants interested in the display name and the URI of a particular floor participant. In addition, a floor participant may find it useful to request information about itself. For example, a floor participant, after experiencing connectivity problems (e.g., its TCP connection with the floor control server was down for a while and eventually was re-established), may need to request information about all the floor requests associated to itself that still exist.

12.3.1. Sending a UserQuery Message

The ABNF in Section 5.3.5 describes the attributes that a UserQuery message can contain. In addition, the ABNF specifies normatively which of these attributes are mandatory, and which ones are optional.

The client sets the Conference ID and the Transaction ID in the common header following the rules given in Section 8.1. The client sets the User ID in the common header to the client's identifier. This User ID will be used by the floor control server to authenticate and authorize the request.

If the floor participant the client is requesting information about is not the client issuing the UserQuery message (which is identified by the User ID in the common header of the message), the client MUST insert a BENEFICIARY-ID attribute.

12.3.2. Receiving a Response

A message from the floor control server is considered a response to the UserQuery message if the message from the floor control server has the same Conference ID, Transaction ID, and User ID as the UserQuery message, as described in Section 8.1. On receiving such a response, the client follows the rules in Section 9 that relate to floor control server authentication.

If the response is a UserStatus message, the client obtains information about the floor participant in a BENEFICIARY-INFORMATION grouped attribute and about the status of the floor requests associated with the floor participant in FLOOR-REQUEST-INFORMATION attributes.

If the response is an Error message, the floor control server could

not process the UserQuery message for some reason, which is described in the Error message.

12.4. Obtaining the Capabilities of a Floor Control Server

A client that wishes to obtain the capabilities of a floor control server does so by sending a Hello message to the floor control server.

12.4.1. Sending a Hello Message

The ABNF in Section 5.3.11 describes the attributes that a Hello message can contain. In addition, the ABNF specifies normatively which of these attributes are mandatory, and which ones are optional.

The client sets the Conference ID and the Transaction ID in the common header following the rules given in Section 8.1. The client sets the User ID in the common header to the client's identifier. This User ID will be used by the floor control server to authenticate and authorize the request.

12.4.2. Receiving Responses

A message from the floor control server is considered a response to the Hello message by the client if the message from the floor control server has the same Conference ID, Transaction ID, and User ID as the Hello message, as described in Section 8.1. On receiving such a response, the client follows the rules in Section 9 that relate to floor control server authentication.

If the response is a HelloAck message, the floor control server could process the Hello message successfully. The SUPPORTED-PRIMITIVES and SUPPORTED-ATTRIBUTES attributes indicate which primitives and attributes, respectively, are supported by the server.

If the response is an Error message, the floor control server could not process the Hello message for some reason, which is described in the Error message.

13. Floor Control Server Operations

This section specifies how floor control servers can perform different operations, such as granting a floor, using the protocol elements described in earlier sections.

On reception of a message from a client, the floor control server MUST check whether the value of the Primitive is supported. If it is

not, the floor control server SHOULD send an Error message, as described in Section 13.8, with Error code 3 (Unknown Primitive).

On reception of a message from a client, the floor control server MUST check whether the value of the Conference ID matched an existing conference. If it does not, the floor control server SHOULD send an Error message, as described in Section 13.8, with Error code 1 (Conference does not Exist).

On reception of a message from a client, the floor control server follows the rules in Section 9 that relate to the authentication of the message.

On reception of a message from a client, the floor control server MUST check whether it understands all the mandatory ('M' bit set) attributes in the message. If the floor control server does not understand all of them, the floor control server SHOULD send an Error message, as described in Section 13.8, with Error code 4 (Unknown Mandatory Attribute). The Error message SHOULD list the attributes that were not understood.

13.1. Reception of a FloorRequest Message

On reception of a FloorRequest message, the floor control server follows the rules in Section 9 that relate to client authentication and authorization. If while processing the FloorRequest message, the floor control server encounters an error, it SHOULD generate an Error response following the procedures described in Section 13.8.

> BFCP allows floor participants to have several ongoing floor requests for the same floor (e.g., the same floor participant can occupy more than one position in a queue at the same time). A floor control server that only supports a certain number of ongoing floor requests per floor participant (e.g., one) can use Error Code 8 (You have Already Reached the Maximum Number of Ongoing Floor Requests for this Floor) to inform the floor participant.

When communicating over unreliable transport and upon receiving a FloorRequest from a participant, the floor control server MUST respond with a FloorRequestStatus message within the transaction failure window to complete the transaction.

13.1.1. Generating the First FloorRequestStatus Message

The successful processing of a FloorRequest message by a floor control server involves generating one or several FloorRequestStatus messages, the first of which SHOULD be generated as soon as possible.

If the floor control server cannot accept, grant, or deny the floor request right away (e.g., a decision from a chair is needed), it SHOULD use a Request Status value of Pending in the OVERALL-REQUEST-STATUS attribute (within the FLOOR-REQUEST-INFORMATION grouped attribute) of the first FloorRequestStatus message it generates.

> The policy that a floor control server follows to grant or deny floors is outside the scope of this document. A given floor control server may perform these decisions automatically while another may contact a human acting as a chair every time a decision needs to be made.

The floor control server MUST copy the Conference ID, the Transaction ID, and the User ID from the FloorRequest into the FloorRequestStatus, as described in Section 8.2. Additionally, the floor control server MUST add a FLOOR-REQUEST-INFORMATION grouped attribute to the FloorRequestStatus. The attributes contained in this grouped attribute carry information about the floor request.

The floor control server MUST assign an identifier that is unique within the conference to this floor request, and MUST insert it in the Floor Request ID field of the FLOOR-REQUEST-INFORMATION attribute. This identifier will be used by the floor participant (or by a chair or chairs) to refer to this specific floor request in the future.

The floor control server MUST copy the Floor IDs in the FLOOR-ID attributes of the FloorRequest into the FLOOR-REQUEST-STATUS attributes in the FLOOR-REQUEST-INFORMATION grouped attribute. These Floor IDs identify the floors being requested (i.e., the floors associated with this particular floor request).

The floor control server SHOULD copy (if present) the contents of the BENEFICIARY-ID attribute from the FloorRequest into a BENEFICIARY-INFORMATION attribute inside the FLOOR-REQUEST-INFORMATION grouped attribute. Additionally, the floor control server MAY provide the display name and the URI of the beneficiary in this BENEFICIARY-INFORMATION attribute.

The floor control server MAY provide information about the requester of the floor in a REQUESTED-BY-INFORMATION attribute inside the FLOOR-REQUEST-INFORMATION grouped attribute.

The floor control server MAY copy (if present) the PRIORITY attribute from the FloorRequest into the FLOOR-REQUEST-INFORMATION grouped attribute.

Note that this attribute carries the priority requested by the participant. The priority that the floor control server assigns to the floor request depends on the priority requested by the participant and the rights the participant has according to the policy of the conference. For example, a participant that is only allowed to use the Normal priority may request Highest priority for a floor request. In that case, the floor control server would ignore the priority requested by the participant.

The floor control server MAY copy (if present) the PARTICIPANT-PROVIDED-INFO attribute from the FloorRequest into the FLOOR-REQUEST-INFORMATION grouped attribute.

13.1.2. Generation of Subsequent FloorRequestStatus Messages

A floor request is considered to be ongoing as long as it is not in the Cancelled, Released, or Revoked states. If the OVERALL-REQUEST-STATUS attribute (inside the FLOOR-REQUEST-INFORMATION grouped attribute) of the first FloorRequestStatus message generated by the floor control server did not indicate any of these states, the floor control server will need to send subsequent FloorRequestStatus messages.

When the status of the floor request changes, the floor control server SHOULD send new FloorRequestStatus messages with the appropriate Request Status. The floor control server MUST add a FLOOR-REQUEST-INFORMATION attribute with a Floor Request ID equal to the one sent in the first FloorRequestStatus message to any new FloorRequestStatus related to the same floor request. (The Floor Request ID identifies the floor request to which the FloorRequestStatus applies.)

When using BFCP over reliable transports, the floor control server MUST set the Transaction ID of subsequent FloorRequestStatus messages to 0. When using BFCP over unreliable transports, the Transaction ID MUST be non-zero and unique in the context of outstanding transactions over unreliable transports as described in Section 8.

The rate at which the floor control server sends FloorRequestStatus messages is a matter of local policy. A floor control server may choose to send a new FloorRequestStatus message every time the floor request moves in the floor request queue, while another may choose only to send a new FloorRequestStatus message when the floor request is Granted or Denied.

The floor control server may add a STATUS-INFO attribute to any of the FloorRequestStatus messages it generates to provide extra information about its decisions regarding the floor request (e.g.,

why it was denied).

Floor participants and floor chairs may request to be informed about the status of a floor following the procedures in Section 12.1. If the processing of a floor request changes the status of a floor (e.g., the floor request is granted and consequently the floor has a new holder), the floor control server needs to follow the procedures in Section 13.5 to inform the clients that have requested that information.

The common header and the rest of the attributes are the same as in the first FloorRequestStatus message.

The floor control server can discard the state information about a particular floor request when this reaches a status of Cancelled, Released, or Revoked.

When communicating over unreliable transport and a FloorRequestStatusAck message is not received within the transaction failure window, the floor control server MUST retransmit the FloorRequestStatus message according to Section 6.2.

13.2. Reception of a FloorRequestQuery Message

On reception of a FloorRequestQuery message, the floor control server follows the rules in Section 9 that relate to client authentication and authorization. If while processing the FloorRequestQuery message, the floor control server encounters an error, it SHOULD generate an Error response following the procedures described in Section 13.8.

The successful processing of a FloorRequestQuery message by a floor control server involves generating a FloorRequestStatus message, which SHOULD be generated as soon as possible.

When communicating over unreliable transport and upon receiving a FloorRequestQuery from a participant, the floor control server MUST respond with a FloorRequestStatus message within the transaction failure window to complete the transaction.

The floor control server MUST copy the Conference ID, the Transaction ID, and the User ID from the FloorRequestQuery message into the FloorRequestStatus message, as described in Section 8.2. Additionally, the floor control server MUST include information about the floor request in the FLOOR-REQUEST-INFORMATION grouped attribute to the FloorRequestStatus.

The floor control server MUST copy the contents of the

FLOOR-REQUEST-ID attribute from the FloorRequestQuery message into the Floor Request ID field of the FLOOR-REQUEST-INFORMATION attribute.

The floor control server MUST add FLOOR-REQUEST-STATUS attributes to the FLOOR-REQUEST-INFORMATION grouped attribute identifying the floors being requested (i.e., the floors associated with the floor request identified by the FLOOR-REQUEST-ID attribute).

The floor control server SHOULD add a BENEFICIARY-ID attribute to the FLOOR-REQUEST-INFORMATION grouped attribute identifying the beneficiary of the floor request. Additionally, the floor control server MAY provide the display name and the URI of the beneficiary in this BENEFICIARY-INFORMATION attribute.

The floor control server MAY provide information about the requester of the floor in a REQUESTED-BY-INFORMATION attribute inside the FLOOR-REQUEST-INFORMATION grouped attribute.

The floor control server MAY provide the reason why the floor participant requested the floor in a PARTICIPANT-PROVIDED-INFO.

The floor control server MAY also add to the FLOOR-REQUEST-INFORMATION grouped attribute a PRIORITY attribute with the Priority value requested for the floor request and a STATUS-INFO attribute with extra information about the floor request.

The floor control server MUST add an OVERALL-REQUEST-STATUS attribute to the FLOOR-REQUEST-INFORMATION grouped attribute with the current status of the floor request. The floor control server MAY provide information about the status of the floor request as it relates to each of the floors being requested in the FLOOR-REQUEST-STATUS attributes.

13.3. Reception of a UserQuery Message

On reception of a UserQuery message, the floor control server follows the rules in Section 9 that relate to client authentication and authorization. If while processing the UserQuery message, the floor control server encounters an error, it SHOULD generate an Error response following the procedures described in Section 13.8.

The successful processing of a UserQuery message by a floor control server involves generating a UserStatus message, which SHOULD be generated as soon as possible.

When communicating over unreliable transport and upon receiving a UserQuery from a participant, the floor control server MUST respond

with a UserStatus message within the transaction failure window to complete the transaction.

The floor control server MUST copy the Conference ID, the Transaction ID, and the User ID from the UserQuery message into the USerStatus message, as described in Section 8.2.

The sender of the UserQuery message is requesting information about all the floor requests associated with a given participant (i.e., the floor requests where the participant is either the beneficiary or the requester). This participant is identified by a BENEFICIARY-ID attribute or, in the absence of a BENEFICIARY-ID attribute, by a the User ID in the common header of the UserQuery message.

The floor control server MUST copy, if present, the contents of the BENEFICIARY-ID attribute from the UserQuery message into a BENEFICIARY-INFORMATION attribute in the UserStatus message. Additionally, the floor control server MAY provide the display name and the URI of the participant about which the UserStatus message provides information in this BENEFICIARY-INFORMATION attribute.

The floor control server SHOULD add to the UserStatus message a FLOOR-REQUEST-INFORMATION grouped attribute for each floor request related to the participant about which the message provides information (i.e., the floor requests where the participant is either the beneficiary or the requester). For each FLOOR-REQUEST-INFORMATION attribute, the floor control server follows the following steps.

The floor control server MUST identify the floor request the FLOOR-REQUEST-INFORMATION attribute applies to by filling the Floor Request ID field of the FLOOR-REQUEST-INFORMATION attribute.

The floor control server MUST add FLOOR-REQUEST-STATUS attributes to the FLOOR-REQUEST-INFORMATION grouped attribute identifying the floors being requested (i.e., the floors associated with the floor request identified by the FLOOR-REQUEST-ID attribute).

The floor control server SHOULD add a BENEFICIARY-ID attribute to the FLOOR-REQUEST-INFORMATION grouped attribute identifying the beneficiary of the floor request. Additionally, the floor control server MAY provide the display name and the URI of the beneficiary in this BENEFICIARY-INFORMATION attribute.

The floor control server MAY provide information about the requester of the floor in a REQUESTED-BY-INFORMATION attribute inside the FLOOR-REQUEST-INFORMATION grouped attribute.

The floor control server MAY provide the reason why the floor participant requested the floor in a PARTICIPANT-PROVIDED-INFO.

The floor control server MAY also add to the FLOOR-REQUEST-INFORMATION grouped attribute a PRIORITY attribute with the Priority value requested for the floor request.

The floor control server MUST include the current status of the floor request in an OVERALL-REQUEST-STATUS attribute to the FLOOR-REQUEST-INFORMATION grouped attribute. The floor control server MAY add a STATUS-INFO attribute with extra information about the floor request.

The floor control server MAY provide information about the status of the floor request as it relates to each of the floors being requested in the FLOOR-REQUEST-STATUS attributes.

13.4. Reception of a FloorRelease Message

On reception of a FloorRelease message, the floor control server follows the rules in Section 9 that relate to client authentication and authorization. If while processing the FloorRelease message, the floor control server encounters an error, it SHOULD generate an Error response following the procedures described in Section 13.8.

The successful processing of a FloorRelease message by a floor control server involves generating a FloorRequestStatus message, which SHOULD be generated as soon as possible.

When communicating over unreliable transport and upon receiving a FloorRelease from a participant, the floor control server MUST respond with a FloorRequestStatus message within the transaction failure window to complete the transaction.

The floor control server MUST copy the Conference ID, the Transaction ID, and the User ID from the FloorRelease message into the FloorRequestStatus message, as described in Section 8.2.

The floor control server MUST add a FLOOR-REQUEST-INFORMATION grouped attribute to the FloorRequestStatus. The attributes contained in this grouped attribute carry information about the floor request.

The FloorRelease message identifies the floor request it applies to using a FLOOR-REQUEST-ID. The floor control server MUST copy the contents of the FLOOR-REQUEST-ID attribute from the FloorRelease message into the Floor Request ID field of the FLOOR-REQUEST-INFORMATION attribute.

The floor control server MUST identify the floors being released

(i.e., the floors associated with the floor request identified by the FLOOR-REQUEST-ID attribute) in FLOOR-REQUEST-STATUS attributes to the FLOOR-REQUEST-INFORMATION grouped attribute.

The floor control server MUST add an OVERALL-REQUEST-STATUS attribute to the FLOOR-REQUEST-INFORMATION grouped attribute. The Request Status value SHOULD be Released, if the floor (or floors) had been previously granted, or Cancelled, if the floor (or floors) had not been previously granted. The floor control server MAY add a STATUS-INFO attribute with extra information about the floor request.

13.5. Reception of a FloorQuery Message

On reception of a FloorQuery message, the floor control server follows the rules in Section 9 that relate to client authentication. If while processing the FloorQuery message, the floor control server encounters an error, it SHOULD generate an Error response following the procedures described in Section 13.8.

When communicating over unreliable transport and upon receiving a FloorQuery from a participant, the floor control server MUST respond with a FloorStatus message within the transaction failure window to complete the transaction.

A floor control server receiving a FloorQuery message from a client SHOULD keep this client informed about the status of the floors identified by FLOOR-ID attributes in the FloorQuery message. Floor Control Servers keep clients informed by using FloorStatus messages.

An individual FloorStatus message carries information about a single floor. So, when a FloorQuery message requests information about more than one floor, the floor control server needs to send separate FloorStatus messages for different floors.

The information FloorQuery messages carry may depend on the user requesting the information. For example, a chair may be able to receive information about pending requests, while a regular user may not be authorized to do so.

13.5.1. Generation of the First FloorStatus Message

The successful processing of a FloorQuery message by a floor control server involves generating one or several FloorStatus messages, the first of which SHOULD be generated as soon as possible.

The floor control server MUST copy the Conference ID, the Transaction ID, and the User ID from the FloorQuery message into the FloorStatus message, as described in Section 8.2.

If the FloorQuery message did not contain any FLOOR-ID attribute, the floor control server sends the FloorStatus message without adding any additional attribute and does not send any subsequent FloorStatus message to the floor participant.

If the FloorQuery message contained one or more FLOOR-ID attributes, the floor control server chooses one from among them and adds this FLOOR-ID attribute to the FloorStatus message. The floor control server SHOULD add a FLOOR-REQUEST-INFORMATION grouped attribute for each floor request associated to the floor. Each FLOOR-REQUEST-INFORMATION grouped attribute contains a number of attributes that provide information about the floor request. For each FLOOR-REQUEST-INFORMATION attribute, the floor control server follows the following steps.

The floor control server MUST identify the floor request the FLOOR-REQUEST-INFORMATION attribute applies to by filling the Floor Request ID field of the FLOOR-REQUEST-INFORMATION attribute.

The floor control server MUST add FLOOR-REQUEST-STATUS attributes to the FLOOR-REQUEST-INFORMATION grouped attribute identifying the floors being requested (i.e., the floors associated with the floor request identified by the FLOOR-REQUEST-ID attribute).

The floor control server SHOULD add a BENEFICIARY-ID attribute to the FLOOR-REQUEST-INFORMATION grouped attribute identifying the beneficiary of the floor request. Additionally, the floor control server MAY provide the display name and the URI of the beneficiary in this BENEFICIARY-INFORMATION attribute.

The floor control server MAY provide information about the requester of the floor in a REQUESTED-BY-INFORMATION attribute inside the FLOOR-REQUEST-INFORMATION grouped attribute.

The floor control server MAY provide the reason why the floor participant requested the floor in a PARTICIPANT-PROVIDED-INFO.

The floor control server MAY also add to the FLOOR-REQUEST-INFORMATION grouped attribute a PRIORITY attribute with the Priority value requested for the floor request.

The floor control server MUST add an OVERALL-REQUEST-STATUS attribute to the FLOOR-REQUEST-INFORMATION grouped attribute with the current status of the floor request. The floor control server MAY add a STATUS-INFO attribute with extra information about the floor request.

The floor control server MAY provide information about the status of the floor request as it relates to each of the floors being requested

in the FLOOR-REQUEST-STATUS attributes.

13.5.2. Generation of Subsequent FloorStatus Messages

If the FloorQuery message carried more than one FLOOR-ID attribute, the floor control server SHOULD generate a FloorStatus message for each of them (except for the FLOOR-ID attribute chosen for the first FloorStatus message) as soon as possible. These FloorStatus messages are generated following the same rules as those for the first FloorStatus message (see Section 13.5.1), but their Transaction ID is 0 when using reliable transports and non-zero and unique in the context of outstanding transactions when using unreliable transports (cf. Section 8).

After generating these messages, the floor control server sends FloorStatus messages, periodically keeping the client informed about all the floors for which the client requested information. The Transaction ID of these messages MUST be 0 when using reliable transports and non-zero and unique in the context of outstanding transactions when using unreliable transports (cf. Section 8).

> The rate at which the floor control server sends FloorStatus messages is a matter of local policy. A floor control server may choose to send a new FloorStatus message every time a new floor request arrives, while another may choose to only send a new FloorStatus message when a new floor request is Granted.

When communicating over unreliable transport and a FloorStatusAck message is not received within the transaction failure window, the floor control server MUST retransmit the FloorStatus message according to Section 6.2.

13.6. Reception of a ChairAction Message

On reception of a ChairAction message, the floor control server follows the rules in Section 9 that relate to client authentication and authorization. If while processing the ChairAction message, the floor control server encounters an error, it SHOULD generate an Error response following the procedures described in Section 13.8.

The successful processing of a ChairAction message by a floor control server involves generating a ChairActionAck message, which SHOULD be generated as soon as possible.

When communicating over unreliable transport and upon receiving a ChairAction from a chair, the floor control server MUST respond with a ChairActionAck message within the transaction failure window to complete the transaction.

The floor control server MUST copy the Conference ID, the Transaction ID, and the User ID from the ChairAction message into the ChairActionAck message, as described in Section 8.2.

The floor control server needs to take into consideration the operation requested in the ChairAction message (e.g., granting a floor) but does not necessarily need to perform it as requested by the floor chair. The operation that the floor control server performs depends on the ChairAction message and on the internal state of the floor control server.

For example, a floor chair may send a ChairAction message granting a floor that was requested as part of an atomic floor request operation that involved several floors. Even if the chair responsible for one of the floors instructs the floor control server to grant the floor, the floor control server will not grant it until the chairs responsible for the other floors agree to grant them as well.

So, the floor control server is ultimately responsible for keeping a coherent floor state using instructions from floor chairs as input to this state.

If the new Status in the ChairAction message is Accepted and all the bits of the Queue Position field are zero, the floor chair is requesting that the floor control server assign a queue position (e.g., the last in the queue) to the floor request based on the local policy of the floor control server. (Of course, such a request only applies if the floor control server implements a queue.)

13.7. Reception of a Hello Message

On reception of a Hello message, the floor control server follows the rules in Section 9 that relate to client authentication. If while processing the Hello message, the floor control server encounters an error, it SHOULD generate an Error response following the procedures described in Section 13.8.

When communicating over unreliable transport and upon receiving a Hello from a participant, the floor control server MUST respond with a HelloAck message within the transaction failure window to complete the transaction.

The successful processing of a Hello message by a floor control server involves generating a HelloAck message, which SHOULD be generated as soon as possible. The floor control server MUST copy the Conference ID, the Transaction ID, and the User ID from the Hello into the HelloAck, as described in Section 8.2.

The floor control server MUST add a SUPPORTED-PRIMITIVES attribute to the HelloAck message listing all the primitives (i.e., BFCP messages) supported by the floor control server.

The floor control server MUST add a SUPPORTED-ATTRIBUTES attribute to the HelloAck message listing all the attributes supported by the floor control server.

13.8. Error Message Generation

Error messages are always sent in response to a previous message from the client as part of a client-initiated transaction. The ABNF in Section 5.3.13 describes the attributes that an Error message can contain. In addition, the ABNF specifies normatively which of these attributes are mandatory and which ones are optional.

The floor control server MUST copy the Conference ID, the Transaction ID, and the User ID from the message from the client into the Error message, as described in Section 8.2.

The floor control server MUST add an ERROR-CODE attribute to the Error message. The ERROR-CODE attribute contains an Error Code from Table 5. Additionally, the floor control server may add an ERROR-INFO attribute with extra information about the error.

14. Security Considerations

BFCP uses TLS/DTLS to provide mutual authentication between clients and servers. TLS/DTLS also provides replay and integrity protection and confidentiality. It is RECOMMENDED that TLS/DTLS with non-null encryption always be used. BFCP entities MAY use other security mechanisms as long as they provide similar security properties.

The remainder of this section analyzes some of the threats against BFCP and how they are addressed.

An attacker may attempt to impersonate a client (a floor participant or a floor chair) in order to generate forged floor requests or to grant or deny existing floor requests. Client impersonation is avoided by having servers only accept BFCP messages over authenticated TLS/DTLS connections. The floor control server assumes that attackers cannot highjack the TLS/DTLS connection and, therefore, that messages over the TLS/DTLS connection come from the client that was initially authenticated.

An attacker may attempt to impersonate a floor control server. A successful attacker would be able to make clients think that they

hold a particular floor so that they would try to access a resource (e.g., sending media) without having legitimate rights to access it. Floor control server impersonation is avoided by having servers only accept BFCP messages over authenticated TLS/DTLS connections, as well as ensuring clients only send and accept messages over authenticated TLS/DTLS connections.

Attackers may attempt to modify messages exchanged by a client and a floor control server. The integrity protection provided by TLS/DTLS connections prevents this attack.

An attacker may attempt to fetch a valid message sent by a client to a floor control server and replay it over a connection between the attacker and the floor control server. This attack is prevented by having floor control servers check that messages arriving over a given authenticated TLS/DTLS connection use an authorized user ID (i.e., a user ID that the user that established the authenticated TLS/DTLS connection is allowed to use).

Attackers may attempt to pick messages from the network to get access to confidential information between the floor control server and a client (e.g., why a floor request was denied). TLS/DTLS confidentiality prevents this attack. Therefore, it is RECOMMENDED that TLS/DTLS be used with a non-null encryption algorithm.

15. IANA Considerations

> [Editorial note: This section instructs the IANA to register new entries in the BFCP Primitive subregistry in Section 15.2 and for the BFCP Error Code subregistry in Section 15.4.]

The IANA has created a registry for BFCP parameters called "Binary Floor Control Protocol (BFCP) Parameters". This registry has a number of subregistries, which are described in the following sections.

15.1. Attribute Subregistry

This section establishes the Attribute subregistry under the BFCP Parameters registry. As per the terminology in RFC 5226 [3], the registration policy for BFCP attributes shall be "Specification Required". For the purposes of this subregistry, the BFCP attributes for which IANA registration is requested MUST be defined by a standards-track RFC. Such an RFC MUST specify the attribute's type, name, format, and semantics.

For each BFCP attribute, the IANA registers its type, its name, and

the reference to the RFC where the attribute is defined. The following table contains the initial values of this subregistry.

Type	Attribute	Reference
1	BENEFICIARY-ID	[RFC XXXX]
2	FLOOR-ID	[RFC XXXX]
3	FLOOR-REQUEST-ID	[RFC XXXX]
4	PRIORITY	[RFC XXXX]
5	REQUEST-STATUS	[RFC XXXX]
6	ERROR-CODE	[RFC XXXX]
7	ERROR-INFO	[RFC XXXX]
8	PARTICIPANT-PROVIDED-INFO	[RFC XXXX]
9	STATUS-INFO	[RFC XXXX]
10	SUPPORTED-ATTRIBUTES	[RFC XXXX]
11	SUPPORTED-PRIMITIVES	[RFC XXXX]
12	USER-DISPLAY-NAME	[RFC XXXX]
13	USER-URI	[RFC XXXX]
14	BENEFICIARY-INFORMATION	[RFC XXXX]
15	FLOOR-REQUEST-INFORMATION	[RFC XXXX]
16	REQUESTED-BY-INFORMATION	[RFC XXXX]
17	FLOOR-REQUEST-STATUS	[RFC XXXX]
18	OVERALL-REQUEST-STATUS	[RFC XXXX]

Table 7: Initial values of the BFCP Attribute subregistry

15.2. Primitive Subregistry

[Editorial note: This section instructs the IANA to register the following new values for the BFCP Primitive subregistry: FloorRequestStatusAck, FloorStatusAck, Goodbye, and GoodbyeAck.]

This section establishes the Primitive subregistry under the BFCP Parameters registry. As per the terminology in RFC 5226 [3], the registration policy for BFCP primitives shall be "Specification Required". For the purposes of this subregistry, the BFCP primitives for which IANA registration is requested MUST be defined by a standards-track RFC. Such an RFC MUST specify the primitive's value, name, format, and semantics.

For each BFCP primitive, the IANA registers its value, its name, and the reference to the RFC where the primitive is defined. The following table contains the initial values of this subregistry.

Value	Primitive	Reference
1	FloorRequest	[RFC XXXX]
2	FloorRelease	[RFC XXXX]
3	FloorRequestQuery	[RFC XXXX]
4	FloorRequestStatus	[RFC XXXX]
5	UserQuery	[RFC XXXX]
6	UserStatus	[RFC XXXX]
7	FloorQuery	[RFC XXXX]
8	FloorStatus	[RFC XXXX]
9	ChairAction	[RFC XXXX]
10	ChairActionAck	[RFC XXXX]
11	Hello	[RFC XXXX]
12	HelloAck	[RFC XXXX]
13	Error	[RFC XXXX]
14	FloorRequestStatusAck	[RFC XXXX]
15	FloorStatusAck	[RFC XXXX]
16	Goodbye	[RFC XXXX]
17	GoodbyeAck	[RFC XXXX]

Table 8: Initial values of the BFCP primitive subregistry

15.3. Request Status Subregistry

This section establishes the Request Status subregistry under the BFCP Parameters registry. As per the terminology in RFC 5226 [3], the registration policy for BFCP request status shall be "Specification Required". For the purposes of this subregistry, the BFCP request status for which IANA registration is requested MUST be defined by a standards-track RFC. Such an RFC MUST specify the value and the semantics of the request status.

For each BFCP request status, the IANA registers its value, its meaning, and the reference to the RFC where the request status is defined. The following table contains the initial values of this subregistry.

Value	Status	Reference
1	Pending	[RFC XXXX]
2	Accepted	[RFC XXXX]
3	Granted	[RFC XXXX]
4	Denied	[RFC XXXX]
5	Cancelled	[RFC XXXX]
6	Released	[RFC XXXX]
7	Revoked	[RFC XXXX]

Table 9: Initial values of the Request Status subregistry

15.4. Error Code Subregistry

[Editorial note: This section instructs the IANA to register the following new values for the BFCP Error Code subregistry: 10, 11, 12, 13 and 14.]

This section establishes the Error Code subregistry under the BFCP Parameters registry. As per the terminology in RFC 5226 [3], the registration policy for BFCP error codes shall be "Specification Required". For the purposes of this subregistry, the BFCP error codes for which IANA registration is requested MUST be defined by a standards-track RFC. Such an RFC MUST specify the value and the semantics of the error code, and any Error Specific Details that apply to it.

For each BFCP primitive, the IANA registers its value, its meaning, and the reference to the RFC where the primitive is defined. The following table contains the initial values of this subregistry.

Value	Meaning	Reference
1	Conference does not Exist	[RFC XXXX]
2	User does not Exist	[RFC XXXX]
3	Unknown Primitive	[RFC XXXX]
4	Unknown Mandatory Attribute	[RFC XXXX]
5	Unauthorized Operation	[RFC XXXX]
6	Invalid Floor ID	[RFC XXXX]
7	Floor Request ID Does Not Exist	[RFC XXXX]
8	You have Already Reached the Maximum Number of Ongoing Floor Requests for this Floor	[RFC XXXX]
9	Use TLS	[RFC XXXX]
10	Unable to parse message	[RFC XXXX]
11	Use DTLS	[RFC XXXX]
12	Unsupported Version	[RFC XXXX]
13	Incorrect Message Length	[RFC XXXX]
14	Generic Error	[RFC XXXX]

Table 10: Initial Values of the Error Code subregistry

16. Changes from RFC 4582

Following is the list of technical changes and other non-trivial fixes from [17].

Main purpose of this work was to revise the specification to support BFCP over unreliable transport, resulting in the following changes:

Overview of Operation (Section 4):

Expand the description of client-initiated and server-initiated transactions.

COMMON-HEADER Format (Section 5.1):

Ver(sion) field, where the value 2 is used for the extensions for unreliable transport. Added new R and F flag-bits for unreliable transport. Res(erved) field is now 3 bit. New optional Fragment Offset and Fragment Length fields.

New primitives (Section 5.1):

Added five new primitives: FloorRequestStatusAck, FloorStatusAck, Goodbye, and GoodbyeAck.

New error codes (Section 5.2.6):
Added three new error codes: "Unable to Parse Message", "Use DTLS" and "Unsupported Version".

ABNF for new primitives (Section 5.3):
New subsections with normative ABNF for the new primitives.

Transport split in two (Section 6):
Section 6 specifying the transport was split in two subsections; Section 6.1 for reliable transport and Section 6.2 for unreliable transport. Where the specification for unreliable transport amongst other issues deals with reliability, congestion control, fragmentation and ICMP.

Mandate DTLS (Section 7 and Section 9):
Mandate DTLS support when transport over UDP is used.

Transaction changes (Section 8):
Server-initiated transactions over unreliable transport has non-zero and unique Transaction ID. Over unreliable transport, the retransmit timers T1 and T2 described in Section 8.3 applies.

Requiring timely response (Section 10.1.2, Section 10.2.2, Section 11.2, Section 12.1.2, Section 12.2.2, Section 12.3.2, Section 12.4.2, Section 10.1.3 and Section 12.1.3):
Describing that a given response must be sent within the transaction failure window to complete the transaction.

Updated IANA Considerations (Section 15):
Added the new primitives and error codes to Section 15.2 and Section 15.4 respectively.

Examples over unreliable transport (Appendix A):
Added sample interactions over unreliable transport for the scenarios in Figure 2 and Figure 3

Motivation for unreliable transport (Appendix B):
Introduction to and motivation for extending BFCP to support unreliable transport.

The clarification and bug fixes:

ABNF fixes (Figure 22, Figure 24, ="fig:reqby-information"/>, Figure 28, Figure 30, and the ABNF figures in Section 5.3):
Although formally correct in [17], the notation has changed in a number of Figures to an equivalent form for clarity, e.g. s/*1(FLOOR-ID)/[FLOOR-ID]/ in Figure 38 and s/*[XXX]/*(XXX)/ in

the other figures.

Typo (Section 12.4.2):
Change from SUPPORTED-PRIMITIVES to SUPPORTED-PRIMITVIES in the second paragraph.

Corrected attribute type (Section 13.1.1):
Change from PARTICIPANT-PROVIDED-INFO to PRIORITY attributed in the eighth paragraph, since the note below describes priority and that the last paragraph deals with PARTICIPANT-PROVIDED-INFO.

New error codes (Section 5.2.6):
Added two additional error codes: "Incorrect Message Length" and "Generic Error".

17. Acknowledgements

The XCON WG chairs, Adam Roach and Alan Johnston, provided useful ideas for RFC 4582 [17]. Additionally, Xiaotao Wu, Paul Kyzivat, Jonathan Rosenberg, Miguel A. Garcia-Martin, Mary Barnes, Ben Campbell, Dave Morgan, and Oscar Novo provided useful comments during the work with RFC 4582. The authors also acknowledge contributions to the revision of BFCP for use over an unreliable transport from Geir Arne Sandbakken who had the initial idea, Alfred E. Heggestad, Trond G. Andersen, Gonzalo Camarillo, Roni Even, Lorenzo Miniero, Joerg Ott, Eoin McLeod, Mark K. Thompson, Hadriel Kaplan, Dan Wing, Cullen Jennings, David Benham, Nivedita Melinkeri, Woo Johnman, Vijaya Mandava and Alan Ford. In the final phase Erns Horvath did a thorough review revealing issues that needed clarification and changes.

18. References

18.1. Normative References

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

[2] Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, January 2008.

[3] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.

[4] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.

[5] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security Version 1.2", RFC 6347, January 2012.

[6] Yergeau, F., "UTF-8, a transformation format of ISO 10646", STD 63, RFC 3629, November 2003.

[7] Camarillo, G. and T. Kristensen, Ed., "Session Description Protocol (SDP) Format for Binary Floor Control Protocol (BFCP) Streams", draft-ietf-bfcpbis-rfc4583bis-02 (work in progress), July 2012.

[8] Fischl, J., Tschofenig, H., and E. Rescorla, "Framework for Establishing a Secure Real-time Transport Protocol (SRTP) Security Context Using Datagram Transport Layer Security (DTLS)", RFC 5763, May 2010.

[9] Wing, D., "Symmetric RTP / RTP Control Protocol (RTCP)", BCP 131, RFC 4961, July 2007.

[10] Jennings, C., Mahy, R., and F. Audet, "Managing Client-Initiated Connections in the Session Initiation Protocol (SIP)", RFC 5626, October 2009.

[11] Rosenberg, J., Mahy, R., Matthews, P., and D. Wing, "Session Traversal Utilities for NAT (STUN)", RFC 5389, October 2008.

18.2. Informational References

[12] Rosenberg, J. and H. Schulzrinne, "An Offer/Answer Model with Session Description Protocol (SDP)", RFC 3264, June 2002.

[13] Koskelainen, P., Ott, J., Schulzrinne, H., and X. Wu, "Requirements for Floor Control Protocols", RFC 4376, February 2006.

[14] Barnes, M., Boulton, C., and O. Levin, "A Framework for Centralized Conferencing", RFC 5239, June 2008.

[15] Rosenberg, J., "Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols", RFC 5245, April 2010.

[16] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002.

[17] Camarillo, G., Ott, J., and K. Drage, "The Binary Floor Control Protocol (BFCP)", RFC 4582, November 2006.

[18] Huitema, C., "Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs)", RFC 4380, February 2006.

[19] Eggert, L. and G. Fairhurst, "Unicast UDP Usage Guidelines for Application Designers", BCP 145, RFC 5405, November 2008.

[20] Thaler, D., "Teredo Extensions", RFC 6081, January 2011.

[21] Stewart, R., "Stream Control Transmission Protocol", RFC 4960, September 2007.

[22] Rosenberg, J., Keranen, A., Lowekamp, B., and A. Roach, "TCP Candidates with Interactive Connectivity Establishment (ICE)", RFC 6544, March 2012.

[23] Manner, J., Varis, N., and B. Briscoe, "Generic UDP Tunnelling (GUT)", draft-manner-tsvwg-gut-02 (work in progress), July 2010.

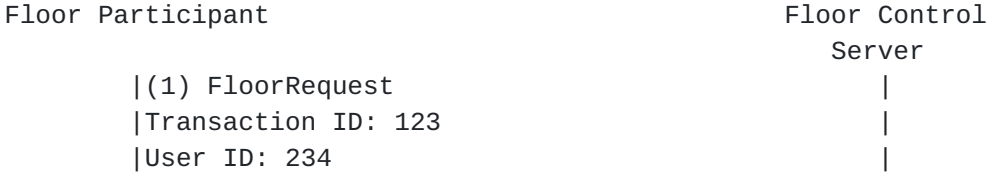
[24] Stucker, B., Tschofenig, H., and G. Salgueiro, "Analysis of Middlebox Interactions for Signaling Protocol Communication along the Media Path", draft-ietf-mmusic-media-path-middleboxes-04 (work in progress), January 2012.

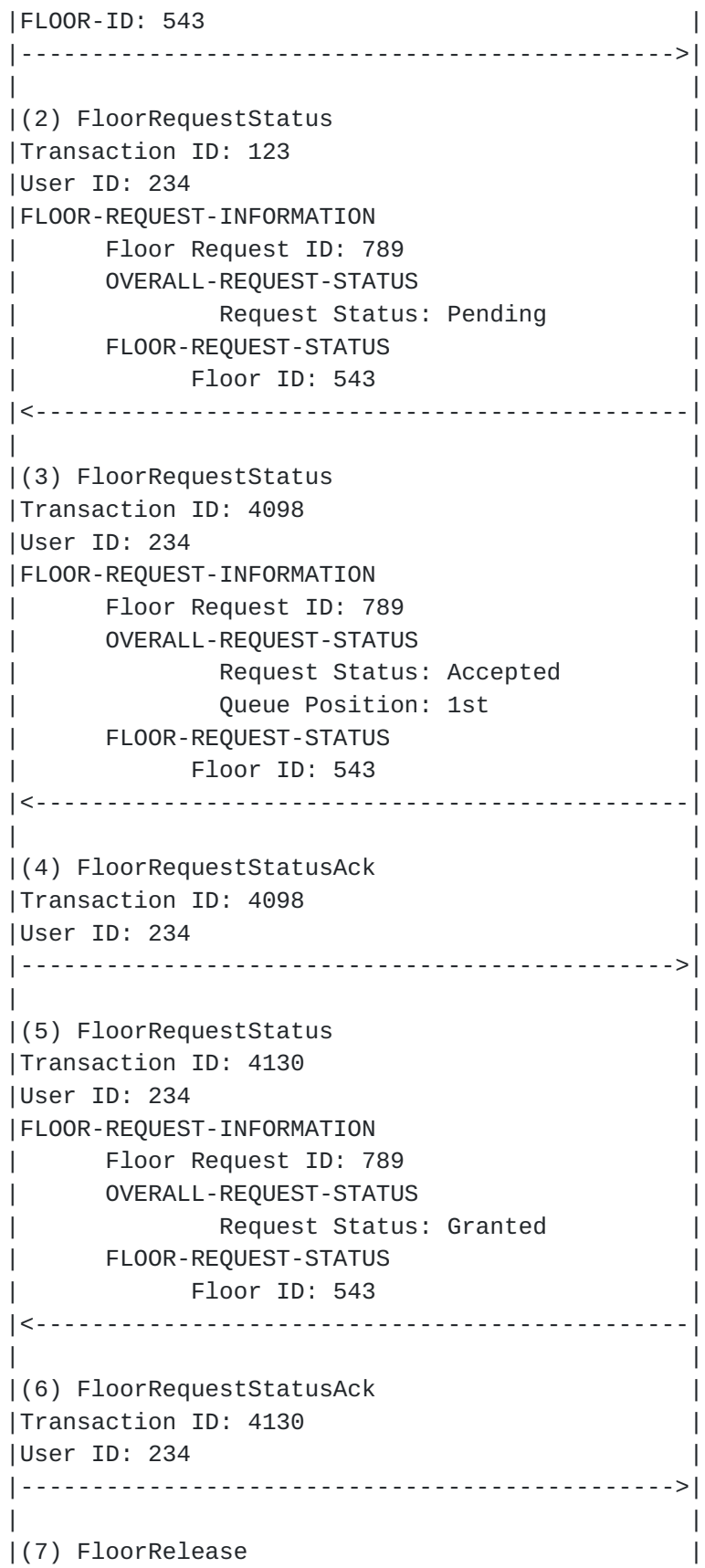
[25] Guha, S. and P. Francis, "Characterization and Measurement of TCP Traversal through NATs and Firewalls", 2005, <http://saikat.guha.cc/pub/imc05-tcpnat.pdf/>.

[26] Ford, B., Srisuresh, P., and D. Kegel, "Peer-to-Peer Communication Across Network Address Translators", April 2005, <http://www.brynosaurus.com/pub/net/p2pnat.pdf/>.

Appendix A. Example Call Flows for BFCP over Unreliable Transport

With reference to Section 4.1, the following figures show representative call-flows for requesting and releasing a floor, and obtaining status information about a floor when BFCP is deployed over an unreliable transport. The figures here show a loss-less interaction.




|FLOOR-ID: 543 |
|----------->|
| |
|(2) FloorRequestStatus |
|Transaction ID: 123 |
|User ID: 234 |
|FLOOR-REQUEST-INFORMATION |
| Floor Request ID: 789 |
| OVERALL-REQUEST-STATUS |
| Request Status: Pending |
| FLOOR-REQUEST-STATUS |
| Floor ID: 543 |
|<-----------|
| |
|(3) FloorRequestStatus |
|Transaction ID: 4098 |
|User ID: 234 |
|FLOOR-REQUEST-INFORMATION |
| Floor Request ID: 789 |
| OVERALL-REQUEST-STATUS |
| Request Status: Accepted |
| Queue Position: 1st |
| FLOOR-REQUEST-STATUS |
| Floor ID: 543 |
|<-----------|
| |
|(4) FloorRequestStatusAck |
|Transaction ID: 4098 |
|User ID: 234 |
|----------->|
| |
|(5) FloorRequestStatus |
|Transaction ID: 4130 |
|User ID: 234 |
|FLOOR-REQUEST-INFORMATION |
| Floor Request ID: 789 |
| OVERALL-REQUEST-STATUS |
| Request Status: Granted |
| FLOOR-REQUEST-STATUS |
| Floor ID: 543 |
|<-----------|
| |
|(6) FloorRequestStatusAck |
|Transaction ID: 4130 |
|User ID: 234 |
|----------->|
| |
|(7) FloorRelease |

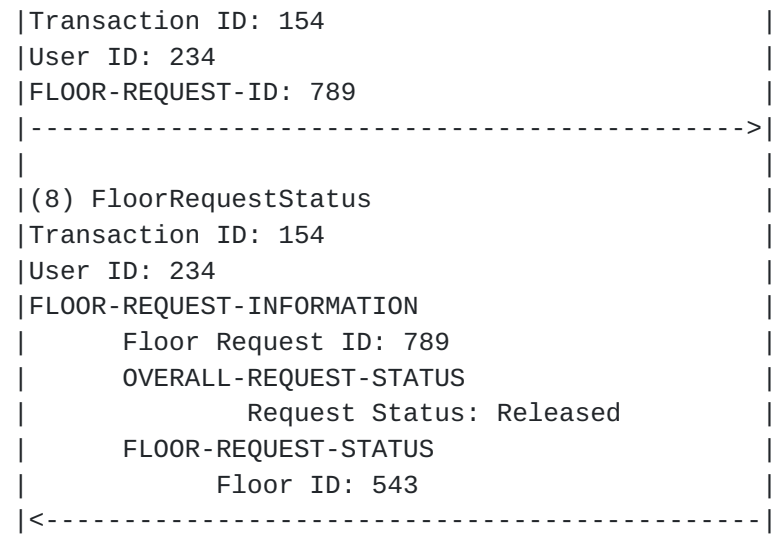
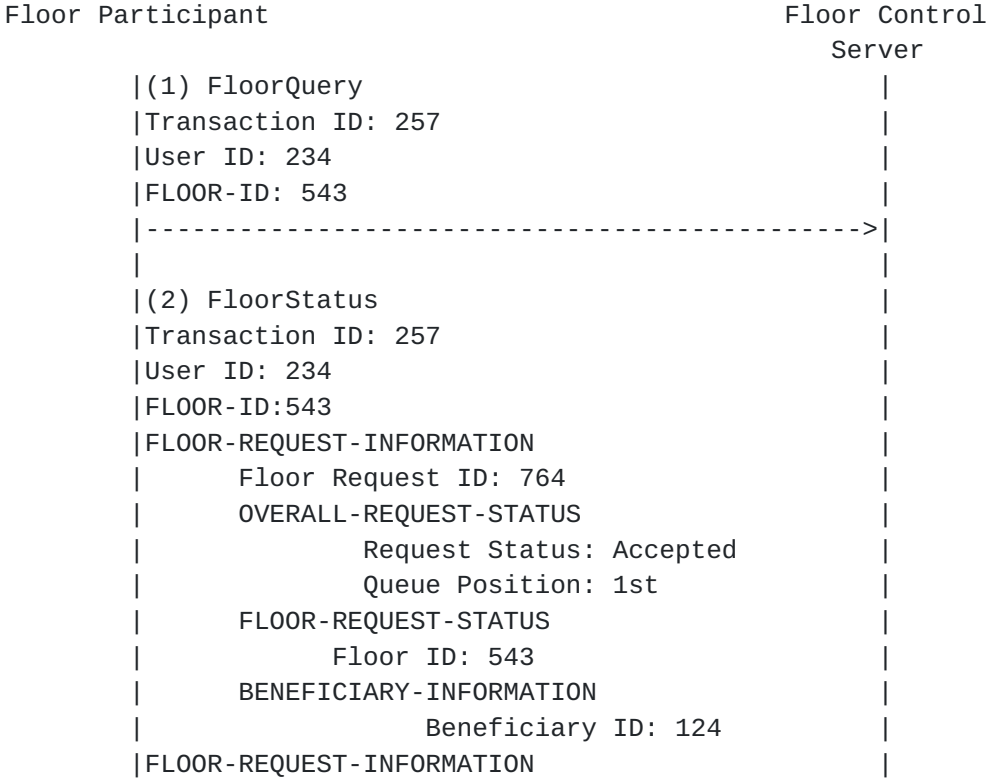
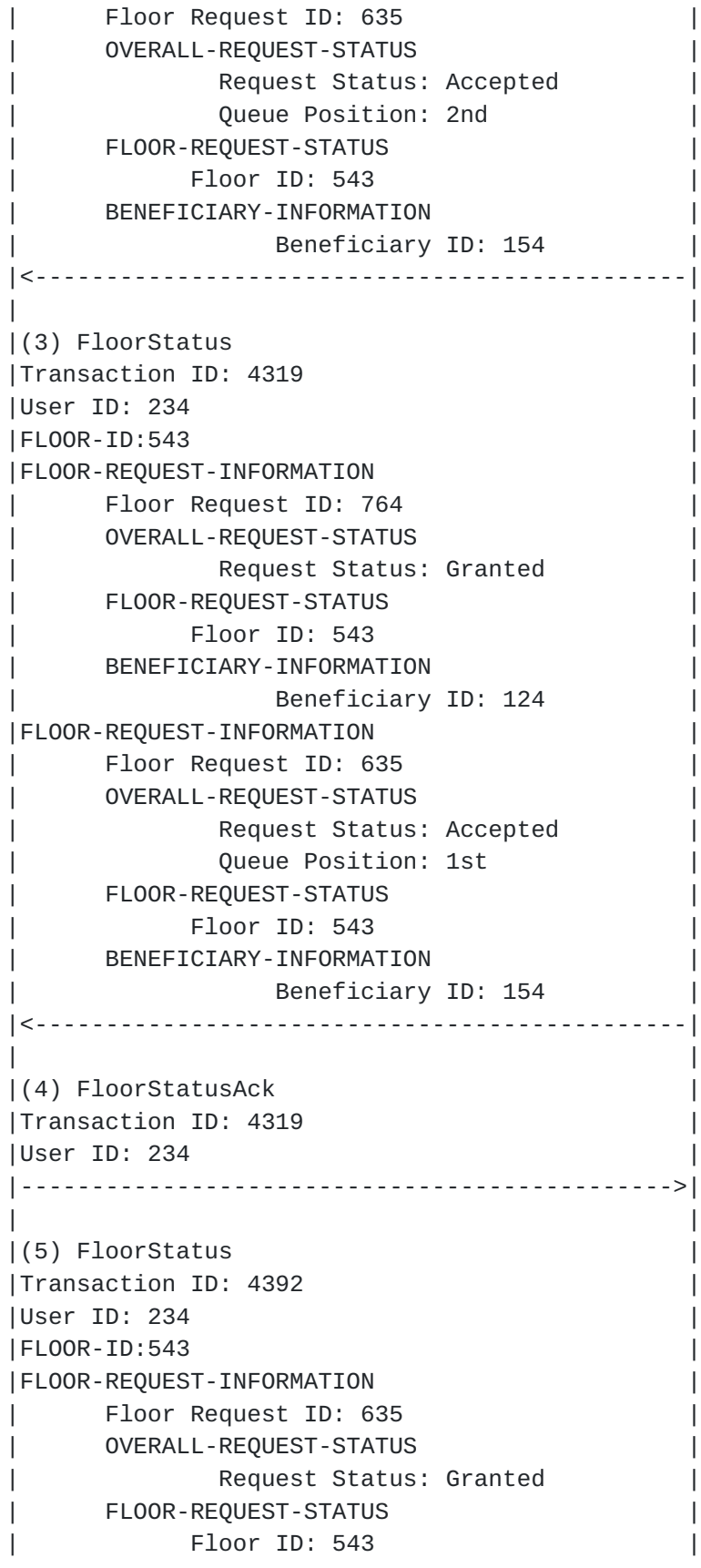


Figure 48: Requesting and releasing a floor

Note that in Figure 48, the FloorRequestStatus message from the floor control server to the floor participant is a transaction-closing message as a response to the client-initiated transaction with Transaction ID 154. It does not and SHOULD NOT be followed by a FloorRequestStatusAck message from the floor participant to the floor control server.




| Floor Request ID: 635 |
| OVERALL-REQUEST-STATUS |
| Request Status: Accepted |
| Queue Position: 2nd |
| FLOOR-REQUEST-STATUS |
| Floor ID: 543 |
| BENEFICIARY-INFORMATION |
| Beneficiary ID: 154 |
|<----------|
| |
|(3) FloorStatus |
|Transaction ID: 4319 |
|User ID: 234 |
|FLOOR-ID:543 |
|FLOOR-REQUEST-INFORMATION |
| Floor Request ID: 764 |
| OVERALL-REQUEST-STATUS |
| Request Status: Granted |
| FLOOR-REQUEST-STATUS |
| Floor ID: 543 |
| BENEFICIARY-INFORMATION |
| Beneficiary ID: 124 |
|FLOOR-REQUEST-INFORMATION |
| Floor Request ID: 635 |
| OVERALL-REQUEST-STATUS |
| Request Status: Accepted |
| Queue Position: 1st |
| FLOOR-REQUEST-STATUS |
| Floor ID: 543 |
| BENEFICIARY-INFORMATION |
| Beneficiary ID: 154 |
|<----------|
| |
|(4) FloorStatusAck |
|Transaction ID: 4319 |
User ID: 234
(5) FloorStatus
Transaction ID: 4392
User ID: 234
FLOOR-ID:543
FLOOR-REQUEST-INFORMATION
Floor Request ID: 635
OVERALL-REQUEST-STATUS
Request Status: Granted
FLOOR-REQUEST-STATUS
Floor ID: 543

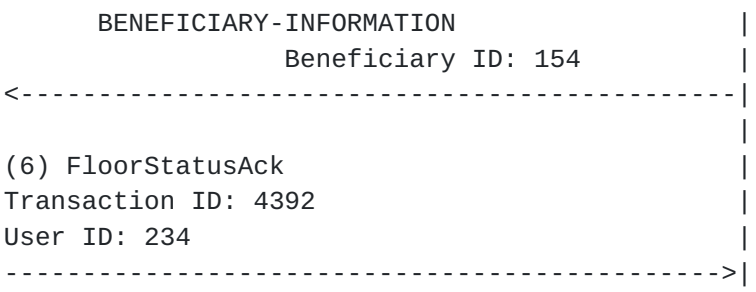


Figure 49: Obtaining status information about a floor

Appendix B. Motivation for Supporting Unreliable Transport

[Editorial note: This appendix is contained in this draft as an aid and rationale for new readers and reviewers. However, it is not yet decided whether this Appendix will be part of the final (RFC) version or not.]

B.1. Motivation

In existing video conferencing deployments, BFCP is used to manage the floor for the content sharing associated with the conference. For peer to peer scenarios, including business to business conferences and point to point conferences in general, it is frequently the case that one or both endpoints exists behind a NAT/ firewall. BFCP roles are negotiated in the offer/answer exchange as specified in [7], resulting in one endpoint being responsible for opening the TCP connection used for the BFCP communication.

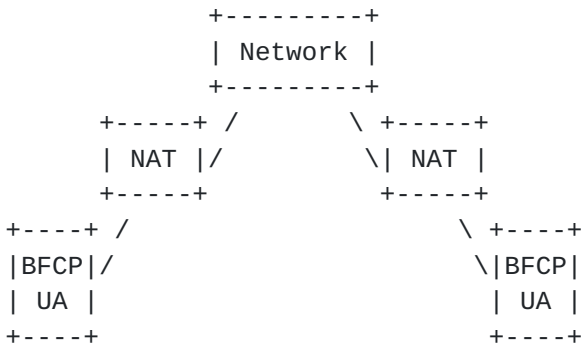


Figure 50: Use Case

The communication session between the video conferencing endpoints typically consists of a number of RTP over UDP media streams, for audio and video, and a BFCP connection for floor control. Existing deployments are most common in, but not limited to, enterprise

networks. In existing deployments, NAT/firewall traversal for the RTP streams works using ICE and/or other methods, including those described in [24].

When enhancing an existing SIP based video conferencing deployment with support for content sharing, the BFCP connection often poses a problem. The reasons for this fall into two general classes. First, there may be a strong preference for UDP based signaling in general. On high capacity endpoints (e.g. PSTN gateways or SIP/H.323 inter-working gateways), TCP can suffer from head of line blocking, and it uses many kernel buffers. Network operators view UDP as a way to avoid both of these. Second, establishment and traversal of the TCP connection involving ephemeral ports, as is typically the case with BFCP over TCP, can be problematic, as described in Appendix A of [22]. A broad study of NAT behavior and peer-to-peer TCP establishment for a comprehensive set of TCP NAT traversal techniques over a wide range of commercial NAT products concluded it was not possible to establish a TCP connection in 11% of the cases [25]. The results are worse when focusing on enterprise NATs. A study of hole punching as a NAT traversal technique across a wide variety of deployed NATs reported consistently higher success rates when using UDP than when using TCP [26].

It is worth noticing that BFCP over UDP were already used in real deployments, underlining the necessity to specify a common way to exchange BFCP messages where TCP is not appropriate, to avoid a situation where multiple different and non-interoperable would co-exist in the market. The purpose of this draft is to formalize and publish the extension from the standard specification to facilitate complete interoperability between implementations.

B.1.1. Alternatives Considered

In selecting the approach of defining UDP as an alternate transport for BFCP, several alternatives were considered and explored to some degree. Each of these is discussed briefly in the following subsections. In summary, while the not chosen alternatives work in a number of scenarios, they are not sufficient, in and of themselves, to address the use case targeted by this draft. The last alternative, presented in Appendix B.1.1.7, is the selected one and is specified in this draft.

It is also worth noting that the IETF Transport Area were asked for a way to tunnel TCP over UDP, but at that point there was no consensus on how to achieve that.

B.1.1.1. ICE TCP

ICE TCP [22] extends ICE to TCP based media, including the ability to offer a mix of TCP and UDP based candidates for a single stream. ICE TCP has, in general, a lower success probability for enabling TCP connectivity without a relay if both of the hosts are behind a NAT (see Appendix A of [22]) than enabling UDP connectivity in the same scenarios. The happens because many of the currently deployed NATs in video conferencing networks do not support the flow of TCP hand shake packets seen in case of TCP simultaneous-open, either because they do not allow incoming TCP SYN packets from an address to which a SYN packet has been sent to recently, or because they do not properly process the subsequent SYNACK. Implementing various techniques advocated for candidate collection in [22] should increase the success probability, but many of these techniques require support from some network elements (e.g., from the NATs). Such support is not common in enterprise firewalls and NATs.

B.1.1.2. Teredo

Teredo [18] enables nodes located behind one or more IPv4 NATs to obtain IPv6 connectivity by tunneling packets over UDP. Teredo extensions [20] provide additional capabilities to Teredo, including support for more types of NATs and support for more efficient communication.

As defined, Teredo could be used to make BFCP work for the video conferencing use cases addressed in this draft. However, running the service requires the help of "Teredo servers" and "Teredo relays" [18]. These servers and relays generally do not exist in the existing video conferencing deployments. It also requires IPv6 awareness on the endpoints. It should also be noted that ICMP6, as used with Teredo to complete an initial protocol exchange and confirm that the appropriate NAT bindings have been set up, is not a conventional feature of IPv4 or even IPv6, and some currently deployed IPv6 firewalls discard ICMP messages. As these networks continue to evolve and tackle the transaction to IPv6, Teredo servers and relays may be deployed, making Teredo available as a suitable alternative to BFCP over UDP.

B.1.1.3. GUT

GUT [23] attempts to facilitate tunneling over UDP by encapsulating the native transport protocol and its payload (in general the whole IP payload) within a UDP packet destined to the well-known port GUT_P. Unfortunately, it requires user-space TCP, for which there is not a readily available implementation, and creating one is a large project in itself. This draft has expired and its future is still

not clear as it has not yet been adopted by a working group.

B.1.1.4. UPnP IGD

Universal Plug and Play Internet Gateway Devices (UPnP IGD) sit on the edge of the network, providing connectivity to the Internet for computers internal to the LAN, but do not allow Internet devices to connect to computers on the internal LAN. IGDs enable a computer on an internal LAN to create port mappings on their NAT, through which hosts on the Internet can send data that will be forwarded to the computer on the internal LAN. IGDs may be self-contained hardware devices or may be software components provided within an operating system.

In considering UPnP IGD, several issues exist. Not all NATs support UPnP, and many that do support it are configured with it turned off by default. NATs are often multilayered, and UPnP does not work well with such NATs. For example, a typical DSL modems acts as a NAT, and the user plugs in a wireless access point behind that, which adds another layer NAT. The client can discover the first layer of NAT using multicast but it is harder to figure out how to discover and control NATs in the next layer up.

B.1.1.5. NAT PMP

The NAT Port Mapping Protocol (NAT PMP) allows a computer in a private network (behind a NAT router) to automatically configure the router to allow parties outside the private network to contact it. NAT PMP runs over UDP. It essentially automates the process of port forwarding. Included in the protocol is a method for retrieving the public IP address of a NAT gateway, thus allowing a client to make this public IP address and port number known to peers that may wish to communicate with it.

Many NATs do not support PMP. In those that do support it, it has similar issues with negotiation of multilayer NATs as UPnP. Video conferencing is used extensively in enterprise networks, and NAT PMP is not generally available in enterprise-class routers.

B.1.1.6. SCTP

It would be quite straight forward to specify a BFCP binding for SCTP [21], and then tunnel SCTP over UDP in the use case described in Appendix B.1. SCTP is gaining some momentum currently. There is ongoing discussion in the RTCWeb WG regarding this approach. However, this approach for tunneling over UDP was not mature enough when considered and not even fully specified.

B.1.1.7. BFCP over UDP transport

To overcome the problems with establishing TCP flows between BFCP entities, an alternative is to define UDP as an alternate transport for BFCP, leveraging the same mechanisms in place for the RTP over UDP media streams for the BFCP communication. When using UDP as the transport, it is recommended to follow the guidelines provided in [19].

Minor changes to the transaction model are introduced in that all requests now have an appropriate response to complete the transaction. The requests are sent with a retransmit timer associated with the response to achieve reliability. This alternative does not change the semantics of BFCP. It permits UDP as an alternate transport.

Existing implementations, in the spirit of the approach detailed in earlier versions of this draft, have demonstrated this approach to be feasible. Initial compatibility among implementations has been achieved at previous interoperability events. The authors view this extension as a pragmatic solution to an existing deployment challenge. This is the chosen approach, and the extensions is specified in this document.

Authors' Addresses

Gonzalo Camarillo
Ericsson
Hirsalantie 11
Jorvas 02420
Finland

Email: gonzalo.camarillo@ericsson.com

Keith Drage
Alcatel-Lucent
Quadrant, StoneHill Green, Westlea
Swindon, Wilts
UK

Email: drage@alcatel-lucent.com

Tom Kristensen (editor)
Cisco
Philip Pedersens vei 22
N-1366 Lysaker
Norway

Email: tomkrist@cisco.com, tomkri@ifi.uio.no

Joerg Ott
Aalto University
Otakaari 5 A
Espoo, FIN 02150
Finland

Email: jo@comnet.tkk.fi

Charles Eckel
Cisco
170 West Tasman Drive
San Jose, CA 95134
United States

Email: eckelcu@cisco.com