

BFCPBIS Working Group  
Internet-Draft  
Updates: rfc4582bis, rfc4583bis (if approved)  
Intended status: Standards Track  
Expires: August 13, 2014

V. Pascual  
A. Roman  
Quobis  
S. Cazeaux  
France Telecom Orange  
G. Salgueiro  
Cisco  
S. Garcia Murillo  
Medooze  
February 9, 2014

The WebSocket Protocol as a Transport for the Binary Floor Control  
Protocol (BFCP)  
draft-pascual-bfcpbis-bfcp-websocket-00

## Abstract

The WebSocket protocol enables two-way realtime communication between clients and servers. This document specifies a new WebSocket sub-protocol as a reliable transport mechanism between Binary Floor Control Protocol (BFCP) entities to enable usage of BFCP in new scenarios. This document normatively updates [I-D.draft-ietf-bfcpbis-rfc4582bis] and [I-D.draft-ietf-bfcpbis-rfc4583bis]

## 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 August 13, 2014.

## Copyright Notice

Copyright (c) 2014 IETF Trust and the persons identified as the document authors. All rights reserved.

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

## Table of Contents

1. Introduction . . . . .	2
2. Terminology . . . . .	3
2.1. Definitions . . . . .	3
3. The WebSocket Protocol . . . . .	4
4. The WebSocket BFCP Sub-Protocol . . . . .	4
4.1. Handshake . . . . .	5
4.2. BFCP encoding . . . . .	5
5. BFCP WebSocket Transport . . . . .	6
6. Fields in the 'm' Line . . . . .	6
7. Authentication . . . . .	7
8. Security Considerations . . . . .	8
9. IANA Considerations . . . . .	9
9.1. Registration of the WebSocket BFCP Sub-Protocol . . . . .	9
9.2. Registration of the 'TCP/WS/BFCP' and 'TCP/WSS/BFCP' SDP 'proto' Values . . . . .	9
9.3. Registration of the 'ws-uri' SDP media attribute . . . . .	9
9.4. Acknowledgements . . . . .	10
10. References . . . . .	10
10.1. Normative References . . . . .	10
10.2. Informative References . . . . .	10
Authors' Addresses . . . . .	11

## 1. Introduction

The WebSocket [RFC6455] protocol enables two-way message exchange between clients and servers on top of a persistent TCP connection (optionally secured with TLS [RFC5246]). The initial protocol handshake makes use of HTTP [RFC2616] semantics, allowing the WebSocket protocol to reuse existing HTTP infrastructure.

The Binary Floor Control Protocol (BFCP) is a protocol to coordinate access to shared resources in a conference. It is defined in [I-D.ietf-bfcpbis-rfc4582bis] and is used between floor participants and floor control servers, and between floor chairs (i.e., moderators) and floor control servers.

Modern web browsers include a WebSocket client stack complying with the WebSocket API [WS-API] as specified by the W3C. It is expected that other client applications (those running in personal computers and devices such as smartphones) will also make a WebSocket client stack available. This document updates [I-D.ietf-bfcpbis-rfc4582bis] and [I-D.ietf-bfcpbis-rfc4583bis] in order to enable the usage of BFCP in these scenarios.

The transport over which BFCP entities exchange messages depends on how the clients obtain information to contact the floor control server (e.g. using an SDP offer/answer exchange per [I-D.ietf-bfcpbis-rfc4583bis] or the procedure described in RFC5018 [RFC5018]). [I-D.ietf-bfcpbis-rfc4582bis] defines two transports for BFCP: TCP and UDP. This specification defines a new WebSocket sub-protocol (as defined in section 1.9 in [RFC6455]) for transporting BFCP messages between a WebSocket client and server, a new reliable and message boundary transport for BFCP. In order to enable this, this document also defines two new SDP 'proto' values.

This document does not restrict the selection nor prevent the usage of other transport mechanisms for the BFCP protocol. Transport selection is entirely at the discretion of the application. As an example, an RTCWeb applications may choose to use either DataChannel or WebSocket transport for BFCP, while non-RTCWeb applications could still benefit from the ubiquity of the WebSocket protocol and make use of the transport for BFCP defined in this document.

## 2. Terminology

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

### 2.1. Definitions

**BFCP WebSocket Client:** A BFCP entity capable of opening outbound connections to WebSocket servers and communicating using the WebSocket BFCP sub-protocol as defined by this document.

**BFCP WebSocket Server:** A BFCP entity capable of listening for inbound connections from WebSocket clients and communicating using the WebSocket BFCP sub-protocol as defined by this document.

### 3. The WebSocket Protocol

The WebSocket protocol [RFC6455] is a transport layer on top of TCP (optionally secured with TLS [RFC5246]) in which both client and server exchange message units in both directions. The protocol defines a connection handshake, WebSocket sub-protocol and extensions negotiation, a frame format for sending application and control data, a masking mechanism, and status codes for indicating disconnection causes.

The WebSocket connection handshake is based on HTTP [RFC2616] and utilizes the HTTP GET method with an "Upgrade" request. This is sent by the client and then answered by the server (if the negotiation succeeded) with an HTTP 101 status code. Once the handshake is completed the connection upgrades from HTTP to the WebSocket protocol. This handshake procedure is designed to reuse the existing HTTP infrastructure. During the connection handshake, client and server agree on the application protocol to use on top of the WebSocket transport. Such an application protocol (also known as a "WebSocket sub-protocol") defines the format and semantics of the messages exchanged by the endpoints. This could be a custom protocol or a standardized one (as the WebSocket BFCP sub-protocol defined in this document). Once the HTTP 101 response is processed both client and server reuse the underlying TCP connection for sending WebSocket messages and control frames to each other. Unlike plain HTTP, this connection is persistent and can be used for multiple message exchanges.

The WebSocket protocol defines message units to be used by applications for the exchange of data, so it provides a message boundary-preserving transport layer. These message units can contain either UTF-8 text or binary data, and can be split into multiple WebSocket text/binary transport frames as needed by the WebSocket stack.

The WebSocket API [WS-API] for web browsers only defines callbacks to be invoked upon receipt of an entire message unit, regardless of whether it was received in a single WebSocket frame or split across multiple frames.

### 4. The WebSocket BFCP Sub-Protocol

The term WebSocket sub-protocol refers to an application-level protocol layered on top of a WebSocket connection. This document specifies the WebSocket BFCP sub-protocol for carrying BFCP messages through a WebSocket connection.

#### 4.1. Handshake

The BFCP WebSocket Client and BFCP WebSocket Server negotiate usage of the WebSocket BFCP sub-protocol during the WebSocket handshake procedure as defined in section 1.3 of [RFC6455]. The Client **MUST** include the value "bfc" in the Sec-WebSocket-Protocol header in its handshake request. The 101 reply from the Server **MUST** contain "bfc" in its corresponding Sec-WebSocket-Protocol header.

Below is an example of a WebSocket handshake in which the Client requests the WebSocket BFCP sub-protocol support from the Server:

```
GET / HTTP/1.1
Host: bfc-ws.example.com
Upgrade: websocket
Connection: Upgrade
Sec-WebSocket-Key: dGhlIHNhbXBsZSBub25jZQ==
Origin: http://www.example.com
Sec-WebSocket-Protocol: bfc
Sec-WebSocket-Version: 13
```

The handshake response from the Server accepting the WebSocket BFCP sub-protocol would look as follows:

```
HTTP/1.1 101 Switching Protocols
Upgrade: websocket
Connection: Upgrade
Sec-WebSocket-Accept: s3pPLMBiTxaQ9kYGzzhZRbK+xOo=
Sec-WebSocket-Protocol: bfc
```

Once the negotiation has been completed, the WebSocket connection is established and can be used for the transport of BFCP messages. The WebSocket messages transmitted over this connection **MUST** conform to the negotiated WebSocket sub-protocol.

#### 4.2. BFCP encoding

BFCP messages use a TLV (Type-Length-Value) binary encoding, therefore BFCP WebSocket Clients and BFCP WebSocket Servers **MUST** be transported in unfragmented binary WebSocket frames (FIN:1,opcode:%x2) to exchange BFCP messages. The WebSocket frame data **MUST** be a valid BFCP message, so the length of the payload of the WebSocket frame **MUST** be lower than the maximum size allowed ( $2^{16} + 12$  bytes) for a BFCP message as described in [I-D.ietf-bfcpbis-rfc4582bis]. In addition, the encoding rules for reliable protocols defined in [I-D.ietf-bfcpbis-rfc4582bis] **MUST** be followed.

## 5. BFCP WebSocket Transport

WebSocket [RFC6455] is a reliable protocol and therefore the BFCP WebSocket sub-protocol defined by this document is a reliable BFCP transport. Thus, client and server transactions using WebSocket for transport MUST follow the procedures for reliable transports as defined in [I-D.ietf-bfcpbis-rfc4582bis] and [I-D.ietf-bfcpbis-rfc4583bis]

BFCP WebSocket clients cannot receive incoming WebSocket connections initiated by any other peer. This means that a BFCP Websocket client MUST actively initiate a connection towards a BFCP Websocket server

Each BFCP message MUST be carried within a single WebSocket message, and a WebSocket message MUST NOT contain more than one BFCP message.

## 6. Fields in the 'm' Line

Rules to generate an 'm' line for a BFCP stream are described in [I-D.ietf-bfcpbis-rfc4583bis], Section 3

New values are defined for the transport field: TCP/WS/BFCP and TCP/WSS/BFCP.

TCP/WS/BFCP is used when BFCP runs on top of WS, which in turn runs on top of TCP.

TCP/WSS/BFCP is used when BFCP runs on top of WSS, which in turn runs on top of TLS and TCP.

When TCP is used as the transport, the port field is set following the rules in Section 7 of [I-D.ietf-bfcpbis-rfc4582bis]. Depending on the value of the 'setup' attribute, the port field contains the port to which the remote endpoint will direct BFCP messages or is irrelevant (i.e., the endpoint will initiate the connection towards the remote endpoint) and should be set to a value of 9, which is the discard port. Connection attribute and port MUST follow the rules of [RFC4145]

Some web browsers do not allow non-secure Websocket connections to be made. So, while the recommendation to use Secure WebSockets (i.e. TCP/WSS) is for security reasons, it is also to achieve maximum compatibility among clients.

When using Secure Websockets the CNAME of the SSL certificate must match the WebSocket connection URI host, and while it is possible to generate self signed certificates with IPs as CNAME, it will not be viable in most cases for certificates signed by well known

authorities. So, a new attribute 'ws-uri' is defined in this specification to indicate the connection uri for the WebSocket Client. The Augmented BNF syntax as described in [RFC4234] is:

```
ws-uri      = "a=ws-uri:" ws-URI
```

Where ws-URI is defined in [RFC6455]

When the 'ws-uri' attribute is present in the BFCP media section of the SDP, the IP and port provided in the 'c' lines SHALL be ignored and the full uri SHALL be used instead to open the WebSocket connection

The following are examples of 'm' lines for BFCP connections:

Offer (browser):

```
m=application 9 TCP/WSS/BFCP *  
a=setup:active  
a=connection:new  
a=floorctrl:c-only  
m=audio 55000 RTP/AVP 0  
m=video 55002 RTP/AVP 31
```

Answer (server):

```
m=application 50000 TCP/WSS/BFCP *  
a=setup:passive  
a=connection:new  
a=ws-uri:wss://bfcps-ws.example.com?token=3170449312  
a=floorctrl:s-only  
a=confid:4321  
a=userid:1234  
a=floorid:1 m-stream:10  
a=floorid:2 m-stream:11  
m=audio 50002 RTP/AVP 0  
a=label:10  
m=video 50004 RTP/AVP 31  
a=label:11
```

## 7. Authentication

Section 9 of [I-D.ietf-bfcpsbis-rfc4582bis] states that BFCP clients and floor control servers SHOULD authenticate each other prior to accepting messages, and RECOMMENDS that mutual TLS/DTLS authentication be used. However, browser-based WebSocket clients have no control over the use of TLS in the WebSocket API [WS-API], so it is RECOMMENDED that standard Web-based methods for client and server authentication are used, as follows.

When a BFCP WebSocket client connects to a BFCP WebSocket server, it SHOULD use TCP/WSS as its transport. The WebSocket client SHOULD inspect the TLS certificate offered by the server and verify that it is valid.

Since the WebSocket API does not distinguish between certificate errors and other kinds of failure to establish a connection, it is expected that browser vendors will warn end users directly of any kind of problem with the server certificate.

A floor control server that receives a message over TCP/WS can request the use of TCP/WSS by generating an Error message, as described in Section 13.8 of [I-D.ietf-bfcpbis-rfc4582bis], with an Error code with a value of 9 (use TLS).

Prior to sending BFCP requests, a BFCP WebSocket client connects to a BFCP WebSocket server and performs the connection handshake. As described in Section 3 the handshake procedure involves a HTTP GET method request from the client and a response from the server including an HTTP 101 status code.

In order to authorize the WebSocket connection, the BFCP WebSocket server MAY inspect any cookie [RFC6265] headers present in the HTTP GET request. For many web applications the value of such a cookie is provided by the web server once the user has authenticated themselves to the web server, which could be done by many existing mechanisms. As an alternative method, the BFCP WebSocket Server could request HTTP authentication by replying to the Client's GET method request with a HTTP 401 status code. The WebSocket protocol [RFC6455] covers this usage in section 4.1:

If the status code received from the server is not 101, the WebSocket client stack handles the response per HTTP [RFC2616] procedures, in particular the client might perform authentication if it receives 401 status code.

## 8. Security Considerations

Considerations from [I-D.ietf-bfcpbis-rfc4582bis], [I-D.ietf-bfcpbis-rfc4583bis] and RFC5018 [RFC5018] apply.

BFCP relies on lower-layer security mechanisms to provide replay and integrity protection and confidentiality. It is RECOMMENDED that the BFCP traffic transported over a WebSocket communication be protected by using a secure WebSocket connection (using TLS [RFC5246] over TCP).



## 9. IANA Considerations

### 9.1. Registration of the WebSocket BFCP Sub-Protocol

This specification requests IANA to register the WebSocket BFCP sub-protocol under the "WebSocket Subprotocol Name" Registry with the following data:

Subprotocol Identifier: `bfcf`

Subprotocol Common Name: WebSocket Transport for BFCP (Binary Floor Control Protocol)

Subprotocol Definition: TBD: this document

### 9.2. Registration of the 'TCP/WS/BFCP' and 'TCP/WSS/BFCP' SDP 'proto' Values

This document defines two new values for the SDP 'proto' field under the Session Description Protocol (SDP) Parameters registry. The resulting entries are shown in Figure 1 below:

Value	Reference
-----	-----
TCP/WS/BFCP	[TBD: this document]
TCP/WSS/BFCP	[TBD: this document]

Figure 1: Values for the SDP 'proto' field

### 9.3. Registration of the 'ws-uri' SDP media attribute

This section instructs the IANA to register the following SDP attribute under the Session Description Protocol (SDP) Parameters registry:

Contact name TBD

Attribute name `ws-uri`

Long-form attribute name WebSocket Connection URI

Type of attribute Media level

Subject to charset No

Purpose of attribute The 'ws-uri' attribute is intended to be used as connection URI for opening the WebSocket.

Allowed attribute values A ws-URI as defined in [RFC6455]

#### 9.4. Acknowledgements

The authors want to thank Robert Welboun, from Acme Packet, who made significant contributions to the first version of this document.

#### 10. References

##### 10.1. Normative References

- [I-D.ietf-bfcpbis-rfc4582bis]  
Camarillo, G., Drage, K., Kristensen, T., Ott, J., and C. Eckel, "The Binary Floor Control Protocol (BFCP)", draft-ietf-bfcpbis-rfc4582bis-10 (work in progress), November 2013.
- [I-D.ietf-bfcpbis-rfc4583bis]  
Camarillo, G. and T. Kristensen, "Session Description Protocol (SDP) Format for Binary Floor Control Protocol (BFCP) Streams", draft-ietf-bfcpbis-rfc4583bis-08 (work in progress), November 2013.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
- [RFC4145] Yon, D. and G. Camarillo, "TCP-Based Media Transport in the Session Description Protocol (SDP)", RFC 4145, September 2005.
- [RFC4234] Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", RFC 4234, October 2005.
- [RFC5018] Camarillo, G., "Connection Establishment in the Binary Floor Control Protocol (BFCP)", RFC 5018, September 2007.
- [RFC6455] Fette, I. and A. Melnikov, "The WebSocket Protocol", RFC 6455, December 2011.

##### 10.2. Informative References

- [RFC2616] Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., and T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1", RFC 2616, June 1999.
- [RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.

[RFC6265] Barth, A., "HTTP State Management Mechanism", RFC 6265, April 2011.

[WS-API] W3C and I. Hickson, Ed., "The WebSocket API", May 2012.

Authors' Addresses

Victor Pascual  
Quobis

Email: victor.pascual@quobis.com

Anton Roman  
Quobis

Email: anton.roman@quobis.com

Stephane Cazeaux  
France Telecom Orange

Email: stephane.cazeaux@orange.com

Gonzalo Salgueiro  
Cisco Systems, Inc.  
7200-12 Kit Creek Road  
Research Triangle Park, NC 27709  
US

Email: gsalguei@cisco.com

Sergio Garcia Murillo  
Medooze

Email: sergio.garcia.murillo@gmail.com