

WebSockets

The Real-Time Web, Delivered

July 23, 2011

Brian McKelvey

Co-Founder - Worlize Inc.

twitter - @theturtle32

www.worlize.com

Whiteboard Demo

- **Get FireFox 7 Alpha**
- <http://www.mozilla.com/firefox/channel/>

The Problem

- No officially supported way to do real-time communications in the browser.

Hacks, Hacks, Hacks

- Polling
- Long-polling
- IFrame Streaming
- HTMLFile (MSIE)
- XHR-Multipart (Firefox)

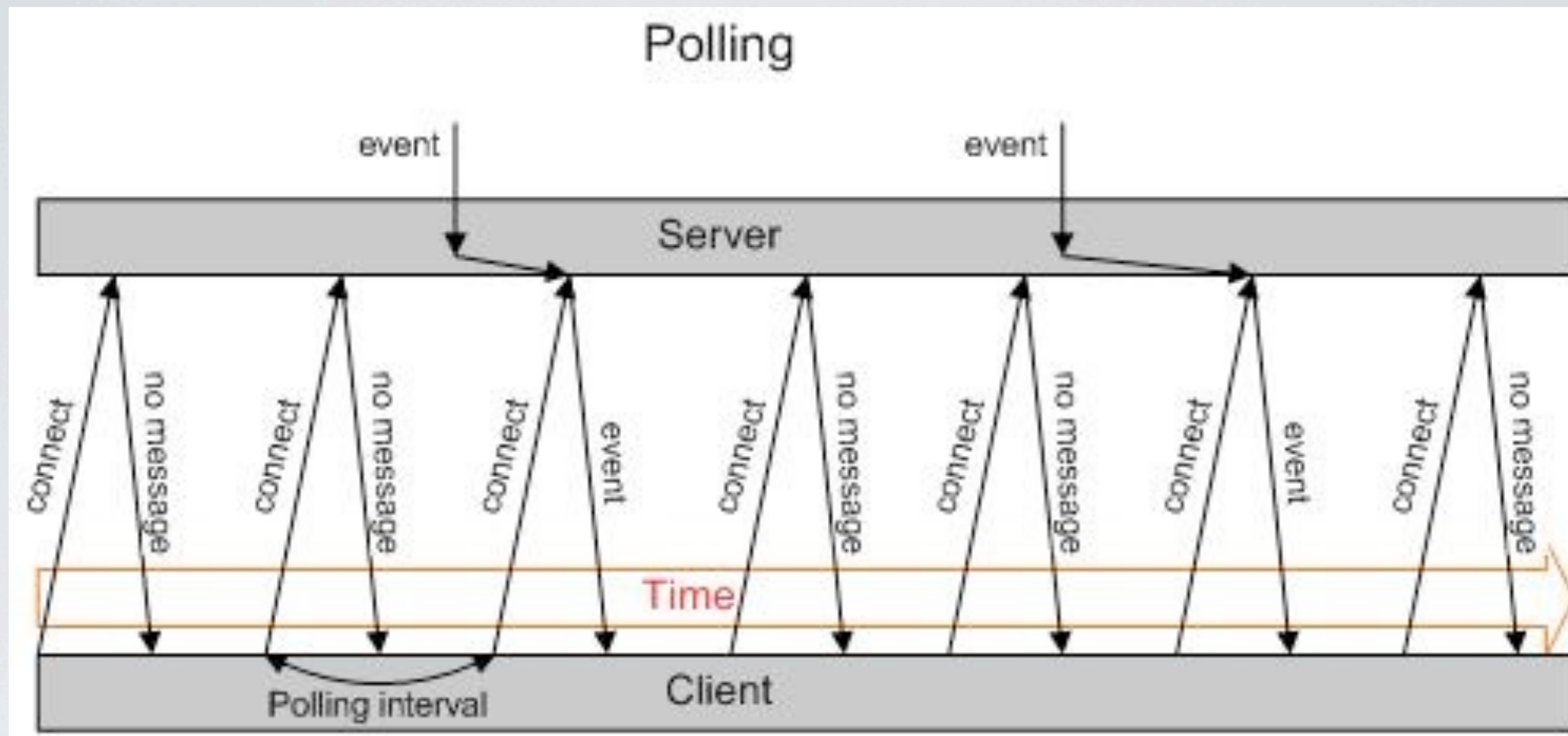


Diagram from http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.ajax.devguide.help/docs/PureAjax_pubsub_clients.html

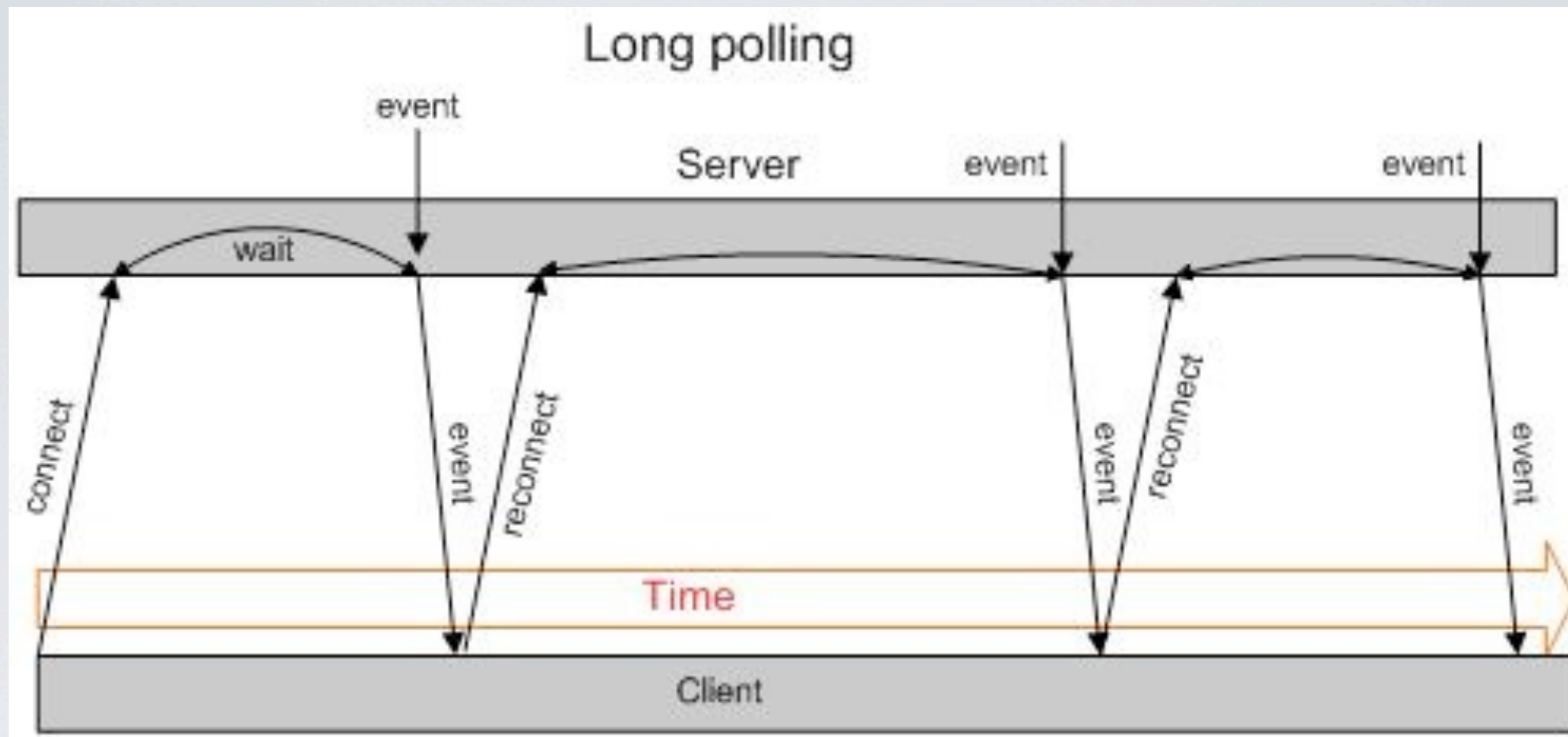


Diagram from http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.ajax.devguide.help/docs/PureAjax_pubsub_clients.html

The Solution: WebSockets

- Maintains a persistent bi-directional communications channel
- Eliminates the need for hacks

Why not TCP Sockets?

- API Simplicity
 - TCP is a stream-oriented protocol
 - We want a message-oriented protocol
- Security
 - Scan a Local Network
 - DDOS Attack

WebSocket Drafts

- **Started at WhatWG**

- WhatWG Draft-75 (old browsers)
- WhatWG Draft-76 (*Chrome, Safari*)

- **Moved to IETF**

- **HyBi** - *HyperText Bi-directional Working Group*
 - Draft-00 (*Same as WhatWG Draft-76*)
 - Draft-07 (*Firefox 6 beta*)
 - Draft-09 (*Firefox 7 alpha*)

The Details: Handshake

- **Built on HTTP**

- Traverse existing proxies/intermediaries
- Co-exist on same port with HTTP/HTTPS server

The Details: Handshake

Client Request

GET /chat HTTP/1.1

Connection: Upgrade

Upgrade: websocket

Sec-WebSocket-Version: 8

Sec-WebSocket-Key: reaiKXo+d4Hkqt45PNTlNg==

Sec-WebSocket-Origin: http://piglet.worlize.com:8080

Sec-WebSocket-Protocol: superchat, boringchat

Sec-WebSocket-Extensions: deflate-stream

The Details: Handshake

Server Response

HTTP/1.1 101 Switching Protocols

Connection: Upgrade

Upgrade: websocket

Sec-WebSocket-Accept: ly0M3juCftp2uqk8/9fVWt4Vfol=

Sec-WebSocket-Protocol: superchat

Sec-WebSocket-Extensions: deflate-stream

The Details: Handshake

- **Security**

- Cross-Origin handling via **Sec-WebSocket-Origin**
- **Sec-WebSocket-Key** Validation
 - Prevent cross-protocol attacks
 - Fail early if a dumb intermediary provides a cached response.
- **Sec-** headers prevent XHR from being used to contact a WebSocket server

The Details: Masking

- Most contentious issue in the HyBi Working Group.
- **All** client-to-server messages are masked.
- **Why** is this necessary?
 - Prevent cache-poisoning attacks
 - Prevent talking to overly permissive servers
 - Concern over this issue caused some browser vendors to **pull support** for WebSockets draft-76.

The Details: Masking

- How does it work?
 - Randomly generated four-byte mask key per frame
 - Applied using XOR to frame payload
- Reduces compression efficiency for client-to-server messages

The Details: Framing

- Simple framing protocol facilitates **message** oriented API
- 2 to 10 bytes for frame header
- Contains **flags**, **opcode**, and payload **length**
- Payload length is a variable length field.

The Details: Framing

- **Data frame types:**

- Binary Message
- UTF-8 Text Message
- Continuation
(fragmentation)

- **Control frame types:**

- Ping
- Pong
- Close

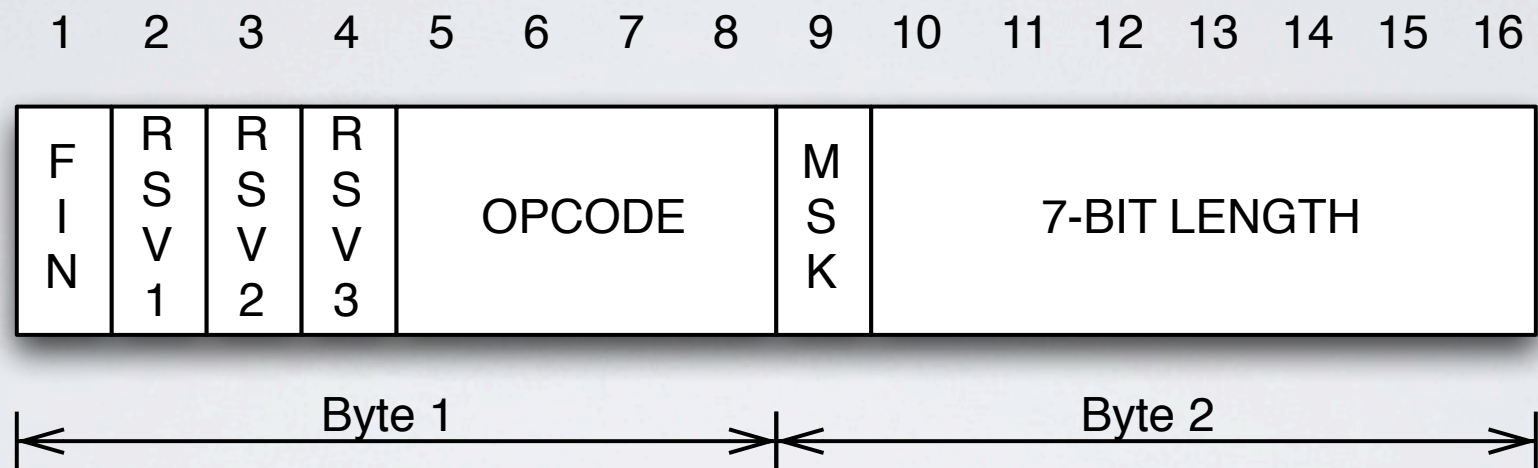
The Details: Framing

- **Fragmentation**

- Allows control frames in the middle of a long message
- In coordination with a future extension can facilitate multiplexing.

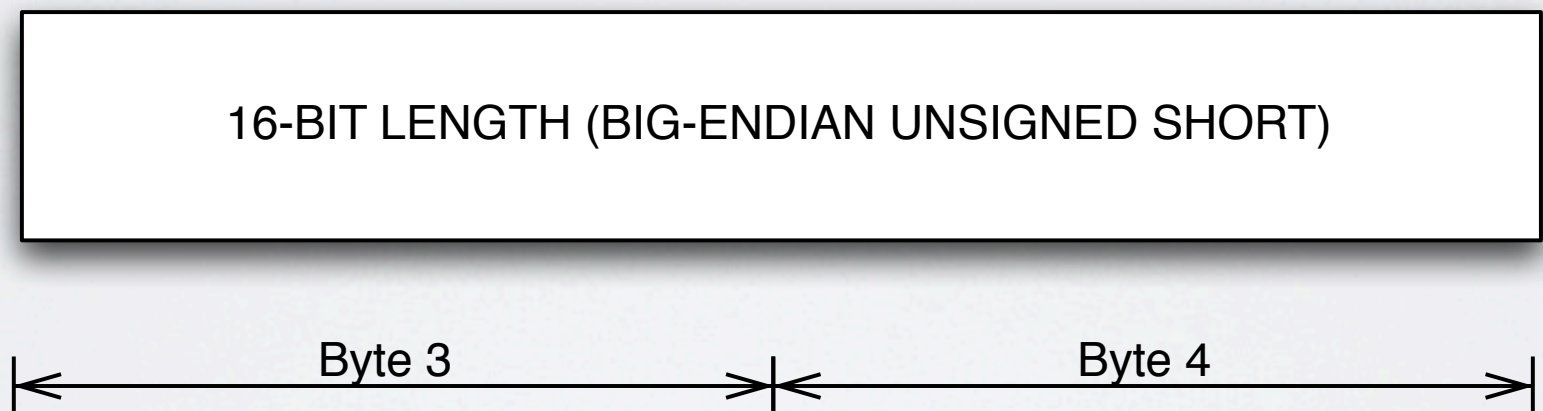
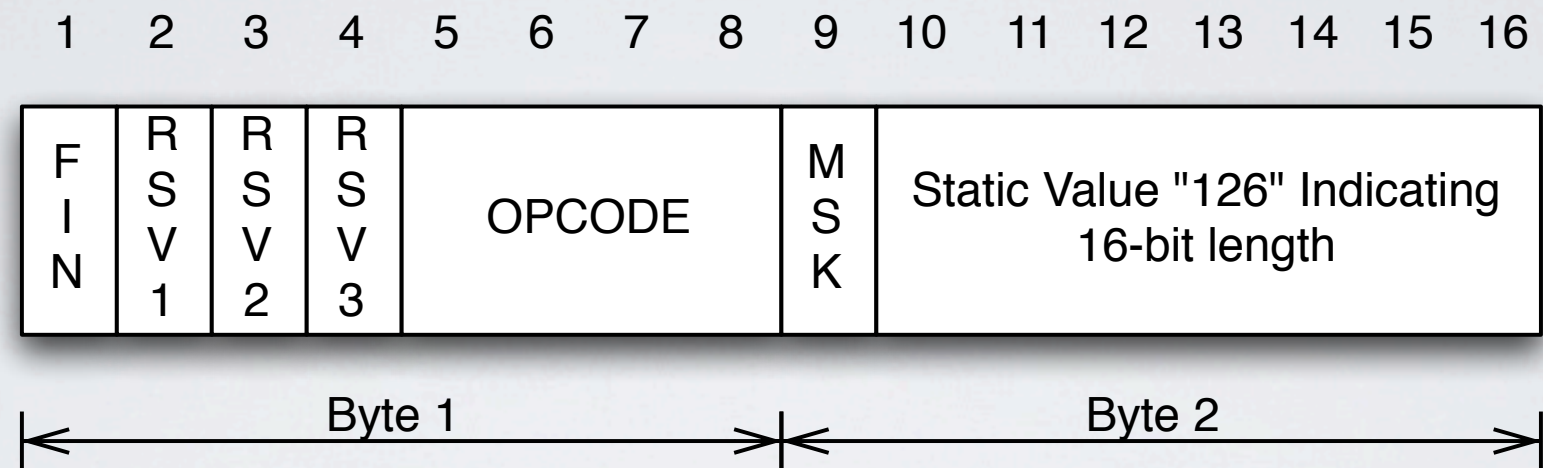
Basic Frame Header

Frames less than 126 bytes



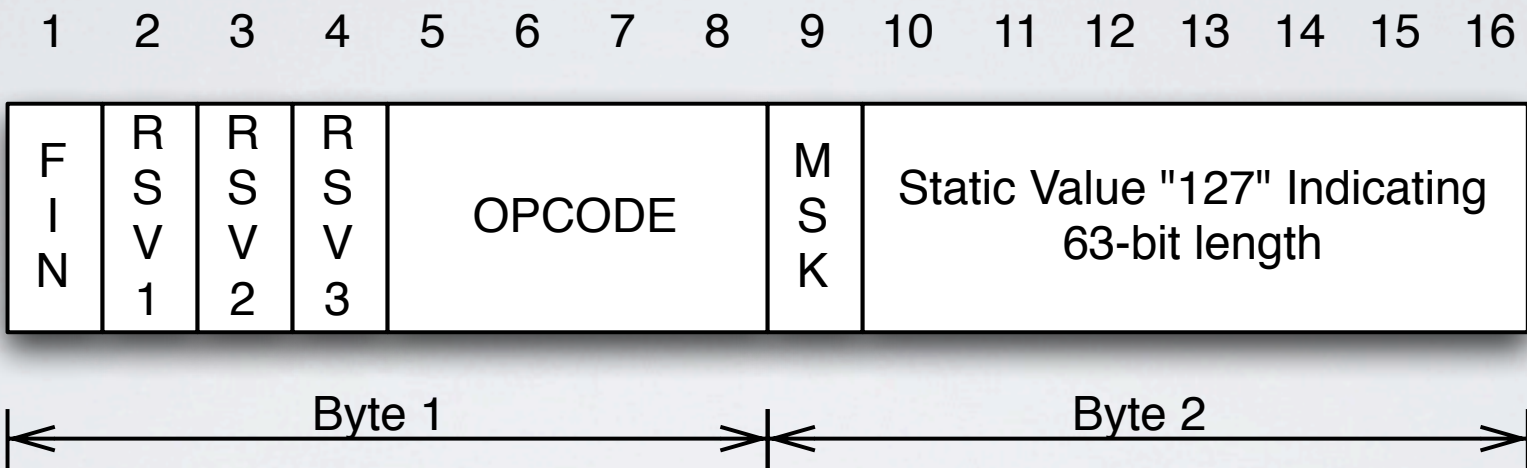
Medium Frame Header

≥ 126 bytes && < 65535 bytes



Long Frame Header

> 65535 bytes



0	63-BIT LENGTH (BIG-ENDIAN UNSIGNED)
	63-BIT LENGTH (Continued)
	63-BIT LENGTH (Continued)
	63-BIT LENGTH (Continued)

Server Implementations

- Node.js: **WebSocket-Node**
 - <https://github.com/Worlize/WebSocket-Node>
- ANSI C: **libwebsockets**
 - <http://git.warmcat.com/cgi-bin/cgit/libwebsockets/>
- Java: **Jetty**
 - <http://webtide.intalio.com/2011/04/getting-started-with-websockets/>

Client Implementations

- Node.js: **WebSocket-Node**
 - <https://github.com/Worlize/WebSocket-Node>
- ActionScript 3: **AS3WebSocket**
 - <https://github.com/Worlize/AS3WebSocket>
- ANSI C: **libwebsockets**
 - <http://git.warmcat.com/cgi-bin/cgit/libwebsockets/>

Demo

Shared Whiteboard Example

- Available in the 'examples' folder of:
<https://github.com/Worlize/WebSocket-Node>

Requires FireFox 7 Alpha!